From: Megan [redacted]
Sent: Monday, February 13, 2023 6:18 PM
To: Regulations
Subject: privacy audits and assessments
Attachments: white paper 4.18.18.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

--

Megan Gray
GrayMatters Law & Policy
Washington, DC (AdMo)
[redacted]

Understanding and Improving Privacy "Audits" under FTC Orders

April 2018

by Megan Gray

Table of Contents

Understanding and Improving Privacy "Audits" under FTC Orders

April 2018
by Megan Gray*

I. Introduction

The Federal Trade Commission (FTC) is the primary federal agency protecting consumer privacy. The agency regularly touts its important and extensive work as the chief consumer privacy "cop on the beat." But this chest-thumping can backfire -- consumers may more readily share personal information via online platforms based on a belief that the FTC is guarding against misuse. The FTC actually has pursued only a small number of privacy cases relating to a company's unreasonable or excessive collection, use, and retention of consumer data, carving out those instances when the company acts contrary to an express privacy statement, fails to adequately protect against malicious and unknown hackers, or violates a specific federal statute (e.g., COPPA, FCRA).

This is why the FTC's 2011 and 2012 orders against Google and Facebook were heralded so heartily. For the first time, it was thought, the FTC had the unambiguous ability to ensure the companies instituted reasonable privacy protections.[1] As Berin Szoka of Tech Freedom noted, "the FTC is finding a way to regulate online privacy sans national legislation directly addressing the issue."[2] Moreover, the orders required independent,

---

* The author is a non-residential Fellow at Stanford Law School's Center for Internet and Society. This is a paper in progress, published to stimulate discussion and critical comment. The author has researched and written this paper, based on publicly available documents, in her non-work, non-family time, which is necessarily limited; she anticipates future edits will greatly improve on this draft. The views expressed in this paper are those of the author and do not necessarily reflect the author's past, present, or future employers or clients.

[1] The orders state the company must "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information..."

[2] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

third-party audits, it was thought, to verify the companies' compliance, thereby relieving any concern the FTC did not have the resources to monitor compliance.[3]

David Vladeck, the then-Director of the FTC's Consumer Protection Bureau, asserted, "I think the [audit] commitment that Google and Facebook have made is really an important one. Auditors are going to come in and make sure they are actually meeting the commitments laid out in their privacy policy. The audits are designed to make sure that companies bake privacy in at every step of offering a product or service. This is going to require the expenditure of a lot of money and a lot of time for companies that did not start out doing things this way. ….They've got to go back and rebuild their business in a way that takes privacy into account."[4]

According to Maneesha Mithal, of the FTC's Privacy and Identity Protection Division, "The main difference is that a [data breach] security audit is about how to protect info from unauthorized access, while a privacy audit is about how to protect info from authorized *and* unauthorized access."[5] An outside privacy expert elaborated: "[D]ata security audits...focus on ensuring that information the company has on us isn't vulnerable to hackers. But a privacy audit focuses more on how a company is using

---

[3] Not all FTC privacy or data security cases have a third-party audit provision. *See,* e.g., *FTC v. Frostwire, LLC* (2011), https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon.

[4] "The FTC Privacy Cop Cracks Down" by Technology Review (June 26, 2012), https://www.technologyreview.com/s/428342/the-ftcs-privacy-cop-cracks-down/. *See also* David Vladeck closing letter to Google on the StreetView wi-fi collection: "...Google should develop and implement reasonable procedures, including collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored." https://www.ftc.gov/enforcement/cases-proceedings/closing-letters/google-inquiry.

[5] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/. *See also* 2012 FTC letter to Commenter Meg Roggensack of Human Rights First: "[T]he order requires Facebook to...obtain biennial privacy audits by an independent third-party professional. We believe that the biennial privacy assessments will provide an effective means to monitor Facebook's compliance with the order, including with respect to its relationship with its service providers. Each assessment will involve a detailed, written evaluation of Facebook's privacy practices over a two-year period, and will require the auditor to certify that Facebook's privacy controls have adequately protected the privacy of 'covered information' throughout the relevant two-year period." https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmbltrs.pdf.

someone's personal information internally -- how it's aggregated or re-purposed -- and when it's being shared with third parties (such as advertisers)."[6] Jim Kohm, of the FTC's Enforcement Division, predicted that any audit might take an entire six months to conduct, and would likely cost hundreds of thousands of dollars.[7]

II. Closer Inspection of FTC Privacy Orders

The initial excitment eventually dissipated. On closer inspection, the orders arguably did not require "reasonable privacy protections." Rather, the orders were more constrained, and required only a "comprehensive privacy program" that was "reasonably designed" to "address" "privacy risks." Under this language, given the companies' lengthy privacy policies essentially stating that users did not have any privacy, the FTC could face an uphill battle in asserting misuse of consumer data. This struggle would be complicated by the orders' inclusion of a reasonableness standard – the FTC carries the burden of proof in any judicial proceeding, and (arguably) no consensus exists on reasonableness in this context. Moreover, in transforming any privacy case against the companies from a Section 5-based violation into an order-based violation, the FTC arguably increased its challenges, because it would have to relinquish control over any such case -- the Department of Justice (DOJ), not the FTC, litigates the agency's civil penalty cases.[8]

---

[6] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

[7] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

[8] 15 U.S.C. §56(a) (1). If DOJ rejects the case or does not file the civil penalty action within 45 days, the FTC can file the lawsuit itself, but DOJ rarely declines FTC referrals. Few practitioners understand the legal intricacies distinguishing an FTC civil penalty case, an FTC contempt case, and an FTC Section 5 case (which itself can be subdivided into Section 5 administrative cases and Section 5 federal court cases). Key points: (a) violation of an FTC administrative order (e.g., Google, Facebook) is a civil penalty case, filed by DOJ in the name of the United States; it carries a "preponderance of evidence" standard of proof and can result in money fines without evidence of actual consumer harm, as well as injunctive relief; (b) violation of an FTC federal court order (e.g., Wyndam) is a contempt action filed by the FTC; it carries a higher "clear and convincing" standard of proof, and monetary awards are difficult to obtain in the privacy context; (c) Section 5 privacy cases carry a "preponderance of evidence" standard of proof, but, when the consumer has incurred no direct out-of-pocket loss, the company almost never pays money; and (d) Section 5 administrative cases cannot result in a monetary award, but, following the conclusion of the case, the FTC can file a second case in federal court under Section 19 to obtain financial resitution for consumers.

As a result, the third-party audits took on added significance. Because the public versions of those audits are heavily redacted and written in almost impenetrable language, the public learned little.[9] Careful review, however, shows the audits are woefully inadequate."[10]

III. Closer Inspection of Privacy "Audits" Under FTC Orders

The third-party "audits" required under FTC orders sound more impressive than they actually are.[11] For example, the Google audits evaluate just seven points, so vague or duplicative as to be meaningless. In sum: (1) Google has a written, comprehensive privacy program; (2) Google has specific employees working on the privacy program; (3) Google has a privacy risk assessment process and undertakes to mitigate those risks; (4) Google has procedures to address identified privacy risks; (5) Google monitors the effectiveness of its privacy program; (6) Google has contracts with third parties who are capable of protecting privacy; and (7) Google evaluates and adjusts its privacy program as needed when its business changes.

---

[9] Redacted versions are available on ftc.gov and epic.org. Standard FTC order language can confuse. FTC orders require an initial compliance report, which is written by the company itself and is fully available to the public (i.e., unredacted). The initial third-party "assessment" is submitted later, with only a redacted version publicly released; subsequent third-party assessments, depending on particular order requirements, might not be submitted to the FTC at all. *See*, e.g., https://epic.org/privacy/ftc/googlebuzz/FTC-Initial-Assessment-09-26-12.pdf, https://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf, https://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf, https://www.ftc.gov/system/files/documents/foia_requests/1209googleprivacy.pdf. The initial third-party Google privacy assessment, as posted at epic.org, appears to be missing page
24 but is available at ftc.gov (with the entire page redacted).

[10] *See* "Assessing the FTC's Privacy Assessments, by Chris Hoofnagle (2016), https://ieeexplore.ieee.org/document/7448350/. *See also* Robert Gellman's critique of the audits conducted by the self-regulatory organization Network Advertising Initiative (NAI): "Lacking in Facts, Independence, and Credibility:
The 2011 NAI Annual Compliance Report" (July 2012), https://bobgellman.com/rg-docs/RG-NAI-2011.pdf.

[11] "Why Facebook's 2011 Promises Haven't Protected Users," Wired (April 11, 2018) (discussing third-party audits), https://www.wired.com/story/why-facebooks-2011-promises-havent-protected-users/.

This seven-point privacy program was "audited" by an independent, third-party "assessor," whose role was merely to find some evidence that supported actual implementation of the seven points. For example, the auditor confirmed that Google has a publicly available, written privacy policy; employees who focus on privacy risks; privacy training for some employees; privacy settings available for users; a form for managers to complete when a privacy issue arises; and contractual privacy provisions with third parties.[12]

These assessments could not be more starkly different from what FTC management described in earlier news reports.[13] What happened?

[12] Some businesses, particularly small start-ups, may only need a de minimus privacy program like this. *See* AICPA's Privacy Maturity Model, https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf. While FTC orders require assessors to "explain how the privacy controls are appropriate to the respondent's size and complexity, the nature and scope of the company's activities, and the sensitivity of the covered info," assessors do not appear to do so, other than to verbatim parrot that text. For example, in answering this question, the Facebook assessor intones, "Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by [sic] the order), Facebook management developed the company-specific criteria (assertions) detailed on pages 77-78 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment."

[13] "We don't want [an auditor] who is going to just rubber stamp their procedures," said the FTC's Jim Kohm. "So What Are These Privacy Audits That Company and Facebook Have To Do For The Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/. While the agency may not have fully appreciated this rubber-stamp risk when the orders issued, it became aware of the problem at some later point. *See,* e.g.*,* World Privacy Forum comment in *FTC v. Uber* (September 2017), "While this requirement for assessments appears impressive on the surface, it has serious shortcomings. The obligation for an assessment is less than meets the eye.... Commission staff also sometimes refers to the assessments as audits.... We find this to be significantly misleading. We suggest that any Commission staff member who discusses a Commission consent decree in public and who refers to an assessment as an audit be required to stay after work and write 100 times '*An assessment is not an audit'....*", https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141341.pdf.

IV. An "Attestation" Is a Type of "Audit," Which Is a Type of "Assessment" that Relies on "Assertions"

Of the many audit models available from national and international standard-setting bodies, Google and Facebook selected the "attestation" model, which relies on conclusory hearsay, formally known as "management assertions."[14] As a result, assessments can be circular (e.g., "Management asserts it has a reasonable privacy program. Based on management's assertion, we certify that the company has a reasonable privacy program.").[15] The FTC's privacy cases have not usually stemmed from intentional transgressions; rather, the cases usually arise from issues the company

[14] The contracts ("engagement letters") between the assessors and the assessed companies are not publicly available. *U.S. v. Consumer Portfolio Services* (a 2014 FTC civil penalty case) could provide model language: "The management letter between [the company] and the third party monitor shall grant Commission staff access to the third party monitor's staff, work papers, and other materials prepared in the course of the...audit...", https://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc.

Because the engagement letters are non-public, and because of the heavy redactions in the assessments themselves, one cannot be sure which auditing standards apply. The assessors may not have followed the professional standards by which they are bound. The assessments state they are attestation models governed by AICPA (American Institute of Certified Public Accountants) and IAASB (International Auditing and Assurance Standards Board). AICPA categorizes privacy audits as either attestation engagements, privacy review engagements, or agreed-upon (specified auditing) procedure engagements. AICPA further subdivides attestation engagements into SOC1, SOC2, and SOC3. Based on features of the redacted Google and Facebook assessments, they are likely SOC2 attestations. AICPA subdivides SOC2 into Type 1 and Type 2 engagements. AICPA's SOC2 Guide is only available for purchase. This Guide is an authoritative AICPA interpretation and application of AT Section 101, which is the official standard for a SOC2 engagement. SOC reports are a new development, following the auditing world's transition in June 2011 from SAS 70 (AICPA's Standards on Auditing Statements) to SSAE 16 (AICPA's Standards on Attestation Engagements), a transition to align more closely to IAASB (and its ISAE 3402, which incorporates ISAE 3000 as foundation).

[15] For example, the Google assessors use the following certification language: "In our opinion, Google's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period, in all material respects...based upon the Google Privacy Program set forth in Attachment A of Management's Assertion in Exhibit I." (emphasis added).

overlooked or did not adequately disclose to consumers. A privacy audit that relies on management assertions will rarely uncover these blind spots.[16]

In a similar assessment context, one security expert opined that the attestation certification is not a seal of approval because the standard allows the company itself to decide what risks to document and what risk-management processes to adopt. "In sporting metaphor, [the company] **gets to design their own high-jump bar, document how tall it is and what it is made of, how they intend to jump over it and then they jump over it. The certification agency simply attests that they have successfully performed a high-jump over a bar of their own design."** (emphasis added). He added: "What would be really interesting would be if the company publishes their security requirements, their standards, their policies and risk assessments, so everyone can see what kind of high-jump they have just performed -- how high, how hard, and landing upon what kind of mat? It would be that which would inform me of how far I would trust a company with sensitive data…"[17]

Another security expert elaborated: "An example illustrating the difference between assessing security and auditing security might help clarify this point. Let's look at access controls. One component of access control security is a strong password policy. An assessment would check to see if the organization has a strong password policy while a security audit would actually attempt to set up access with a weak password to see if the control actually has been implemented and works as defined in the policy."[18]

Similarly, a ComputerWorld article trivialized an Uber privacy audit.[19] The article quotes from the purported audit: "While it was not in the scope of our review to perform a technical audit of Uber's data security controls, based on our review of data security policies and interviews with employees, we found that Uber has put in place and continues to develop a data seurity program that is reasonably designed to protect

---

[16] Arguably, a privacy audit relying on management assertions is wholly unsuitable when the company has been recently fined by a government agency for being less than forthright during an investigation into the company's privacy practices. In 2012, the Federal Communications Commission (FCC) fined Google on this basis in connection with its StreetView program. https://apps.fcc.gov/edocs_public/attachmatch/DA-12-592A1_Rcd.pdf.

[17] https://www.dogsbodytechnology.com/blog/iso27001-certification/.

[18] http://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.

[19] http://www.computerworld.com/article/2880596/uber-shows-how-not-to-do-a-privacy-report.html.

Consumer Data from unauthorized access, use, disclosure, or loss."[20] The article made this point: "Let's zero in on the key utterance: 'it was not in the scope of our review to perform a technical audit of Uber's data security controls.' Based on the report and its stated methodology, the investigators weren't trying to see if Uber really obeyed its own written privacy policies. It was merely allowed to see if that written policy was an appropriate policy. But privacy policies, written by lawyers and HR specialists, are rarely the problem. The problem tends to be what employees actually do."[21]

V. Avenues to Improve FTC Privacy Assessments

The FTC's third-party privacy assessments have the potential to be an incredibly important component of the agency's enforcement program, especially given the Commission's small size and budget. The FTC, if so inclined, could pursue a variety of avenues to obtain better assessments. Most obvious, the FTC could state that "attestations" do not comply with an order's assessment provision. However, the term "assessment" is not well defined in the orders – and a common legal principle is that ambiguous terms are construed against the drafter. That said, this doctrine arguably would not apply in this situation (e.g., the term is not ambiguous because the standard dictionary definition should apply, not a technical certified-auditor definition).

Alternatively, the FTC could go beyond any submitted assessment, and conduct its own assessment under a diferent order provision.[22] The orders require companies to retain all materials that call into question the company's compliance with the order, as well as all materials relied on in preparing the assessment. Moreover, companies must respond to any relevant FTC inquiry within ten days.[23] Under these provisions, the FTC could obtain, for example, any assessment submitted to the company itself or other regulators,

---

[20] The redacted version of the Google assessment contains a similar disclaimer. "We are not responsible for Google's interpretation of, or compliance with, information security or privacy-related laws."

[21] Commenters to FTC privacy orders have raised these issues to the Commission, but the agency has not altered the assessment provision. *See* World Privacy Forum comment in *FTC v. Uber* (September 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141341.pdf.

[22] *But see* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.* (FTC should not fault a company's data security if a third-party assessor approved it), https://www.ftc.gov/public-statements/2015/12/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v.

[23] *U.S. v. Morton Salt Co.*, 338 U.S. 632, 650 (1950).

domestic or foreign, and use that assessment to identify discrepancies or any areas for improvement.[24]

A. Improving Attestation Assessments

But even if the FTC did not want to entirely reject the submitted assessments or mount an argument against the "choice of model" (i.e., attestation), the FTC could insist companies submit revised assessments, improved in numerous ways, while still operating under the attestation framework. A properly designed attestation with sufficient granularity will look very much like an audit.

1. Examination Focus (Scope)

At the onset, an assessor determines the scope of the project. For a large company, attestation guidance seems to require a privacy assessment to be separately conducted along product lines.[25] By lumping multiple Google divisions (e.g., automonous cars, YouTube, search, email, voice-activated assistant, etc.) into a single privacy assessment, and using the same measuring stick for all, an assessment will have such a high level of abstraction (review at 10,000-foot level) that it serves no useful function. Noting that the redacted 2012 Google assessment is a mere 22 pages, one privacy professor opined, "How could such a short document account for all the company's information collection and handling activites from its multiple product lines?"[26]

---

[24] *See* the Irish Data Protection Commission's requirement that Facebook implement 45 granular privacy changes. As conveyed in the cover letter to the Facebook initial assessment, "Our privacy efforts received a substantial boost in 2011 and 2012, when the Data Protection Commissioner in Ireland [reviewed our compliance] with European data protection law. That review resulted in two comprehensive audit reports that documented Facebook's controls...and identified areas where we can continue to improve."

[25] "The scope of the engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (retail operations, but not manufacturing operations or only operations originating on the entity's web site or specified web domains) or geographic locations (such as only Canadian operations). In addition, the scope of the engagement generally should be consistent with the description of the entities and activities covered in the privacy policy." www.webtrust.org/download/Trust_Services_PC_10_2006.pdf.

[26] *See* "Assessing the FTC's Privacy Assessments, by Chris Hoofnagle (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163.

Similarly, Google and Facebook regularly acquire a large number of companies.[27] Their redacted assessments do not indicate how those acquisitions are folded into either the company's privacy program or evaluated during the assessment period.[28] Ironically, immediately after touting the wide variety of Google services, 30,000 employees, and 70 offices in 40 countries, the Google assessor claimed that user data falls into only 3 categories: log data, account data, and [redacted].

Given these odd attributes, the FTC could insist on revised assessments with more appropriate and explicit scoping parameters. *See U.S. v. Upromise* (2017 FTC civil penalty order violation case alleging, among other issues, that "Upromise obtained and submitted assessments that were impermissibly narrow in scope...").[29]

2. Protocol Issues (Selection of Controls and Criteria)

Many detailed protocols exist for evaluating privacy programs. The standard-bearer is AICPA's GAPP (for "generally accepted privacy principles"), which is comprehensive and granular, even providing extensive illustrative privacy controls).[30] The Google and

[27] https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet.

[28] The most recent Google assessment identifies its Motorola acquisition, but unilaterally carves out its compliance for over a year after the acquisition. Of separate interest, FTC orders have a provision requiring companies to report "any change in [the company] that may affect compliance obligations arising under this order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order..." (emphasis added). Arguably, the emphasized text requires reports on many acquisitions, particularly those implicating user data enhancement or user profile applications.

[29] https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc.

[30] GAPP is of course different from GAAP ("generally accepted accounting principles"). *See* https://en.wikipedia.org/wiki/Generally_Accepted_Privacy_Principles; http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_Principles%20and%20Criteria.pdf. At last check, GAPP was being updated. ISACA (Information Systems Audit and Control Association) may also have a robust privacy protocol (denominated G31). Microsoft also promotes a robust, well-documented data governance program, https://download.microsoft.com/download/2/0/a/20a1529e-65cb-4266-8651-1b57b0e42daa/protecting-data-and-privacy-in-the-cloud.pdf, https://www.microsoft.com/en-us/trustcenter/about/transparency, https://www.microsoft.com/en-us/trustcenter/privacy/we-set-and-adhere-to-stringent-standards. Aprio is another entity that provides extensive auditing protocols for online businesses, https://www.aprio.com/wp-content/uploads/aprios-iso-27001-certification-program2.pdf.

Facebook assessments rejected GAPP in favor of customized checklists, which bear no resemblance to GAPP.[31]

By using tailor-made controls and criteria within an attestation framework, the Google and Facebook assessments are almost indecipherable, requiring certified-auditor knowledge.[32] The auditing profession uses dense and confusing terms, the meanings of which are often counter-intuitive or have a heightened-scrutiny illusion. For example, a company could be subject to an auditor's "examination" and "testing" of certain data – but this activity could be as simple as the auditor confirming that the company has a posted privacy policy. For example, the Google assessor states that it "independently tested each Google privacy control listed in the Management Assertion and Supporting Privacy Controls" and "[o]ur test procedures included, where appropriate, selecting samples and performing a combination of inquiry, observation, inspection, and/or examination procedures." Yet, pursuant to auditor nomenclature, the assessor's "inquiry test" could have been merely interviews of certain employees to ask rote questions repeating the management assertions. Similarly, while it may be reassuring to learn an assessor reviewed thousands of individual artifacts that were collected from dozens of company employees, in reality, this is meaningless without additional context (e.g., what is an artifact, were any duplicative or irrelevant).[33]

To better understand the protocol grounds on which the FTC could question the assessment, one must understand two key terms. "Controls" are policies and procedures that address risks associated with reporting, operations, or compliance and, when

---

[31] Confusingly, while the Google assessment claims to follow AICPA, it does not track GAPP. Rather, the assessment complies with AICPA rules for attestation engagements; it does not follow AICPA for the substantive protocol. AICPA procedural rules do not require use of the GAPP substance for controls/criteria; AICPA says use of GAPP is merely a recommendation. Thus, both use and non-use of GAPP is a "procedure and standard generally accepted in the industry," which is the applicable FTC order requirement. Similar to Google, the Facebook initial compliance report and the cover letter to its initial assessment claim it has adopted the GAPP framework as a benchmark, but that is not borne out in the mangement assertions undergirding the assessment. However, "[I]f a practitioner does not apply the attestation guidance [i.e., GAPP] included in an applicable attestation interpretation, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance." AICPA AT Section 50 (para 6), Defining Professional Requirements in Statements on Standards for Attestation Engagements.

[32] While the FTC often hires consultants for technical issues, it has a limited budget. The agency could request assistance from its sister agency, the U.S. Governmental Accounting Office (GAO); James Dalkin is a GAO director with expertise in AICPA attestations.

[33] *See also* AICPA AU 325 (standards for defining "deficiency in internal control," "significant deficiency," and "material weakness").

operating effectively, enable an entity to meet specified "criteria." "Criteria" are the benchmarks used to measure compliance with the controls. In an attestation, company management selects the criteria. However, the standard-setting body for auditors conducting attestations states that "any relevant factors [that are] omitted [can not] alter the conclusion [of the report]."[34] The FTC could point to a plethora of missing, conclusion-altering factors that make the selected controls and/or criteria inadequate, as detailed below.

i. Failure to Assess Fair Information Principles: The FTC could insist the protocol include the long-standing Fair Information Principles (FIPs) -- Notice, Choice/consent, Access/participation, Integrity/security, Enforcement/redress, Use Limitation/deletion.[35] The 2012 White House's Consumer Privacy Bill of Rights also included Respect for Context, Focused Collection, and other elements.[36] An assessor who excludes a FIP from the protocol should expressly justify its exclusion. Some audits assert, "The scope of the engagement should cover all of the activities in the information cycle for relevant personal information. These should include collection, use, retention, disclosure, disposal, or anonymization. Defining a business segment that does not include this entire cycle could be misleading to the user of the practitioner's report."[37]

---

[34] *See* AT 101.24. For example, when parsed, the Google assessment shows that its management, not its auditor, determined the criteria ("PWC used pre-defined materiality criteria developed during the planning phase"). *See also* ISAE 3000, another pertinent auditing standard: "If criteria are specifically designed for the purpose of preparing the subject matter information in the particular circumstances of the engagement, they are not suitable if they result in subject matter information or an assurance report that is misleading to the intended users. It is desirable in such cases for the intended users or the engaging party to acknowledge that specifically developed criteria are suitable for the intended users' purposes. The absence of such an acknowledgement may affect what is to be done to assess the suitability of the applicable criteria, and the information provided about the criteria in the assurance report." https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga. When last reviewed, ISAE 3000 was being finalized, and PriceWaterhouseCoopers submitted comments to weaken this portion.

[35] "Fair Information Practices: A Basic History," Bob Gellman, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. *See also* the 2017 privacy advocates' letter to FTC commissioners on incorporating FIPs into the agency's privacy work, https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.

[36] *See* https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

[37] *See* www.webtrust.org/download/Trust_Services_PC_10_2006.pdf.

ii. Failure to Map Data Flow of Consumer Information: Data flow maps are usually the key aspect of privacy audits.[38] "Understanding the data associated with personal information is useful for identifying the processes that involve or could involve personal data, and for the owner of those processes. By identifying the processes and business owners of personal information, the business can then understand the end-to-end flow of personal information including:

- Definition of specific personal information about customers and employees the organization collects and retains, including the methods in which this information is obtained, captured, stored, and transmitted.
- Definition of specific personal information that is used in carrying out business, for example, in sales, marketing, fundraising, and customer relations, including the methods in which this information is obtained, captured, stored, and transmitted.
- Definition of specific personal information that is obtained from, or disclosed to, affiliates or third parties, for example, in payroll outsourcing, including the methods in which this information is obtained, captured, stored, and transmitted.
- Identification of infrastructure components used in the receipt, processing, recording, reporting, and communication of personal information.
- Identification of personnel (including third parties) that have been granted access or potentially could access the personal information and how."[39]

From the redacted assessments, it appears companies do not map their internal or external data flows of consumers' personal information, and therefore are unable to assess whether such data goes astray. Without this, it's practically impossible to evaluate compliance with any standard.

iii. Failure to Determine Notice and Consent: Privacy policies are ubiquitous. Lesser known is that the FTC does not require such policies. Instead, the FTC mainstay is "notice and consent," and simply posting a privacy policy does not neccessarily satisfy this standard. Arguably, if a company knows or should know its consumers do not understand, and therefore cannot consent to, data collection, sharing, or

---

[38] *See* Keith Enright (now Google's Privacy Legal Director), "Privacy Audit Checklist," https://cyber.harvard.edu/ecommerce/privacyaudit.html. Mitre also provides an example of data mapping in privacy audits, https://www.mitre.org/publications/technical-papers/how-to-conduct-a-privacy-audit. It is difficult to imagine that any privacy program could effectively function without the company knowing what information it collects from consumers. It would be disappointing if Google or Facebook does not even internally keep an inventory of cookies or apps existing on its website. *See* University of California Berkeley Law's Web Privacy Census, with inventory of deployed cookies, https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/web-privacy-census/ (last conducted in 2012).

[39] https://www.journalofaccountancy.com/issues/2011/jul/20103191.html.

retention, the company has not satisfied its obligations to provide notice or obtain consent. As alleged in the *U.S. v. Upromise* complaint for violating a FTC privacy order, "...Upromise disclosed this information in such a way that many consumers would either not notice or not understand Upromise's explanation of the ... toolbar's data collection and use."[40] The assessments do not appear to evaluate whether consumers had actual notice or effectively consented to the companies' data pratices.

iv. Failure to Identify Privacy Promises: Large online companies regularly assure consumers (and regulators) that privacy is the core of their business. Such statements are frequently specific and issued at the highest level. For example, Google has a YouTube channel dedicated to privacy.[41] Yet, these company privacy statements do not appear to be inventoried or reviewed, apart from the company's essentially static, official privacy policy. The redacted assessments do not appear to identify or evaluate adherence to these more peripheral privacy statements.

v. Failure to Analyze Order Violations: The redacted assessments do not appear to address previously identified order violations or other breaches of self-regulatory programs that occurred or were discovered during the assessment period. For example, while the initial Google assessment covered the time period scrutinized in the FTC's Safari case, the assessement does not mention it, at least in the redacted version.

---

[40] *See also FTC v. Paypal* (Section 5 complaint for confusing privacy settings), https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter. In the remedial *Upromise* order for violating the underlying privacy order, the FTC required the company to "obtain an evaluation and report from a qualified, objective, independent third-party professional specializing in website design and user experience ("evaluator")...For any disclosure or consent governed by Section I of the FTC Order, the evaluator must certify Defendant's adherence to the FTC Order's 'clearly and prominently' disclosure requirement and 'express, affirmative' consent requirement." https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc. *See also FTC. v. Special Data Processing Corp.* (2004 order describing independent, third-party verification of consumer telephonic consents), https://www.ftc.gov/enforcement/cases-proceedings/002-3213/special-data-processing-corporation. In 2014, the National Science Foundation awarded large money grants to researchers to devise effective privacy notices, https://iapp.org/news/a/researchers-earn-grant-to-study-privacy-notices/. *See also* Lauren Willis, "The Consumer Financial Protection Bureau and the Quest for Consumer Comprehension," proposing that CFPB require firms to demonstrate that a significant proportion of their customers understand key pertinent facts about purchased financial products. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2952485.

[41] https://www.youtube.com/user/googleprivacy. *See also U.S. v. Google* (alleging Google's misrepresentations based on (a) privacy statement not part of official privacy policy; and (b) compliance statement vis-a-vis NAI's Code of Conduct), https://www.ftc.gov/enforcement/cases-proceedings/google-inc.

As cited earlier, an assessment's failure to include known (or even suspected) material deviations from management assertions can crater the assessment's worthiness.

VI. New FTC Commissioners May Revisit Privacy Assessment Requirements

The FTC will soon have an entirely new slate of commissioners. They may be amenable to a comprehensive overhaul of how the agency monitors its privacy orders.[42] For example, the commissioners could vote to issue a Policy Enforcement Statement, notifying all companies currently required to submit privacy asssessments that future assessments must have certain features or address particular subjects. The commissioners could also instruct staff to re-design the agency's model order language to explicitly require these characteristics in future orders.

More agressively, the Commission could pursue order modification.[43] The agency could also hire a consulting firm to create an auditing protocol applicable to all companies

[42] The prospect of massive civil penalties for administrative order violations is often overblown, and should not be presumed a strong deterrant. In the online context, a $41,484 per violation calculation may seem astronomical, but the statute and interpreting caselaw warrant caution. Under Section 15 U.S. Code § 45(*l*), administrative order violations can result in "no more than" that amount for each violation, with "[e]ach separate violation...[being] a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey [the order], each day of continuance of such failure or neglect shall be deemed a separate offense." If the order violation, for example, is a failure to require a vendor to sign a privacy pledge, that arguably is a single violation. In analyzing order violations, the first step is determining if the matter is a "continuing failure" or a discrete, affirmative violation. Depending on the answer to that question, the second step is counting either days or violations. And the final step is then calculating the suitable money amount for each day/violation. *See U.S. v. Reader's Digest Association, Inc.*, 464 F. Supp. 1037 (D. Del. 1979); *U.S. v. Alpine Indus.,* 352 F.3d 1017 (6th Cir. 2003) (FTC civil penalty calculated on per-day basis). Of note, the Supreme Court has indicated any civil penalty amount may have constitutional implications under the Eighth Amendment, because the civil penalty is paid to the government and determined by a jury. *United States v. Bajakajian*, 524 U.S. 321 (1998). The agency could be entirely precluded from seeking a civil penalty under the logic of *IntelliGender*, although its application to non-restitutionary civil penalties is questionable. *California v. IntelliGender,* 771 F.3d 1169 (9th Cir. 2014) (California Attorney General restitution claims in an unfair competition case precluded by a prior class action settlement on the same claims).

[43] The Commission can re-open proceedings on its own initiative to modify or set aside all or part of its order if it "is of the opinion that changed conditions of law and fact or the public interest" require it. 15 USC §45(b); 16 CFR §2.51(b). Under such circumstances, the Commission issues an order to show cause to all parties subject to the order, stating any proposed changes and the reasons the changes are needed. Each party must respond or object to the changes within 30 days; otherwise, the changes are made effective.

subject to privacy assessments. In 2011, for example, in connection with its plan to monitor healthcare providers' compliance with a new health privacy law (known as HIPAA), the Department of Health and Human Services (HHS) contracted with KPMG to develop audit protocols and assist with the audits.[44] Such a contract would be too expensive for the FTC, but the agency could seek a special appropriation from Congress or request Congressional approval to use civil penalty collections to fund the contract.

Less ground-breaking, FTC could send the company or its assessor an advance letter raising specific concerns or setting concrete expectations for the assessment.[45] In addition to the issues identified in this article, the new commission may find inspiration from the agency's "Start with Security" roadshows, which synthesized 10 principles from the agency's privacy work.[46] Needless to say, the Commission could also pursue

---

Parties themselves may also pursue order modification. The Commission recently approved Sears' petition to expand its order's online tracking provision, but did not require third-party assessments in the original order or its modification. *See* https://www.ftc.gov/news-events/press-releases/2018/02/ftc-approves-sears-holdings-management-corporation-petition.

[44] https://www.foley.com/hhs-initiates-pilot-audit-program-for-hipaa-compliance-11-22-2011/.

[45] The FTC could also send a "retroactive" letter. The legal doctrine of estoppel does not apply to government actions. *See* https://www.fcsl.edu/sites/fcsl.edu/files/ART%206.pdf. However, a five-year statute of limitations does apply to civil penalty actions. *U.S. v. Ancorp Nat. Servs.*, 516 F.2d, 198 (2d Cir. 1975); *see also Kokesh v. SEC*, 2017 WL 2407471 (U.S. Supreme Court, June 5, 2017). It is unclear if the clock starts when the violation occurs or when the agency learns of the violation. Thus, at least as a theoretical matter, the agency's prior acceptance of a company's assessment might not foreclose the Commission pursuing an order violation case less than five years following that assessment.

[46] *See also* the FTC's recent *Upromise* matter, requiring the FTC to pre-approve, not just the assessor, but the assessment's scope and design. https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc. The Start (and Stick) with Security program addressed: (1) start with security; (2) control access to data sensibly; (3) require secure passwords and authentication; (4) store sensitive personal information securely and protect it during transmission; (5) segment your network and monitor who's trying to get in and out; (6) secure remote access to your network; (7) apply sound security practices when developing new products; (8) make sure your service providers implement reasonable security measures; (9) put procedures in place to keep your security current and address vulnerabilities that may arise; and (10) secure paper, physical media, and devices. https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

rulemaking.[47] The agency previously studied the assessors themselves, although to what end is unknown.[48]

The commissioners could also pursue bigger-picture concepts for improving oversight of its privacy orders, described in more detail below.

A. Reconsider Legal Grounds for Redacting Assessments

Historically, the FTC has published compliance reports without any redactions, but published the assessments only in heavily redacted form.[49] The legal grounds for this disparity are unclear, and third parties seeking the assessments have not challenged the redactions in court. Evaluating whether assessment redactions are even permissible requires consideration of multiple statutes and rules. For example, the applicability of confidentiality rules and FOIA exemptions varies depending on whether the assessment is submitted pursuant to an administrative or court order, whether the assessment is characterized as being submitted voluntarily, etc.[50] A full analysis of this issue is beyond the purview of this article. That said, the subject is important enough to warrant brief discussion.

Evaluating whether the FTC is permitted to redact an assessment is not the end of the analysis. Assuming the agency has the authority to redact an assessment, the next question is whether the agency must do so. If not legally required to redact, the FTC should then consider whether the public would benefit from a full review of the

---

[47] The FTC already has a rule prohibiting some ad tracking - 16 CFR 14.12, enacted in 1978. *See* "It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking," by Jeffrey S. Lubbers, George Washington Law Review, Vol. 83, p. 1979, 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560557 (finding materially longer time associated with the FTC's rulemaking under the Magnuson-Moss procedures, compared to rules enacted under the standard Administrative Procedures Act). *See also* "Performance-Based Consumer Law," by Lauren E. Willis, 82 University of Chicago Law Review 1309 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485667.

[48] "FTC to Study Credit Card Industry Data Security Auditing," March 2016, https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing.

[49] Congress can obtain unredacted versions.

[50] Some FTC privacy orders (such as the Facebook order) do not require the company to submit its biennial assessments to the agency. Instead, the agency only requires the company to submit them "upon request." *See* FTC Operating Manual, Chapter 15 (Confidentiality and Access), https://www.ftc.gov/about-ftc/foia/foia-resources/ftc-administrative-staff-manuals.

assessment.[51] It may redound to the FTC's benefit to have public review and input on assessments, especially if the agency does not have sufficient resources or expertise to evaluate whether the assessors followed applicable auditing or technical standards.[52] Publication may also discourage over-reliance on management assertions, because that can negatively impact the auditor's reputation.

The agency should be prepared to counter an assessor's claim that applicable auditing rules require confidentiality of such reports. While an attestation-type audit may be a "restricted use" report, that does not mean the agency cannot distribute it. "Restricted use" merely means the assessor has to state in the report that it is not *intended* for distribution to nonspecified parties; the assessor is not responsible for controlling distribution. Indeed, the pertinent AICPA rule contemplates wide distribution: "In some cases, restricted-use reports filed with regulatory agencies are required to be made available to the public."[53] Similarly, while the contract between the assessor and the company can limit distribution, that contract does not bind the FTC.

B. Have Assessors Report Directly to the FTC

The agency could restructure the privacy orders so the FTC hires (and directs) the assessors, with the subject company order paying for the work. The agency may initially balk at this idea due to the Miscellaneous Receipts Act (MRA). Under the MRA,

---

[51] The assessed companies would no doubt object and could file a court action to prohibit publication. Or perhaps not; *see* FTC disclosure of very specific data security audit materials in document previously filed under seal in the *LifeLock* data security contempt case, https://www.ftc.gov/about-ftc/foia/frequently-requested-records/lifelock (FOIA Number 2016-00462, Final Response to Requester [Jeff Chester]).

[52] The Public Interest Oversight Board (PIOB) oversees IAASB member compliance with its auditing standards. AICPA does not appear to oversee its members' compliance with Professional Attestation Standards (AT Section 101), but the organization is affiliated with The Center for Audit Quality (CAQ). *See* "Comparing Ethics Codes: AICPA and IFAC," Journal of Accountancy, https://www.journalofaccountancy.com/issues/2010/oct/20103002.html. In Nov. 2011, PCAOB published inspection findings for PriceWaterhouseCoopers (the Google/Facebook assessor), listing serious problems with more than a third of the company's financial audits. "Inspectors noted numerous instances of problems with the testing and disclosures related to fair value measurements and hard-to-value financial instruments and with goodwill impairment…[S]ome audit problems [were found] in areas that aren't typically flagged with great frequency in major firm reports, like excessive reliance on management representations, entity-level controls…" (emphasis added), https://pcaobus.org/Inspections/Reports/Documents/2011_PricewaterhouseCoopers_LLP.pdf.

[53] *See* AU Section 532. AUs are the official interpretations of AICPA requirements (similar to the Notes accompanying each Federal Rule of Civil Procedure).

whenever an agency obtains funds other than through a congressional appropriation, the agency must consider whether the MRA applies to those funds. Money can be "received" for MRA purposes either directly or indirectly. However, money is not considered received *for the government* when the agency does not use the money on its own behalf.[54] While an extensive review of the MRA is beyond the ambit of this article, suffice to note the MRA does not apply when an FTC order requires a company to spend money as part of a program designed to prevent future violations or counter the effects of violations. For example, the FTC may use funds from a defendant to accomplish fencing-in or corrective relief, when that is a reasonable remedy for the violation. When such an affirmative remedy is appropriate, but the agency is concerned whether the violator will in fact accomplish the remedy, the MRA does not preclude the violator paying for the FTC or another entity to carry out the remedy.[55]

C. Identify and Support Violation Reporters

Historically, the agency has been loath to identify what sparks its privacy investigations.[56] But for internal purposes at least, the agency should track exactly how it

---

[54] When the Small Business Administration (SBA) was required by statute to perform annual assessments of certain companies, and the SBA required those companies to pay the third-party assessor, the GAO determined that the agency violated the MRA. In contrast, the FTC is not required to conduct assessments. *See* SBA's Imposition of Oversight Review Fees on PLP Lenders, B-300248 (Comp. Gen. Jan. 15, 2004). *See also* http://fcpablog.squarespace.com/blog/2014/10/1/the-much-misunderstood-miscellaneous-receipts-act-part-3.html.

[55] Although the FTC does not hire him directly, the FTC's *Herbalife* order authorizes the agency to terminate the independent compliance auditor and provides a replacement procedure. Notably, the compliance auditor in that case has to obtain advance FTC approval of his planned work and budget. If the FTC objects to the work plan or budget but the auditor does not resolve the matter to the FTC's satisfaction, the order provides a petitioning process to the court.
https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf

[56] ProPublica, for example, was unable to learn what sparked the FTC's investigation into the 2012 Google/Safari matter. *See* https://www.propublica.org/article/announcing-225-million-fine-ftc-says-investigated-googles-internet-tracking. Tracking the investigative spark will likely require corresponding attention to initial investigations and corollary requirements for internal document retention. *See*
https://hoofnagle.berkeley.edu/2016/06/29/70-of-security-investigations-closed/. Doing so may be challenging; some of the FTC's privacy cases aren't even labeled as such. The International Association of Privacy Professionals (IAPP)'s casebook is designed to capture all FTC privacy and data security cases, but it does not (as one example) list *U.S. v. Consumer Portfolio Services,* a 2014 FTC civil penalty case in which the order required a comprehensive "data integrity" program and used the "audit" term.
https://www.ftc.gov/news-events/press-releases/2014/05/auto-lender-will-pay-55-million-

learns of privacy violations, whether from internal forensic research, company whistleblowers, competitive tattletales, advocacy groups, journalists, etc. If, for example, the FTC's privacy cases are often a result of whistleblowers, knowledge of that fact can help the FTC develop best practices to encourage whistleblowers to come forward, either directly to the FTC or to the assessors.[57]

Indeed, the FTC could require assessors to consider credible privacy complaints. Well-informed consumer groups regularly send lengthy and detailed complaints to the FTC; perhaps assessors should be explicitly required to evaluate their merits (in addition to the FTC's evaluation).

In addition, given consumer groups' technical and time investment in drafting these complaints – particularly if the FTC's internal review identifies them as a frequent source of its cases – the agency could consider a order provision requiring the company to "promptly and thoroughly investigate any complaint received by [company] relating to compliance with this Order and to notify the complainant of the resolution of the complaint and the reason therefor," as the Commission required in the *Herbalife* multi-level marketing order.[58]

D. Create Positive Incentives for Subject Companies to Report Violations Independently of Assessments

Audit experts often point to an effective compliance program model developed by the U.S. Sentencing Commission.[59] The key attribute is an incentive to self-report violations. Currently, a company under FTC order has no incentive to report deficiencies in its privacy program. In fact, because data misuse (unlike data breaches) is often never discovered, a company actually has a disincentive to report problems. Rather than relying on an assessor's sleuthing abilities or a company's good faith, the FTC may be

---

settle-ftc-charges-it-harassed. Another complication may be that the FTC's records disposition requirements have not been updated since 2009. *See* National Archive and Records Administration (NARA) document N1-122-09-1, https://www.archives.gov/files/records-mgmt/rcs/schedules/independent-agencies/rg-0122/n1-122-09-001_sf115.pdf.

[57] "Ex-Facebook insider says covert data harvesting was routine," The Guardian (March 20, 2018) (describing his unsuccessful efforts in 2011 and 2012 to persuade senior Facebook executives to exercise contractual audit provisions on external developers siphoning consumer data, and his decision to denounce the company in a 2017 New York Times op-ed), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[58] https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf.

[59] *See,* e.g., http://www.acc.com/legalresources/quickcounsel/eaecp.cfm.

well served by developing a program similar to that used by the U.S. Sentencing Commission.

"[W]hen the [U.S. Sentencing] Commission promulgated the organizational guidelines, it attempted to alleviate the harshest aspects by incorporating the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range if an organization can demonstrate that it had put in place an effective compliance program. This mitigating credit under the guidelines is contingent on prompt reporting to the authorities and the non-involvement of high-level personnel in the actual offense."[60] Other attributes of the mitigation program include:

- Oversight by high-level personnel
- Due care in delegating substantial discretionary authority
- Effective communication to all levels of employees
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal
- Consistent enforcement of compliance standards including disciplinary mechanisms
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation

Devising a similar program at the FTC might not require legislative changes or rule-making.[61] In fact, the FTC has created safe harbors in other contexts, simply by issuing a Policy Enforcement Statement or including such a provision in a consent order.[62]

---

[60] https://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf.

[61] *See,* e.g., FTC's Civil Penalty Leniency Program for Small Entities, https://www.ftc.gov/policy/federal-register-notices/notice-regarding-compliance-assistance-and-civil-penalty-leniency. *See also* the FTC's Funeral Rule Offender's Program (FROP). In conjunction with the National Funeral Directors Association (NFDA), the FTC created an industry self-certification and training program to increase Funeral Rule compliance. FROP offers a non-litigation alternative for correcting apparent "core" violations of the Funeral Rule. Violators may, at the Commission's discretion, be offered the choice of a conventional investigation and potential law enforcement action (resulting in a federal court order and civil penalties) or participation in FROP. Violators choosing to enroll in FROP make voluntary payments to the U.S. Treasury or state Attorney General, but those payments are usually less than what the Commission would seek as a civil penalty. NFDA attorneys then review the funeral home's practices, bring them into compliance with the Funeral Rule, and then conduct on-site training and testing. https://www.ftc.gov/reports/staff-summary-federal-trade-commission-activities-affecting-older-americans-during-1995-1996.

[62] For example, the FTC laid out its requirements for Section 5's "unfairness" grounds in its 1980 Policy Statement, https://www.ftc.gov/public-statements/1980/12/ftc-policy-

Alternatively, the FTC could more affirmatively inject a mitigation process into a company's privacy program. The Consumer Financial Protection Board (CFPB)'s 2016 data security order could provide a model. In addition to requiring a third-party audit (using the term "audit"), the order incorporates the common-sense realization that a robust audit is likely to identify some deficiencies at every company. With this in mind, the order lays out a process for the company to create a post-audit mitigation plan, which the company submits to the CFPB for approval along with the audit report.[63]

E. Require Board of Director Responsibility for Assessments

The FTC could require a company's board of directors to bear ultimate responsibility for order compliance. For example, the FTC could require a company's board of directors to review the third-party assessment and create a compliance plan.[64] Another model could be the 2002 Sarbanes-Oxley Act, which mandated certain corporate processes to ensure accurate financial reports, with extensive corporate board responsibilities for certifying those reports.[65]

---

statement-unfairness. The FTC has also rescinded its policy statements, as shown by the 2012 withdrawal of the agency's Policy Statement on Monetary Remedies in Competition Cases, https://www.ftc.gov/news-events/press-releases/2012/07/ftc-withdraws-agencys-policy-statement-monetary-remedies. *See also U.S. v. Civil Development Group*, (2010 FTC civil penalty case) (from the Statement of Chairman Robert Pitofsky and Commissioner Sheila F. Anthony: "Part V of the Order provides respondents with a limited rebuttable presumption that they have exercised good faith in complying with key injunctive provisions of the Order, if respondents show, by a preponderance of the evidence, that they have established and maintained the education and compliance program mandated by Part IV.") https://www.ftc.gov/enforcement/cases-proceedings/civic-development-group-llc-scott-pasch-david-keezer-united-states.

[63] *In Re Dwolla*, https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/. Although not a privacy case, the FTC incorporated a corrective action concept with the independent compliance audit required in the *Herbalife* order, https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf.

[64] *In Re Dwolla*, CFPB's 2016 data security order, contains this requirement. https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[65] *See* https://en.wikipedia.org/wiki/ Sarbanes–Oxley_Act.

F. Clarify that Merely Obtaining an Assessment Is Not a Safe Harbor

After receiving an assessor's certification in conformance with an FTC order, a company could argue the FTC is precluded from contesting it.[66] But, while an assessor may determine that a certain issue is not a "material deficiency," the FTC may not agree. To avoid confusion and a company's unwarranted reliance on an assessment, the FTC could preemptively foreclose this issue. The FTC could also clarify whether a company can be in compliance with an order but still subject to a Section 5 case alleging violations of overlapping subject matter.

G. Fully Evaluate Privacy Order Provisions, including Assessments

The agency may benefit from a full cross-divisional review of its privacy order provisions, especially including the assessment provision.[67] Such self-reflection and critical analysis at the FTC is not unprecedented. On the competition side, the Commission was recently lauded, domestically and internationally, for its two-year evaluation of its merger remedies, identifying areas of both strengths and weaknesses.[68] However, the agency's Office of Inspector General reviewed the Bureau of Consumer

---

[66] *United States v. Am. Hosp. Supply Corp.*, 1987 WL 12205 (N.D. Ill. 1987) (defendant's notice to the FTC that it had acquired companies making prohibited products was not "exculpatory" but was considered "in mitigation" of the penalty). *But see* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.* (FTC should not fault a company's data security if a third-party assessor approved it), https://www.ftc.gov/public-statements/2015/12/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v.

[67] Former Republican FTC Commissioner William Kovacic recently advocated a review of the agency's privacy compliance monitoring. "What kind of oversight did [the FTC] exercise? You have to look at that because that was a big part of your compliance mechanism. If that failed, then you have to rethink what you are doing." An FTC spokesman responded, "[T]he commission believes the privacy audits that undergird FTC consent decrees work." https://www.nationaljournal.com/s/665918/can-ftc-handle-facebooks-digital-privacy-challenge. *See also* privacy advocates' February 2017 letter to FTC commissioners, https://consumerfed.org/wp-content/uploads/2017/02/2-15-17-FTC_Letter.pdf.

[68] The 2017 Merger Remedies Taskforce reviewed Commission merger orders from 2006 through 2012, evaluating 89 merger orders affecting 400 markets, with 79 divestitures to 121 buyers. The Taskforce evaluated 50 of those orders using a case study method, interviewing and collecting data from nearly 200 businesses in a wide range of industries. The Taskforce Report included a list of improvements, and implemented them, specifically by updating the agency's Statement for Negotiating Merger Remedies. https://www.ftc.gov/news-events/blogs/competition-matters/2017/02/looking-back-again-ftc-merger-remedies.

Protection's resource allocation and achievement of mission objectives in 2015 and did not identify any issues associated with its oversight of the privacy orders.[69]

VII. Conclusion

The FTC is critically important to ensuring privacy protections for the public. To fulfill this mission, however, the agency should re-evaluate its orders' assessment provision, and ensure it is a robust compliance mechanism. Failure to do so could have unintended consequences for all consumers.

[69] https://www.ftc.gov/system/files/documents/reports/evaluation-ftc-bureau-consumer-protection-resources/2015evaluationftcbcpreport.pdf. *See also* FTC's Office of Policy Planning, "Post-Purchase Consumer Remedies: briefing book for policy review session," (1980), https://catalog.hathitrust.org/Record/000100549.

From: Nicole Day [redacted]
Sent: Wednesday, February 15, 2023 12:37 PM
To: Regulations
Subject: Comments re Service Provider/Contractor Contract Requirements in Proposed Regs

Hello,

In reviewing the newly proposed CCPA regulations, I'm quite confused by the need to include both of the following in § 7051(a):

> (3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any purpose other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.
>
> (4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations.

These are duplicative - "any commercial purpose other than the enumerated Business Purposes specified in the contract" (subsection (4)) would fall under "any purpose other than the Business Purpose(s) in the specified contract" (subsection (3)). If you really think there's a need to include a specific reference to the "commercial purposes" term from the CCPA (spoiler alert: there isn't), just say:

> "Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any purpose, *including any commercial purpose*, other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations."

Nit: capitalization is all over the place in and a bunch of CCPA section references are wrong in these proposed regs. Yikes.

From: Sidney Hoff [redacted]
Sent: Thursday, February 16, 2023 2:55 PM
To: Regulations
Subject: American Express - Comments on ADM Rulemaking (PR 02-2023)
Attachments: AmEx Letter to CPPA re ADM Rulemaking (2.8.23).pdf

American Express submits the following comments for your consideration as you consider developing rules on automated decision making.

Thank you,

[redacted]
RESOLUTE Company, Executive Assistant
[redacted]
1215 K Street
Suite 1100
Sacramento, CA 95814
http://www.resolutecompany.com

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, California 95834
regulations@cppa.ca.gov

February 8, 2023

Re: Automated decision-making and rulemaking

To Ashkan Soltani, Philip Laird, Lydia de la Torre, and Vinhcent Lee:

American Express Company ("AmEx") submits this letter in connection with a provision of the California Privacy Rights Act ("CPRA") that directs the California Privacy Protection Agency ("Agency") to "solicit broad public participation" in issuing "regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology."[1]

Businesses have long used technologies that could be classified as "automation" for important business purposes that serve consumers, including to enhance operational efficiencies (and thereby lower costs, reduce delays, and deliver other benefits for consumers) and that address various compliance challenges, including to detect suspicious transactions and combat unlawful activity.[2] As described below, these technologies serve public policy goals in the financial services industry, in particular, and are leveraged to address compliance challenges faced by banks and other financial institutions.

As the Agency commences its effort to consider possible regulations in this area, AmEx submits this letter to describe these uses of automation and explain important legal questions that the Agency should consider at the outset of the rulemaking process, including potential conflict of law issues. As the framers of the CPRA anticipated by subjecting this topic to a rulemaking proceeding, the regulation of automated decision-making (or "ADM") raises difficult and complex questions. We request that the Agency give due consideration to the legal points raised in this letter, including, most notably, a recommendation that the Agency exempt the financial services industry from ADM rules to avoid any ambiguity about their application to the industry, as these technologies play an important role within the financial services industry to protect consumers and facilitate compliance with existing legal requirements. This is important to avoid putting financial institutions in a position where they are asked to implement processes that could create legal jeopardy under federal laws.

---

[1] *See* Cal. Civ. Code § 1798.185(a), (a)(16). The CPRA amended the California Consumer Privacy Act ("CCPA").

[2] Though these automation technologies may fall outside the scope of the type of "profiling" that the Agency has the authority to regulate, we describe them here to provide the Agency with context in its rulemaking. *See* Cal. Civ. Code § 1798.140(z).

1. **Financial institutions have long used automation to address financial crimes compliance requirements, information security requirements, and other purposes that are consistent with public policy.**

The financial services industry is governed by a complex legal framework consisting of federal and state laws and regulations and extensive supervisory guidance from the industry's regulators. This legal framework is designed to ensure financial institutions operate in a safe and sound manner and protect consumers. Banks are regularly examined for compliance with these laws, regulations, and guidance by federal and state agencies, including the federal banking agencies (Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency). These agencies are authorized to issue cease and desist orders, impose civil monetary penalties, and take other enforcement actions against banks that violate laws and regulations or operate in unsafe or unsound condition.[3]

An important component of this framework protects the financial system and broader economy from bad actors engaged in various financial crimes, such as money laundering, fraud, bribery, and terrorist financing. Financial crimes compliance laws include the Bank Secrecy Act of 1970 and its implementing regulations, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Title III of the USA PATRIOT Act), Trading With the Enemy Act ("TWEA"), International Emergency Economic Powers Act ("IEEPA"), and various provisions of the federal criminal code.[4] These laws are administered and implemented by federal agencies such as the U.S. Securities and Exchange Commission, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and Financial Crimes Enforcement Network ("FinCEN"), and the U.S. Department of Justice.[5]

Against this framework, banks use automation to implement operational processes to comply with financial crimes requirements:

- **Prevention of money laundering and terrorist financing.** Given the significant number of transactions processed by AmEx and other financial institutions and the increase in electronic banking and payments, automated systems have long been a necessity to prevent banks from being used as a vehicle for money laundering and terrorist financing. For instance, in order to detect and report suspicious activity that may

---

[3] *See* 12 U.S.C. § 1818(b), (i).

[4] *See* 31 USC § 5311 *et seq.*; 12 U.S.C. § 95 and 50 U.S.C. § 4301 *et seq.*; 50 U.S.C. § 1701; 18 U.S.C. §§ 1956–1957.

[5] *See* Dep't of Treasury, Press Release, *Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.* (Oct. 11, 2022), https://home.treasury.gov/news/press-releases/jy1006; SEC, Press Release, *SEC Charges Wells Fargo Advisors With Anti-Money Laundering Related Violations* (May 20, 2022), https://www.sec.gov/news/press-release/2022-85; Dep't of Justice, Press Release, *Banker Pleads Guilty to Bank Secrecy Act Charges* (Sept. 13, 2022), https://www.justice.gov/opa/pr/banker-pleads-guilty-bank-secrecy-act-charges.

be predicate offenses to money laundering and terrorist financing, banks design and implement anti-money laundering ("AML") compliance programs that, among other things, enable banks to identify and report suspicious activities to regulators.[6] Automation technologies are relied upon heavily by the financial services industry to analyze voluminous datasets consisting of transaction and customer data. If the industry were unable to use such technologies, the industry would be unable to keep pace with criminals that are leveraging these very same technologies to launder money through the U.S. financial system or to finance terrorism. For that reason, regulators in the financial services industry have encouraged banks to continue innovating and deploying automation to meet their legal obligations.[7]

- **Compliance with economic sanctions**. U.S. economic sanctions administered under TWEA and IEEPA prohibit U.S. persons from doing business with certain sanctioned parties, such as the individuals and organizations identified on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List").[8] The financial services industry plays an important role in making sure that these sanctioned parties are not able to access U.S. financial products and services, so screening potential customers against the SDN List and other watch lists is a key component of financial crimes compliance. Given the sheer volume of entries on the SDN List and number of customers seeking bank accounts and other financial products from financial institutions, automation technologies are used extensively to determine whether customers and counterparties are "hits" on these watch lists. Any limitation on the industry's ability to use automation technologies would present substantial challenges for the industry to comply with economic sanctions requirements.

- **Fraud prevention.** There are nearly 200 billion non-cash payment card transactions each year in the U.S.[9] The ease and efficacy of payment card transaction processing relies on automation to complete payment card transactions in a way that limits fraud risks to cardholders, merchants, and financial institutions, and to complete chargebacks when cardholders challenge transactions. This is not a new development, as modern payment card systems have existed for decades, powered by automated processes that

---

[6] *See* FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL (2014), https://bsaaml.ffiec.gov/docs/manual/BSA_AML_Man_2014_v2_CDDBO.pdf.

[7] *See* BD. OF GOVERNORS OF THE FED. RESERVE SYSTEM ET AL., JOINT STATEMENT ON INNOVATIVE EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING (2018), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf.

[8] *See, e.g.*, OFAC, *Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists* (last updated Jan. 6, 2023), https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

[9] *See* Bd. of Governors of the Fed. Reserve System, *The 2019 Federal Reserve Payments Study* (last updated Jan. 6, 2020), https://www.federalreserve.gov/paymentsystems/2019-December-The-Federal-Reserve-Payments-Study.htm.

transfer information among various financial institutions in order to process the payments that consumers authorize to pay for groceries, childcare, and bills. Many core banking systems and applications use programmed searches and surveillance systems to identify payment transactions that are related, involve known or suspected bad actors, make use of fraudulent payment instruments, or exceed certain thresholds.

- **Detect and prevent identify theft**. Financial institutions are required to have identity theft prevention programs under the amendments to the Fair Credit Reporting Act.[10] These programs must identify red flags for potential identity theft and include protocols for addressing and remediating identity theft.[11] An identity theft prevention program requires sophisticated surveillance and intervention tools that rely on automated technologies to process and analyze datasets in an expeditious manner.

Financial crimes compliance and information security functions depend on automated technologies in order to obtain and analyze significant volumes of data and to produce actionable insights used for reports to the government and to protect customer funds. Of course, banks have many more needs and uses for automated technologies than just these areas, as automated technologies have the potential to produce operational efficiencies and cost savings in many different areas of the bank. For example, automated technologies can be used for processing ACH transactions with greater accuracy and speed. These technologies also can be used for evaluating applications for credit and other banking products and services. Further, the federal banking agencies are exploring the extent to which artificial intelligence is being used in other areas within the industry, such as for cybersecurity purposes.[12]

For all of the various uses described in this section, banks are subject to existing laws, regulations, and guidance that impose limitations on their uses of automated technologies, and federal banking agencies examine these uses to ensure the technologies are being deployed in a safe and sound manner and in compliance with applicable laws and regulations. These existing laws, regulations, and guidance include:

- **Credit underwriting.** The Equal Credit Opportunity Act and its implementing regulation, Regulation B, prohibit unlawful discrimination against members of a protected class in any aspect of a credit transaction.[13] Accordingly, an automated technology that results in discrimination against a protected class such as members of a racial group or age group generally would be illegal.

---

[10] *See, e.g.*, 12 C.F.R. Part 41, Subpart J (Red Flags Rule).

[11] *Id.*

[12] *See* Dep't of Treasury et al., Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning, 86 Fed. Reg. 16837 (March 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

[13] *See* 15 U.S.C. § 1691 *et seq*.

- **Consumer disclosures and harm.** The Dodd-Frank Act and Consumer Financial Protection Bureau ("CFPB") regulations prohibit banks from engaging in unfair, deceptive, or abusive acts or practices ("UDAAP").[14] Prohibited UDAAP could include, for example, making false representations to customers about the use of automated technologies in processing customer data or deploying automated technologies in such a way as to harm customers. Similarly, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits banks from engaging in "unfair or deceptive acts or practices."[15]

- **Model risk management.** Banks are required to comply with regulatory requirements governing their use of models, including initial analyses of model suitability and model testing and validation.[16] Consequently, models that underlie automated technologies are required to be analyzed for compliance with these requirements.

- **Safeguarding information**. The Gramm-Leach-Bliley Act ("GLBA") requires financial institutions to protect the privacy and security of customers' personally identifiable financial information, and these GLBA provisions have been implemented by the federal banking agencies and agencies in the Interagency Guidance Establishing Information Security Standards.[17] In addition, banks are required to comply with federal banking agency guidance pertaining to information technology, including cybersecurity controls.[18]

- **Safety and soundness.** Banks may be subject to enforcement actions such as cease and desist orders, civil monetary penalties, and orders removing individual directors, officers, and employees from their positions if they operate in an unsafe or unsound manner.[19] The requirement that banks must operate in a safe and sound manner confers significant discretion on federal and state bank regulators to determine whether a particular action or inaction is inconsistent with safety and soundness and therefore should be the basis for supervisory criticism or enforcement action. The safety and soundness requirement is the legal foundation for much of the supervisory guidance issued for banks, and it provides a broad lens through which regulators will scrutinize automated technologies and their effects on the bank and its customers.

---

[14] 12 U.S.C. § 5531.

[15] 15 U.S.C. § 45(b).

[16] *See* BD. OF GOVERNORS OF THE FED. RESERVE, SUPERVISORY GUIDANCE ON MODEL RISK MGMT., SR 11-7 (2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf.

[17] *See* 15 U.S.C. § 6801 *et seq*.; *Interagency Guidelines Establishing Information Security Standards*, 12 CFR 30, Appendix B (OCC); 12 CFR 208, Appendix D-2 and 225, Appendix F (FRB); 12 CFR 364, Appendix B (FDIC); and 12 CFR 748, Appendix A (NCUA).

[18] *See* FFIEC, *Information Security*, INFORMATION TECHNOLOGY EXAMINATION HANDBOOK, https://ithandbook.ffiec.gov/laws,-regulations,-guidance/information-security.aspx.

[19] 12 U.S.C. § 1818.

In summary, the financial services industry makes use of automated technologies for important financial crimes compliance and cybersecurity reasons, and imposing limitations on such uses poses risk to the financial system and to customers. Moreover, the industry is subject to a number of existing laws and regulations that impose restrictions on these technologies and serve to mitigate risks of consumer harm.

2. The regulation of automation by financial institutions should be left to financial services regulators, thereby avoiding conflict of law questions and other disruption to regulators' oversight of the financial services industry.

The Agency should not impose additional layers of state requirements in an area that is already subject to extensive regulation, as is the case for financial institutions' use of automation. Exempting highly regulated industries—such as financial institutions—from any new opt-out requirements is consistent with the design of the CCPA framework, serves important public policy goals, and avoids potential conflict of law questions.

The CPRA already contains an express exception for information subject to the GLBA.[20] Moreover, the statutory text plainly provides that "the obligations imposed on businesses . . . shall not restrict a business's ability to . . . comply with federal, state, or local laws."[21] Thus, the statutory design plainly sought to avoid interference with areas that are subject to extensive federal regulation, such as financial services.

Consistent with this statutory design, the proposed rules should avoid introducing any ambiguity about whether financial institutions and other businesses are required to afford opt-out rights to consumers for systems engaged in fraud prevention, information security, and other regulated activities that are supported by automation (often, as noted above, with the encouragement of financial services regulators). It would defy common sense to provide fraudsters and money launderers with opportunities to submit requests to opt-out of ADM processing (or gain access to ADM processing logic), even outside the context of GLBA, which applies to financial products provided for personal, family, and household purposes.[22] Indeed, an imprudently broad opt-out framework would reduce the security of day-to-day payment card transactions and render banks more vulnerable to cybersecurity threat actors, thus subjecting consumers' funds to greater risks of compromise; it would reduce banks' ability to protect the financial systems from being used by bad actors, as well as impede consumers with small businesses from getting loans they need; and it could harm consumers and small businesses who rely on timely payments and deposits.

A contrary result also would invite potential conflicts of law questions that could undermine the new regulatory framework. Longstanding federal constitutional principles

---

[20] Cal. Civ. Code § 1798.145(e).

[21] *Id.* § 1798.145(a), (a)(1).

[22] *See* 12 C.F.R. § 1016.3(e).

preclude the adoption of rules that interfere with federal obligations.[23] Moreover, California law is clear that regulations are not enforceable unless "consistent and not in conflict with the statute."[24] As noted above, the CPRA expressly provides that "obligations imposed on businesses" under the CPRA should not "restrict a business's ability . . . to comply with federal, state or local laws."[25] Yet such conflict and/or restrictions may arise if the Agency were to adopt opt-out requirements that purport to regulate (or create ambiguity with respect to the regulation of) the use of automation by financial institutions in ways that have implications for fraud screening and other compliance processes, the safety and soundness of institutions, and the integrity of the financial system. This threatens to create legal jeopardy for institutions asked to honor opt-out and access requests that could result in exposure under existing federal law (*e.g.*, claims that manual processing of credit card transactions, which is effectively not feasible, constitutes an unfair act or practice under Section 5 of the FTC Act). Further, a lack of clear exemptions risks placing financial institutions in the exact position Agency rulemaking is meant to avoid—without "clear guidance about their responsibilities and rights."[26]

While the Agency does not have the authority to create opt-out rights that interfere with or otherwise restrict a business's ability to comply with requirements imposed under other federal and state legal frameworks, it has authority to narrowly tailor regulations to "make specific" the circumstances in which opt-out rights should be afforded.[27] The statutory design of the CPRA and the California Administrative Procedure Act invites the Agency to limit the scope of any new requirements with respect to ADM technologies to avoid creating conflict of law concerns and detrimental policy consequences.[28]

* * *

AmEx is supportive of appropriate and thoughtful regulation of ADM by the Agency. We hope that this letter helps the Agency focus any future rulemaking related to ADM technologies on areas where the Agency can best protect consumers' rights and strengthen consumer privacy, consistent with the statutory design.[29] While we have focused this letter on

---

[23] *See* U.S. Const. art. VI, cl. 2; *see also Gade v. Nat'l Solid Wastes Mgmt. Assn.*, 505 U.S. 88, 98 (1992) (discussing a long line of federal pre-emption case law).

[24] California Administrative Procedure Act, Cal. Gov't Code § 11342.2.

[25] Cal. Civ. Code § 1798.145(a), (a)(1).

[26] Cal. Privacy Rights Act § 3(C)(2).

[27] *See* Cal. Gov't Code §11342.600 ("'Regulation' means every rule, regulation, order, or standard of general application or the amendment, supplement, or revision of any rule, regulation, order, or standard adopted by any state agency *to implement, interpret, or make specific the law enforced or administered by it*, or to govern its procedure.") (emphasis added).

[28] Cal. Civ. Code § 1798.145(a), (a)(1); *see also* Cal. Gov't Code §11342.600.

[29] *See e.g.,* Cal. Privacy Rights Act § 3 ("In enacting this Act, it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional (continued…)

legal considerations and conflict of law issues, AmEx also encourages the Agency to ensure that any new rights with respect to ADM technologies are interoperable with those adopted in other jurisdictions, which focus on decision-making that lacks the involvement of a human decision-maker and has legal or similarly significant consequences for consumers.[30]

In summary, AmEx encourages the Agency to exclude the financial services industry from future ADM rules. AmEx is in an industry where there are important uses of automation in furtherance of complex federal and state regulatory requirements. As discussed above, automation is a critical tool used to prevent money laundering and terrorist financing, combat fraud, prevent cybercrime, and support banks' ongoing safety and soundness. A rule inhibiting these systems or introducing ambiguity as to when these activities are permitted not only runs contrary to the consumer protective purposes of the CPRA, but also runs contrary to a rulemaking process intended to clarify businesses' responsibilities under the CPRA.

---

right of privacy"); *id.* § 3(C)(4) ("The law should adjust to technological changes, help consumers exercise their rights, and assist businesses with compliance, with the continuing goal of strengthening consumer privacy.").

[30] For example, the Connecticut privacy statute grants consumers a right to opt-out of certain profiling activities in furtherance of "*solely* automated decision-making" that produce "legal or similarly significant effects." An Act Concerning Personal Data Privacy And Online Monitoring, 2022 Conn. Legis. Serv. 22-15 § 4(a)(5)(C) (emphasis added). The Colorado and Virginia privacy statutes similarly grant consumers a right to opt-out of "profiling in furtherance of decisions that produce legal or similarly significant effects" concerning a consumer. Colorado Privacy Act, 2021 Regular Session, 21-190 § 6-1-1306(1)(a)(I)(C); Va. Code Ann. § 59.1-577(A)(5).

From: David Swetnam-Burland [redacted]
Sent: Friday, March 17, 2023 11:49 AM
To: Regulations
Cc: Stacy O. Stitham; Nathaniel A. Bessey
Subject: Preliminary Comments on Proposed Rulemaking, PR 02–2023
Attachments: 2023-03-17 BI CPPA Rulemaking Comments.PDF

Dear Mr. Sabo and the California Privacy Protection Agency:

Please see the attached preliminary comments on proposed rulemaking, PR 02-2023, submitted on behalf of my colleagues, Stacy O. Stitham, Nathaniel A. Bessey, and me.

Thank you for the opportunity to participate in the rulemaking process.

All the best,

David Swetnam–Burland | BRANN & ISAACSON
Dir: [redacted] | Office: 207.786.3566 | [redacted]

BRANN & ISAACSON
ATTORNEYS AND COUNSELORS AT LAW

DAVID SWETNAM-BURLAND | Partner
STACY O. STITHAM | Partner
NATHANIEL A. BESSEY | Partner

March 17, 2023

By Email

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, California 95834

Re: Preliminary Comments on Proposed Rulemaking, PR 02–2023

Dear Mr. Sabo:

We thank the California Privacy Protection Agency for the opportunity to comment on the proposed rulemaking relating to cybersecurity audits and risk assessments.

We are counsel to the online and multichannel commerce industry, representing over 100 such companies on issues that affect the industry, including privacy and data security. While we offer these comments on our own behalf, not on behalf of any particular client, they are informed by our years of experience representing e-commerce companies of all sizes and their service providers.

Our message is simple: prioritize uniformity. We urge the CPPA to draft regulations relating to cybersecurity audits and risk assessments consistent with requirements regulated businesses already face or will soon face. The best way to ensure that consumers' personal information is collected, maintained, and used in a secure manner, consistent with their choices and expectations—the common goal of individuals, businesses, and regulators—is a clear, uniform standard. The goal of consumer privacy is best served when businesses can devote their efforts to compliance, rather than worrying about whether some fine point of California law requires them to redo or revamp a risk assessment already required by contract or the law of another state (such as Colorado, Virginia, or Connecticut).

The e-commerce industry. Revenue from retail e-commerce in the United States was estimated at roughly 905 billion U.S. dollars in 2022. In overwhelming numbers, America's consumers purchase goods and services via the Internet, and in

doing so, routinely provide their personal information for the fulfillment of those purchases and the marketing of additional offers. Protection of that personal information is an issue of great importance for the business community; however, without a single federal standard governing privacy and data security, the industry—largely made up of small to mid-sized businesses—must attempt to reconcile a burgeoning number of different state approaches to the regulation of that information.

While this attempt to achieve regulatory compliance in numerous jurisdictions may not pose a substantial problem to large retailers with dedicated in-house counsel, it can be a significant struggle for smaller online shops without an in-house legal and compliance team. While the smallest companies may be exempt, a retailer need not be Walmart or Amazon to rack up a sufficient quantity of website visitors to come within the scope of the CPPA's asserted jurisdiction.

Uniformity promotes privacy and data security. We urge the CPPA to hew to existing content requirements, such as those recently laid out in regulations for data protection assessments under the Colorado Privacy Act. *See*, *e.g.*, Colo. Dep't of Law, 4 CCR 904-3, part 8 (available at https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf). Like the Colorado Privacy Act, California's statutory requirements focus on identifying and weighing the benefits and risks to all stakeholders of using certain personal information. With Colorado, Virginia, and Connecticut all requiring a similar analysis, online retailers would greatly benefit from the ability to conduct uniform assessments, where required, to evaluate the pros and cons of data usage, rather than conducting separate analyses based on the competing requirements of different states. Consumers would benefit likewise because the retailer's focus would be on the proper treatment of their personal information rather than textual differences between competing regulations of different jurisdictions.

Retailers are not tech companies. In protecting California consumers, California privacy law does not distinguish between retail businesses whose focus is selling goods and tech companies whose focus is gathering, bundling, and selling personal information. The uniform treatment of all "businesses" creates certain inequities when language aimed at curbing potentially abusive practices by social media or search engine giants is imposed on much smaller retail businesses. The CPPA has an opportunity to prevent, or at least minimize, further inequity through this rulemaking process.

First, we ask that the CPPA define "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" so as to exclude all but the largest e-commerce retailers from the requirement of a California-specific cybersecurity audit or risk assessment. The statute identifies the size and complexity of a business and the nature and scope of its processing activities as relevant factors in drafting appropriate regulations. The CPPA can minimize the burdens on retail businesses, as well as the downstream costs to customers, if it tailors requirements so that the burden of compliance is commensurate with the risk. Typical online retailers, who generally collect and use a small set of voluntarily provided personal information, should not be subjected to requirements designed for large platforms or data brokers.

Second, we suggest that the CPPA raise the threshold for compliance with the risk assessment requirement. Bearing in mind the smaller size and lesser complexity of retail businesses, we suggest that, when it comes to the basic business of e-commerce, online sales, the CPPA raise the threshold for risk assessment compliance to entities with the personal information of 200,000 or more California consumers and households.

Third, and finally, we suggest that risk assessments for online retailers be limited to the processing of *sensitive* personal information. The CPPA need not and should not reinvent the wheel by creating different and cumulative security audit requirements where adequate safeguards already exist. In the e-commerce sector, most of the personal information collected and used relates to the sale of goods: name, address, order histories, *etc*. The sensitive data customers typically provide online retailers is payment information needed to complete a purchase. Contracts with payment processors already require merchants to adhere to the Payment Card Industry's Data Security Standard (PCI-DSS), a well-established industry standard. It makes little sense to ask retail businesses to perform broad risk assessments relating to information everyone understands must be provided to complete a retail transaction. By limiting the scope of online retailer risk assessments to *sensitive* personal information, the CPPA can keep the regulatory focus where it should be—on information the use of which is of special concern to consumers.

If adopted, these measures will allow businesses in the e-commerce industry that are large enough to fall within the scope of the statute, but not so large as to have vast resources for in-house privacy compliance, to devote their time to the protection of the types of personal information that warrant the highest level of care.

Thank you again for the opportunity to participate in the rulemaking process.

Very truly yours,

BRANN & ISAACSON

/s/ David Swetnam-Burland
David Swetnam-Burland

/s/ Stacy O. Stitham
Stacy O. Stitham

/s/ Nathaniel A. Bessey
Nathaniel A. Bessey

From: ed howard [redacted]
Sent: Sunday, March 26, 2023 6:00 PM
To: Regulations
Subject: Children's Advocacy Institute testimony and exhibit re. PR 02-2023
Attachments: PRIVACY AGENCY COMMENTS.docx; FB child trafficking complaint.docx

Mr. Sabo, please find attached testimony and an exhibit re. PR-02-2023.

Thank you, in advance, for your consideration.

Best,

Ed Howard
[redacted]

Children's Advocacy Institute

University of San Diego
SCHOOL OF LAW

University of San Diego School of Law
5998 Alcalá Park / San Diego, CA 92110
(619) 260-4806 / (619) 260-4753 (Fax)

2751 Kroy Way
Sacramento, CA 95817 / (916) 844-5646

727 15th Street, NW, 12th Floor
Washington, DC 20005 / (917) 371-5191

Reply to: □ San Diego □ Sacramento □ Washington
info@caichildlaw org / www.caichildlaw.org

March 26, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834
Submitted via email at: regulations@cppa.ca.gov.

RE: PR 02-2023

Dear Mr. Sabo:

The Children's Advocacy Institute at the University of San Diego School of Law (CAI) which for over 30 years has been working to advance the health and well-being of children through research, teaching, legislative and regulatory advocacy, and litigation, respectfully submits these comments related to automated decisionmaking, social media platforms, and children, answering certain of the Agency's questions and urging a regulatory approach to "access and opt-out rights" (Civil Code section 1798.185(a)(16)) for social media platforms and children that maximize child safety by ensuring that the profit-driven zeal of social media platforms for "user engagement" is tempered by child safety.

QUESTION 1: How id "automated decisionmaking" defined?

How AI-driven Social Media Recommendation Machines Work: An Overview.

Automated decisionmaking is at the very heart of how social media platforms operate and, as will be shown, such automation is significantly responsible for the worst child mental health crisis the nation has ever experienced.

Algorithms like recommendation algorithms take inputs -- data falling within identified categories -- and process those inputs following a set of rules. This algorithmic process results in an output:

in YouTube's , TikTok's and Facebook's case, the correspondence between someone visiting YouTube and the chosen set of recommended videos presented and not presented to the user.

AI is a set of technologies that autonomously re-write complex and powerful algorithms such as the YouTube recommendation algorithm. AI machine learning is tasked with writing the recommendation algorithm that matches an individual from among its 2.6 billion users to content drawn from (for example) YouTube's inventory of 800 million videos. Initially the machine is trained to successfully associate past viewing data in various combinations with videos that satisfy users. Where promoted content is viewed, the algorithm is confirmed. Where promoted videos are ignored or rejected by the viewer, the AI itself adjusts the algorithm, seeking to a more successful subsequent engagement. The AI recommendation algorithm is constantly improving by checking its predictions against the subsequent behavior of the viewer. Google rightly describes its recommendation system as "constantly evolving, learning every day from over 80 billion pieces of information [it] calls signals."

These "signals" or "labels" the AI places on data are derived from a platform's vast reservoir of personal behavioral data derived from its many product offerings. The tags or labels that the AI assigns to its data and relationships between data permit a platform's algorithm to locate and retrieve the videos most likely to achieve the goal preprogrammed into the algorithm.

Some "signaled" or "labeled" data will serve to identify the particular user, such as a user's age, gender, address, and type of device. Some will be used to capture a user's prior history with YouTube, such as their views, likes and dislikes, comments, and time of engagement. AI also itself develops and "labels" data that capture specific characteristics of the content found in its inventories. The "labels" the AI assigns to such characteristics permit the AI's algorithm to locate and retrieve the most appealing videos for an individual user. The YouTube recommendation algorithm locates and displays videos that are often watched together or which are related by topic.

AI is so powerful it can across vast amounts of data detect associations that are not evident to humans. A platform's algorithm knows us better than we know ourselves.

As a business matter, platforms seek to maximize the advertising revenue. The dominant ranking factor of the current version of the YouTube recommendation system, for example, is maximizing viewer "satisfaction" or what is more commonly described by other platforms as "user engagement." Engagement is an algorithm built on clicks of the "not interested" button, likes and dislikes, sharing, commenting, average view duration and average percentage viewed.

In this way, platform experiences are personalized to match platforms' billions of users and drive a significant amount of who actually sees what, when, and for how long.

But, that's not all. How the platforms entice users to interact with the platform's recommendations is the final part of the integrated, AI automated recommending machine. YouTube's recommendation system, for example, includes the home page and the Up Next menu of suggested videos. The pages of the other familiar platforms includes "likes," comments, and "nudges" enticing users who have left to return to the platform.

The founding president of Facebook Sean Parker has said "The thought process that went into building these applications… was all about: 'How do we consume as much of your time and conscious attention as possible?'" Erica Pandy, Sean Parker: Facebook Was Designed To Exploit Human "Vulnerability", Axios (Nov. 9, 2017), https://tinyurl.com/5camx6rt. Google's, Facebook's, and TikTok's executives and management may set for the AI a goal for the recommendation algorithm, but automated AI is invented, programed, and "hired" to chart autonomously thereafter the best course to obtain this goal.

How In Detail Particular Parts Of AI-driven Social Media Recommendation Machines Like Google's YouTube Work.

A. Social media platforms' revenue model.

Social media platforms like YouTube and Facebook derive their profits from the sale of on-screen advertising. The more time spent on the platform, the more ads will be seen, the more valuable the advertising becomes. Plus, the more time a user spends on the platform, the more data the platform can derive about the user which, in turn, it can use to keep the user on the platform.

"Advertising isn't just a way for [Facebook] and its ilk to perhaps earn a little bit of revenue in between hosting family photos and personal musings. It's the very purpose of the site's existence, and the same goes for Twitter and LinkedIn." "There's a reason why [Facebook's] 10-K filing with the U. S. Securities and Exchange Commission (SEC) uses the acronym ARPU, as in average revenue per user" and why investors track "monthly median engagement levels" measuring increases or decreases in the average number of likes, comments posted, and ads clicked.

There is no natural end-point to the motivation of social media companies to engage their users more and more through ever more potent recommendations. To achieve revenue and market share growth every quarter – to not peak or decline – platforms must figure out ways to keep us on their platforms more and more. "Facebook's data, algorithms and use of machine learning have continued to improve … "This means that users are seeing more and more relevant content, and this of course leads to more engagement on the platform." Salvador Rodriguez, Facebook has had numerous scandals, So why does user engagement keep growing?, Milwaukee J. Sentinel (Jul 22, 2019), https://tinyurl.com/y66mbvpt.

B. AI-recommendation machines can operate autonomously. Whether such automation can foreseeably cause harms to particular sets of people is a question of fact in each case.

A platform's human employees do not select the content to be delivered to each of the platform's users. AI machine learning algorithms make those "decisions" and generate these outputs to users autonomously. Their only input into the algorithm is to set the AI's goal or objective and provide it with initial means for achieving that goal.

It is really challenging to describe in words just how truly and autonomously intelligent these AI machines are but here is one way of describing it:

> Cicero, released last week [by Facebook], was able to trick humans into thinking it was real … and can invite players to join alliances, craft invasion plans and negotiate peace deals when needed. The model's mastery of language surprised some scientists and its creators, who thought this level of sophistication was years away. But experts said its ability to withhold information, think multiple steps ahead of opponents and outsmart human competitors sparks broader concerns. …"It's a great example of just how much we can fool other human beings," said Kentaro Toyama, a professor and artificial intelligence expert at the University of Michigan[.] "These things are super scary … [and] could be used for evil."

Pranshu Verma, Meta's New AI is Skileld at a Ruthless, Power-Seeking Game, Wash. Post (Dec. 1, 2022), https://tinyurl.com/4vbxp924.

So, if an AI developed by platforms like Google and Facebook is given the instruction "maximize user engagement!" it will do so by testing what recommendations work best and then re-writing and re-writing its own algorithms, at fantastic speeds, adjusting in real time, based not a "neutral" criteria or one that is solely or even mostly determined by what the user thinks it wants. It will serve up content that fulfills the goal of "maximizing engagement" no matter how foreseeably harm might occur, precisely because AI does not foresee harm, unless programmed to avoid it. If a lawsuit alleges that someone was harmed in whole or in part because of an AI-driven recommendation, some form of reasonable human intervention at some phase of the content-gathering and delivery-to-user process is required to minimize or eliminate these harms if the company that issued the instruction is to satisfy its duty of ordinary care in negligence law.

C. Massive amounts of the most intimate data imaginable for the AI.

The behavioral data companies like YouTube and Facebook gather about us for use by recommendation algorithms is far more robust, profoundly intimate, and psychologically attractive than even what would be available from a constant video stream from each room of our homes.

Nobody knows exactly how platforms' AI work but it is likely they use AI that identifies and combines massive amounts of user data from online profiles, browsing activity, smart devices, public sensors, purchased cookie data, video and music preferences, public records, and many other means of data capture. As a result, platforms may have up to a million data points on each user of their "free" services.

Once raw data is collected from this "big data" ecosystem, it is digested by a process known as data analytics, resulting in the creation of individualized behavioral profiles on billions of Google and YouTube users. Through these analytical tools, a platform has assembled a complete behavioral profile on each of its users; one constantly updated based on what the user does and what other users do. In addition to the behavioral and psychographic profiles used as inputs, the

algorithm's recommended output is also customized by the viewer's location, type of device she is using (e.g., smartphone, computer or high definition television), bandwidth and time of day.

D. "Gamification," "nudges" "infinite scroll," "likes," "streaks" and how they work in combination with AI-recommendations to maximize "user engagement."

The final part of how social media platforms' automated targeting works is how recommendations are visually presented to the user. Social media platforms use neuroscientifically grounded techniques that "gamify" how users interact with the content recommended. Here are some examples:

- The infinite scroll which serves up a never-ending stream of videos as the user scrolls downward. Hilary Andersson, Social Media Apps Are 'Deliberately' Addictive to Users, BBC News (Jul. 4, 2018). Hilary Andersson, Social Media Apps Are 'Deliberately' Addictive to Users, BBC News (Jul. 4, 2018), https://tinyurl.com/mwy2vppb.

- Algorithms can shape the user's perception of their relationships with other users without the user's knowledge. Motahhare Eslami et al., "I Always Assumed That I Wasn't Really That Close to [Her]": Reasoning About Invisible Algorithms in News Feeds, Proc. of the 33rd Ann. ACM Conf. on Hum. Factors in Computing Sys. 153, 153-62 (2015), https://tinyurl.com/4fpx5vwn.

- Teens are powerfully influenced by the Facebook "likes" from their peers. Eveline A. Crone & Elly A. Konijn, Media Use and Brain Development During Adolescence, 9 Nat. Commc'n. (2018), pp. 1-10, https://tinyurl.com/rvjun2j5.(See more detailed discussion below)

QUESTIONS 2 AND 3:

- **What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?**

- **What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?**

There are no federal or state laws that seek to ensure that the single-minded zeal of social media platforms to increase "user engagement" is balanced against preventing harm to children. The results of this absence are no less than an historic catastrophe for child consumers

Here is just one data point underscoring the catastrophe. During the rise of social media use among the very young, between 2011 and 2020, there has been a 146% increase in children ages 10 to 14 using firearms to die by their own small hands.[1]

The San Mateo County Office of Education has correctly observed that "there is hard science demonstrating the claim that social media is fueling a mental health epidemic in school-age children."[2] A paraphrase of that County's lawsuit against the platforms describes the current, urgent situation:

> This [lawsuit addresses] one of the most serious issues facing the nation's children, adolescents, and teenagers—perhaps the most serious mental health crisis they have ever faced. Powerful corporations who wield unmatched, highly concentrated technology in pursuit of profit are knowingly creating this unprecedented mental health crisis. [Platforms] have carefully cultivated the crisis, which is a feature—not a bug—of their social media products. Thanks to the U.S. Congress and concerned whistleblowers, critical facts have recently come to light. [The]public can now fairly conclude that the [platforms'] conduct was no accident, but rather that [they] acted knowingly, deliberately, and intentionally.[3]

Social media platforms cannot, either knowingly or by failing to take even the most basic care, be permitted to operate in ways that cause an unprecedented number of children to kill themselves, to overdose, to starve themselves, to become addicted to their products, or to otherwise hurt themselves and other children. This must end immediately and forever, as only binding laws can assure. Utah has shown the way by enacting HR 311, permitting injured children to sue social media platforms for damages and penalties when the platforms knowingly or negligently make addicts of children.[4] This new Utah law is nearly verbatim from last year's AB 2408 (Cunningham and Wicks), a bill that received bi-partisan support and no "no" votes, but died in the Senate Appropriations suspense file.

As discussed below and in detail worthy of an unprecedented child mental health catastrophe, the social media platform giants know precisely what their products are doing to our children – and they are doing it anyway.

TWO PICTURES SAY IT ALL

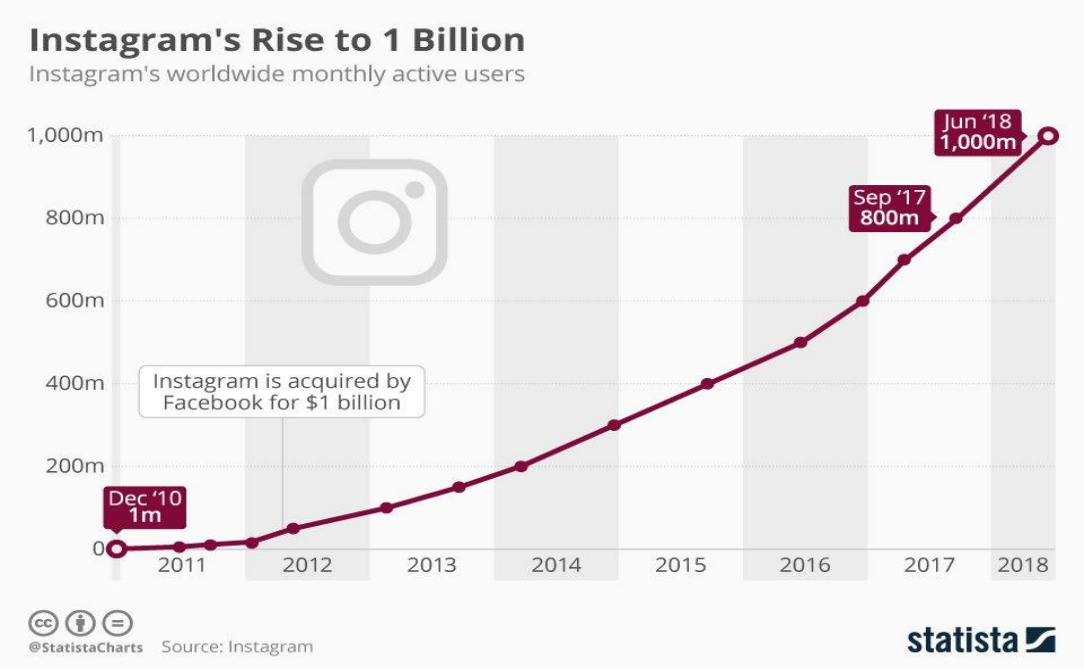
Suicides, self-harm, and major depression are spiking in ways never before seen, especially among teen girls, and two graphs show why:

[1] https://everytownresearch.org/report/the-rise-of-firearm-suicide-among-young-americans/.
[2] https://www.smcoe.org/for-communities/san-mateo-county-school-board-and-superintendent-sue-social-media-companies.html.
[3] https://www.smcoe.org/assets/files/For%20Communities_FIL/Social%20Media%20Lawsuit_FIL/2023-03-13%20[1]%20Social%20Media%20Complaint.pdf.
[4] https://le.utah.gov/~2023/bills/static/HB0311.html.

Increases in Depression, Self-Harm, and Suicide Among U.S. Adolescents
FIGURE 1. Indicators of poor mental health among U.S. girls and young women, 2001–2018 (note, before COVID)

[5]

This never-before-seen spike in suicides among teen girls has occurred during this exact same time frame as the following:



[5] https://prcp.psychiatryonline.org/doi/full/10.1176/appi.prcp.20190015.

Research affirms the cause-and-effect relationship between these charts. For example, excessive use of digital and social media has a documented connection to increases in suicide-related outcomes in teens and children, such as suicidal ideation, plans, and attempts.[6]

So do the facts in individual cases like that of Molly Russell's. A coroner's inquest is like a trial in the United Kingdom. An inquest there investigated the alleged suicide of 14 year old Molly. Voluminous evidence was taken and many witnesses called, including from Facebook. In a ruling that made headlines throughout Europe, the Coroner ruled the algorithms that curate a social media user's experience had pushed harmful content to Molly that she had not requested."[7]

> Thousands of images, videos and other social media material from Molly's accounts were revealed during the investigation, one of the largest public releases of its kind. That provided the sort of detail that researchers studying the mental health effects of social media have long complained that platforms like Meta, which owns Facebook and Instagram, withhold on privacy and ethical grounds.
>
> Molly's social media use included material so upsetting that one courtroom worker stepped out of the room to avoid viewing a series of Instagram videos depicting suicide. A child psychologist who was called as an expert witness said the material was so "disturbing" and "distressing" that it caused him to lose sleep for weeks.[8]

Molly is far from alone in her suffering. Consider these findings from a 2021 U.S. Surgeon General Advisory:

- From 2009 to 2019, the proportion of high school students reporting persistent feelings of sadness or hopelessness increased by 40%;
- the share seriously considering attempting suicide increased by 36%; and
- the share creating a suicide plan increased by 44%.
- Between 2011 and 2015, youth psychiatric visits to emergency departments for depression, anxiety, and behavioral challenges increased by 28%.
- Between 2007 and 2018, suicide rates among youth ages 10–24 in the US increased by 57%.[9]

In explaining the crisis' origins, the Surgeon General noted a "growing concern about the impact of digital technologies, particularly social media, on the mental health and wellbeing of children and young people" and called for greater accountability from social media companies.[10] Business models are often built around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways. This

---

[6] Elizabeth J. Ivie et al., *A Meta-Analysis of the Association Between Adolescent Social Media Use and Depressive Symptoms*, 275 J. OF AFFECTIVE DISORDERS 165, 165–174 (2020), https://tinyurl.com/bdzu6h8h; Alan Mozes, As Social Media Time Rises, So Does Teen Girls' Suicide Risk, U.S. NEWS (Feb. 16, 2021), https://tinyurl.com/49hzmm9v.

[7] https://www.bbc.com/news/uk-england-london-63073489

[8] https://www.nytimes.com/2022/10/01/business/instagram-suicide-ruling-britain html

[9] U.S. Surgeon General's Advisory: PROTECTING YOUTH MENTAL HEALTH, p. 8 (2021), at https://www.hhs.gov/sites/default/files/surgeon-general-youth-mental-health-advisory.pdf

[10] *Id.* at 25.

translates to technology companies focusing on maximizing time spent, not time well spent."[11] Meanwhile, *reducing* social media use has been shown to result in mental health benefits.[12]

FACEBOOK KNOWS

Facebook Knows It Is Making Addicts of Children

> **Zuckerberg Was Warned on Social Media Addiction, Filing Says**
>
> Employees at Meta Platforms and ByteDance were aware of the harmful effects of their platforms on young children and teenagers but disregarded the information or in some cases sought to undermine it, according to claims in a court filing. …
>
> "No one wakes up thinking they want to maximize the number of times they open Instagram that day," one Meta employee wrote in 2021, according to the filing. "But that's exactly what our product teams are trying to do."[13]

As Facebook's first President, Sean Parker, has admitted:

> God only knows what it's doing to our children's brains.
>
> The thought process that went into building these applications, Facebook being the first of them …was all about: "How do we consume as much of your time and conscious attention as possible?" And that means that we need to sort of give you a little dopamine hit every once in a while …you're exploiting a vulnerability in human psychology. The inventors, creators . . . understood this consciously.
>
> And we did it anyway.[14]

In an internal Facebook document entitled "*The Power of Identities: Why Teens and Young Adults Choose Instagram,*" Facebook staff explain secretly to their executives that: "The teenage brain is usually about 80% mature. The remaining 20% rests in the frontal cortex . . . At this time teens are highly dependent on their temporal lobe where emotions, memory, and learning, and the reward system reign supreme . . . Teens' decisions and behavior are mainly driven by emotion, the intrigue of novelty and reward[.]"[15]

So, they know young brains are vulnerable to their technologies and, paraphrasing Parker, "they did it anyway." Thus, here is one of the charts leaked by Frances Haugen, the former Facebook

---

[11] *Id.* (emphasis in original).

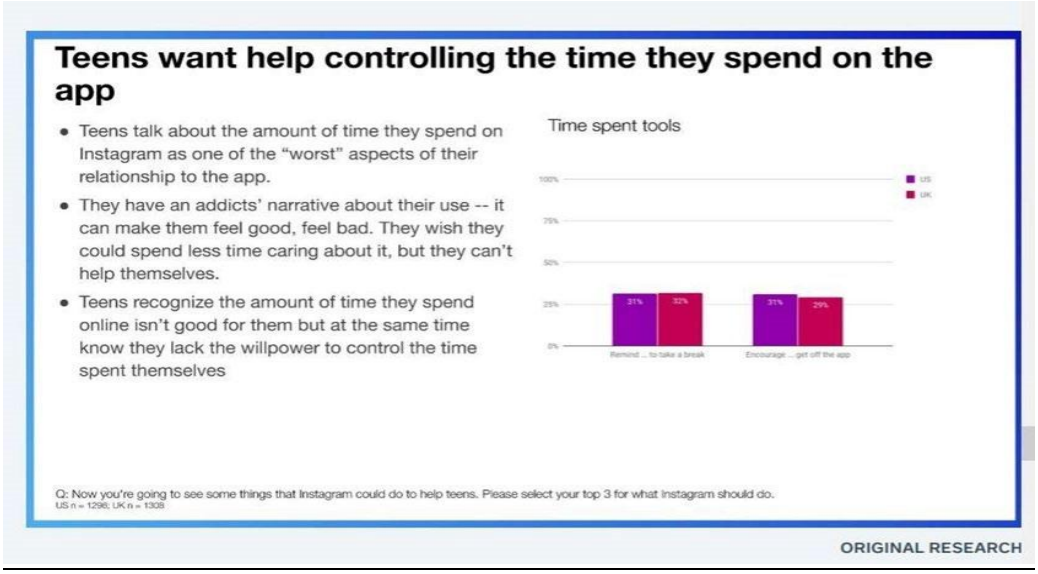
[12] Roberto Mosquera et al., *The Economic Effects of Facebook*, 23 EXP. ECON. 575 (Jun. 2020). Melissa G. Hunt et al., *No More FOMO Limiting Social Media Decreases Loneliness and Depression*, 37 J. SOC. CLINICAL PSYCH. 751 (Guilford Publications Inc. Nov. 2018). Hunt Allcott et al., *The Welfare Effects of Social Media*, 110 AM. EC. REV. 629 (Mar. 2020).

[13] https://www.latimes.com/business/story/2023-03-13/zuckerberg-was-warned-on-social-media-addiction-filing-says.

[14] https://www.axios.com/2017/12/15/sean-parker-unloads-on-facebook-god-only-knows-what-its-doing-to-our-childrens-brains-1513306792.

[15] *The Power of Identities Why Teens and Young Adults Choose Instagram,* p. 30 (internal Facebook documents identifying and explaining that the "4M teens that start using the internet each year" are the only source for "significant [monthly active user] growth in the US."), https://s3.documentcloud.org/documents/21090788/why-teens-and-young-adults-choose-insta.pdf pp. 52-53(last visited Mar.21, 2023). As New York University professor and social psychologist Adam Alter has explained, product features such as "Likes" give users a dopamine hit similar to drugs and alcohol: "The minute you take a drug, drink alcohol, smoke a cigarette . . . when you get a like on social media, all of those experiences produce dopamine, which is a chemical that's associated with pleasure. When someone likes an Instagram post or any content that you share, it's a little bit like taking a drug. As far as your brain is concerned, it's a very similar experience." Eames Yates, *What happens to your brain when you get a like on Instagram*, Business Insider (Mar. 25, 2017), https://www.businessinsider.com/what-happens-to-your-brain-like-instagramdopamine-2017-3; Zara Abrams, *Why young brains are especially vulnerable to social media*, AM. PSYCH. ASS'N (Aug. 25, 2022), https://www.apa.org/news/apa/2022/social-media-children-teens.

executive. Again, this is Facebook's own researched, secret chart documenting "**an addict's narrative"** from children about their own product:



As United States Senator Richard Blumenthal, Democrat of Connecticut, has observed:

> *Facebook has taken big tobacco's playbook, it has hidden its own research on addiction and the toxic effects of its products. … It's chosen growth over children's mental health and wellbeing, greed over preventing the suffering of children.*[16]

Facebook Knows It Prompts Its Child Users to Consider Suicide.

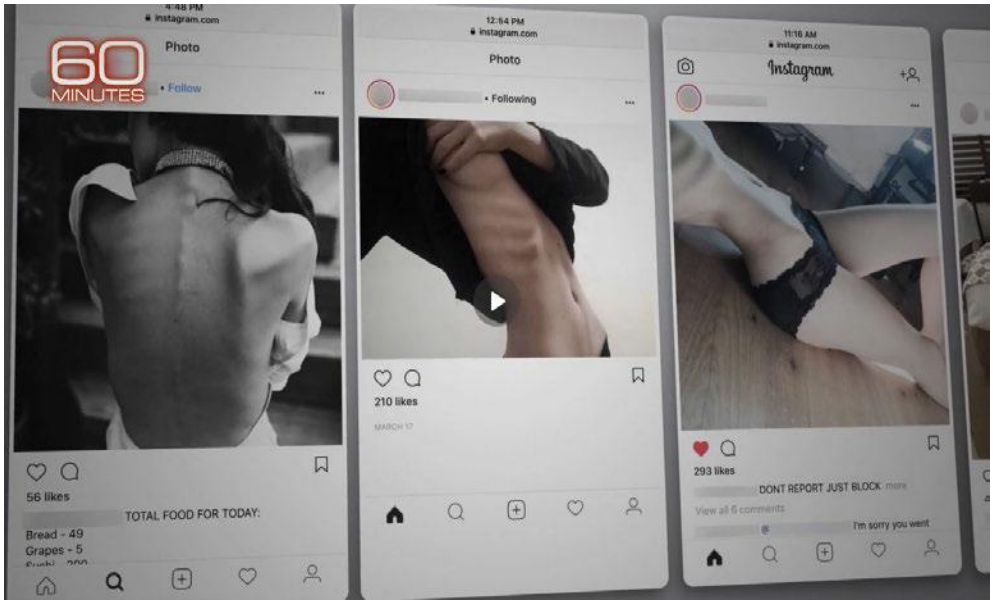
Another slide leaked by Haugen said: "Among teen users [of Instagram] who reported suicidal thoughts… 6% of American [teen] users **traced the desire to kill themselves to Instagram.**"[17]

Facebook Knows It Promotes Pro-Eating Disorder Content to Teen Girls

> **"*Facebook knew Instagram was pushing girls to dangerous content: internal document*" –** *CBS News 12.11.22* – In 2021, according to the document, an Instagram employee ran an internal investigation on eating disorders by opening a false account as a 13-year-old girl looking for diet tips. She was led to graphic content and recommendations to follow accounts titled "skinny binge" and "apple core anorexic."[18]

Just a glance at the content pushed to girls under the secret Facebook investigation, ***including to girls who do not search for it***, underscores the urgency of legislative action:

[16] *Facebook Head of Safety Testimony on Mental Health Effects Full Senate Hearing Transcript*, REV, https://www.rev.com/blog/transcripts/facebook-head-of-safety-testimony-on-mental-health-effects-full-senate-hearing-transcript (Emphasis added).
[17] https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.
[18] https://www.cbsnews.com/news/facebook-instagram-dangerous-content-60-minutes-2022-12-11/.



A March 2020 presentation posted by Facebook researchers to Facebook's internal message board reported that "66% of teen girls on IG experience negative social comparison (compared to 40% of teen boys)" and that "[a]spects of Instagram exacerbate each other to create a perfect storm." **"We make body image issues worse for one in three teen girls**," said one slide from 2019.

As one expert observed, "Instagram perpetuates the myth that our happiness and ability to be loved are dependent on external things: For girls, it's appearance[.]"[19] The picture-perfect images on Instagram's news feeds are so potent that they cement these superficial and harmful values into adolescent brains without them even knowing it."[20]

TIKTOK KNOWS

TikTok Knows It Is Making Addicts of Children

Children on TikTok do not have control over what they see. Like Facebook, TikTok's powerful machine-learning, AI-powered algorithms select content to feed child users to maximize their engagement with the platform instead of simply responding to searches by child users. TikTok uses "a machine-learning system that analyzes each video and tracks user behavior to serve up a continually refined, never-ending stream of TikToks optimized to hold [users'] attention."[21] As another commentator put it, "**you don't tell TikTok what you want to see. It tells you.**"[22]

This, TikTok knows, will result in addiction for some child users. An internal document titled "TikTok Algo 101" frankly explains that in the pursuit of the company's "ultimate goal" of adding daily active users, it has chosen to optimize for two closely related metrics in the stream of videos it serves: "retention"—that is, whether a user comes back—and "time spent."[23]

---

[19] Jennifer Wallace, *Instagram is Even Worse than We Thought for Kids. What Do We Do about It?*, WASHINGTON POST, https://www.washingtonpost.com/lifestyle/2021/09/17/instagram-teens-parent-advice/.
[20] *Id.*
[21] Jia Tolentino, How TikTok Holds Our Attention, New Yorker (Sept. 30, 2019), https://www.newyorker.com/magazine/2019/09/30/how-tiktok-holds-our-attention.
[22] Drew Harwell, How TikTok Ate the Internet, Wash. Post. (Oct. 14, 2022), https://www.theday.com/business/20221015/how-tiktok-ate-the-internet/.
[23] Ben Smith, *How TikTok Reads Your Mind*, N.Y. TIMES (Dec. 5, 2021), https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html.

As the founder of Algo Transparency remarked, "rather than giving [people] what they really want," TikTok's "algorithm tries to get people addicted[.]"[24]

Indeed, a recent study by TikTok based on brain imaging boasts to potential advertisers that those using TikTok engaged with the product about ten times a minute, twice as often as with peer apps.[25] ("Neuro-Insight is a neuroanalytics company that uses unique in-lab, privacy-safe brain imaging technology to measure how the brain responds to communications.")

Observe: *TikTok is boasting to advertisers that it is using brain imaging to validate its product's value to advertisers*.

Unsurprisingly, given all this, an estimated 90–95% of the content viewed on TikTok comes from its algorithms as opposed to what a child seeks out.[26]

The cumulative effect of TikTok's inventions can be medically and clinically addictive to children. As researchers at the Brown University School of Public Health explained, "the infinite scroll and variable reward pattern of TikTok likely increase the addictive quality of the app as they may induce a flow-like state for users that is characterized by a high degree of focus and productivity at the task at hand."[27] And, as Dr. Julie Albright, a Professor at the University of Southern California, similarly explained, TikTok is so popular because child users will "just be in this pleasurable dopamine state, carried away. It's almost hypnotic, you'll keep watching and watching." Users "keep scrolling," according to Dr. Albright, "because sometimes you see something you like, and sometimes you don't. And that differentiation—very similar to a slot machine in Vegas—is key."[28]

TikTok Knows It Prompts Its Child Users to Consider Suicide.

The Wall Street Journal programmed bots on TikTok with various interests such as sports, forestry, dance, astrology, and animals. However, *The Journal* did not disclose these interests upon registration with TikTok. Instead, TikTok's algorithm quickly learned the assigned interests from the "rewatching or pausing on videos" related to the bot's programmed interest.[29]

One bot watched an astonishing 224 videos in 26 minutes, lingering over videos with hashtags for "depression" or "sad." TikTok's algorithm quickly refined its output. Afterward, 93% of the videos TikTok showed that bot were about depression or sadness. One post implored the bot to: "Just go. Leave. Stop trying. Stop pretending. You know it, and so do they. Do Everyone a favor and leave."[30]

---

[24] *Id.*
[25] TikTok Ads Break Through Better Than Tv and Drive Greater Audience Engagement, TikTok, https://www.tiktok.com/business/library/TikTokDrivesGreaterAudienceEngagement.pdf .
[26] *Investigation How TikTok's Algorithm Figures Out Your Deepest Desires*, WALL ST. J. (Jul. 21, 2021), https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigationhow-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796.
[27] Sophia Petrillo, *What Makes TikTok So Addictive? An Analysis of the Mechanisms Underlying the World's Latest Social Media Craze*, BROWN UNDERGRADUATE J. OF PUB. HEALTH (Dec. 13, 2021), https://sites.brown.edu/publichealthjournal/2021/12/13/tiktok/.
[28] John Koetsier, *Digital Crack Cocaine The Science Behind TikTok's Success*, FORBES (Jan. 18, 2020), https://www.forbes.com/sites/johnkoetsier/2020/01/18/digital-crack-cocaine-the-science-behind-tiktoks-success/?sh=32fdcd4e78be.
[29] *Inside TikTok's Algorithm A WSJ Video Investigation*, WALL ST. J. (July 21, 2021), https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477.
[30] Inside TikTok's Algorithm: A WSJ Video Investigation, Wall St. J. (July 21, 2021), https://www.wsj.com/articles/tiktok-algorithm-video-investigation-11626877477.

Center for Countering Digital Hate researchers set up new accounts in the United States, United Kingdom, Canada, and Australia at the minimum age TikTok allows; 13 years old. "These accounts paused briefly on videos about body image and mental health and liked them. What we found was deeply disturbing. Within 2.6 minutes, TikTok recommended suicide content.[31]

TikTok Knows It Promotes Pro-Eating Disorder Content to Teen Girls

In another experiment, *The Wall Street Journal* found that once TikTok's algorithm determined that its bots would watch videos related to weight loss, TikTok "speedily began serving more, until weight-loss and fitness content made up more than half their feeds—even if the bot never sought it out." Indeed, TikTok's algorithm recommended ***over 32,000 weight-loss videos over a two-month period, "many promoting fasting, offering tips for quickly burning belly fat and pushing weight-loss detox programs and participation in extreme weight-loss competitions***."[32] (Note in the footnote the title of the article: "The Corpse Bride Diet")

Others confirm *The Journal's* research. Recently Center for Countering Digital Hate researchers set up new accounts in the United States, United Kingdom, Canada, and Australia at the minimum age TikTok allows; 13 years old. "These accounts paused briefly on videos about body image and mental health and liked them. What we found was deeply disturbing. Within 2.6 minutes, TikTok recommended suicide content. Within 8 minutes, TikTok served content related to eating disorders. Every 39 seconds, TikTok recommended videos about body image and mental health to teens."[33] Indeed, girls were delivered videos advertising breast enhancement oil and weight loss patches—without having followed any other accounts or having searched for terms related to these topics."[34]

Children, mental health providers, families, teachers, and parents must deal with the tragic consequences of TikTok knowingly designing its products in such a way as to barrage body-anxious teen girls with pro-eating disorder content. Alyssa Moukheiber, a treatment center dietitian, explained that TikTok's algorithm can push children into unhealthy behaviors or trigger a relapse of disordered eating. Teenage girls interviewed by *The Wall Street Journal* reported developing eating disorders or relapsing after being influenced by extreme diet videos TikTok promoted to them. Katie Bell, a co-founder of the Healthy Teen Project, explained that "the majority of her 17 teenage residential patients told her TikTok played a role in their eating disorders." And Stephanie Zerwas, an Associate Professor of Psychiatry at the University of North Carolina at Chapel Hill, could not even recount how many of her young patients told her that "I've started falling down this rabbit hole, or I got really into this or that influencer on TikTok, and then it started to feel like eating-disorder behavior was normal, that everybody was doing that."[35]

[31] Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement, FED. TRADE COMM'N (Nov. 17, 2022) at 10, https://tinyurl.com/3mursy95.
[32] Tawnell D. Hobbs, '*The Corpse Bride Diet' How TikTok Inundates Teens With Eating-Disorder Videos*, WALL ST. J. (Dec. 17, 2021), https://www.wsj.com/articles/how-tiktok-inundates-teens-with-eating-disorder-videos-11639754848?mod=tech_lista_pos3.
[33] https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf.
[34] Petition for Rulemaking to Prohibit the Use on Children of Design Features that Maximize for Engagement, FED. TRADE COMM'N (Nov. 17, 2022) at 10, https://tinyurl.com/3mursy95.
[35] Tawnell D. Hobbs, '*The Corpse Bride Diet' How TikTok Inundates Teens With Eating-Disorder Videos*, WALL ST. J. (Dec. 17, 2021), https://www.wsj.com/articles/how-tiktok-inundates-teens-with-eating-disorder-videos-11639754848?mod=tech_lista_pos3.

PLEASE NOTE: ***It isn't the simple existence of the pro-eating disorder content lying around somewhere out there among the billions of uploads addressing every possible topic that is the problem. As documented above, the problem is that undeveloped child minds are being pounded by autonomously operating AI over and over again with dangerous but teen-riveting content, content that (in the case of TikTok) over 90% of the time the child did not seek out for themselves.[36] It is this documented, relentless, automated, pounding combined with dopamine-firing, addictive interfaces like auto-scroll, that explain the unprecedented numbers of children with severe depression, who are dying by suicide, starving themselves, and who become isolated in this perilous world due to social media addiction.***

This relentless pounding is not an inevitable way to deliver content. We use Google search every day, which is organized to deliver relevant content to keep us returning to the platform. Facebook screens out adult pornographic posts effectively, knowing if it did not, it would lose customers. YouTube refuses to post copyrighted songs for fear of being sued. The platforms' decision to use technology and neuroscience to get people—children included—to stay on their products for as long as possible, by any means necessary, no matter how utterly foreseeable the harmful consequences are to children, is a simple business decision of prioritizing profits (the higher the user engagement, the more they can charge for ads) over child safety.

TikTok Knows It Is Facilitating the Sale of Lethal Drugs to Children

One of the bots programmed by *The Wall Street Journal* was programmed to pause on videos referencing drugs and lingered briefly on "a video of a young woman walking through the woods with a caption" referring to "stoner girls." The next day, the algorithm showed the bot a video about a "marijuana-themed cake." Then, the "majority of the next thousand videos" that TikTok's algorithm produced "tout[ed] drugs and drug use," including marijuana, psychedelics, and prescription drugs.[37]

The Wall Street Journal concluded, "that through its powerful algorithms, TikTok can quickly drive minors—among the biggest users of the app—into endless spools of content about sex and drugs."[38]

When it comes to the epidemic of deaths of children from deadly fentanyl, it isn't just TikTok. The unprecedented spike of children dying from overdosing on fentanyl has been documented to be the fault of all social media. According to, for example, *The New York Times* article titled **"Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar--Teenagers and young adults are turning to Snapchat, TikTok and other social media apps to find Percocet, Xanax and other pills. The vast majority are laced with deadly doses of fentanyl, police say**:"

- "Law enforcement authorities say an alarming portion of [fentanyl overdoses] unfolded … from counterfeit pills tainted with fentanyl that teenagers and young adults bought over social media."
- "Social media is almost exclusively the way they get the pills," said Morgan Gire, District Attorney for Placer County, Calif., where 40 people died from fentanyl poisoning last year.

[36] *Investigation How TikTok's Algorithm Figures Out Your Deepest Desires*, WALL ST. J. (Jul. 21, 2021), https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigationhow-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796.
[37] Rob Barry et al., *How TikTok Serves Up Sex and Drug Videos to Minors*, WALL ST. J. (Sept. 8, 2021), https://www.wsj.com/articles/tiktok-algorithm-sex-drugs-minors-11631052944.
[38] *Ibid*.

- "Overdoses are now the leading cause of preventable death among people ages 18 to 45, ahead of suicide, traffic accidents and gun violence, according to federal data.
- "**There are drug sellers on every major social media platform," one expert is quoted as saying…: As long as your child is on one of those platforms, they're going to have the potential to be exposed to drug sellers**."

SNAP KNOWS

Snapchat only looks small in comparison to Facebook and TikTok. Snapchat has 100 million daily users in North America.[39] In 2022, 59% of U.S. teens, 13–17 years of age, used Snapchat, and 15% said they used it "almost constantly."[40]

Snap's executives have admitted that Snapchat's age verification "is effectively useless in stopping underage users from signing up to the Snapchat app."[41] True enough, underage use of Snapchat is rampant. As of 2021, 13% of children ages 8–12 use Snapchat.[42] You can infer how many truly young children use Snap from imagery such as this:

As Sen. Richard Blumenthal, D-Conn, said in a recent U.S. Senate hearing on social media involving TikTok and Snap: "Being different from Facebook is not a defense …. That bar is in the gutter. It's not a defense to say that you are different."[43]

Snap Knows It Is Making Addicts of Children

Research shows that Snapchat's daily users are using Snapchat more constantly than other platforms. For example (remembering how young Snapchat's users are), users are most likely to use Snapchat "right when I wake up," "before work/school," "during work/school," "after work/school," "on vacations," and "when I'm with others[.]"[44]

In a December 2022 statement to advertisers, Snap claimed that "Snapchat delivers on the

[39] October 2022 Investor Presentation at 5, Snap Inc. (Oct. 20, 2022), https://investor.snap.com/events-and-presentations/presentations/default.aspx.
[40] Pew Research Center, *Teens, Social Media and Technology* 2022 (Aug. 10, 2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.
[41] Isobel Asher Hamilton, *Snapchat Admits Its Age Verification Safeguards are Effectively Useless*, BUS. INSIDER (Mar. 19, 2019), https://www.businessinsider.com/snapchat-says-its-age-verification-safeguards-are-effectively-useless-2019-3#:~:text=Collins%20admitted%20that%20the%20system,mobile%20app%20is%20more%20popular.
[42] Victoria Rideout et al., *Common Sense Census Media Use by Tweens and Teens*, 2021 at 5, Common Sense Media, https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf.
[43] Bobby Allyn, *4 Takeaways from the Senate Child Safety Hearing with Youtube, Snapchat and Tiktok*, NPR BUSINESS, at https://www.npr.org/2021/10/26/1049267501/snapchat-tiktok-youtube-congress-child-safety-hearing.587.
[44] Multi-District Litigation Complaint, Snap evidence, SNAP0000103 at 0113.

emotions that Gen Z seeks, and it does so consistently across the platform[.]"[45] To bolster this claim, Snapchat "used a neuroscience measurement … to measure reactions to different brand messaging" "through variations in heart rate rhythm collected by smartwatches."[46]

Snapchat includes a variety of techniques designed psychologically to arm-twist children to stay on the platform; products such as **Snapscores, Snapstreaks**, and **Snap Awards** reward users when they engage with Snapchat and punish them when they fail to engage with Snapchat.

Snapscore keeps a running profile score based on a user's Snapchat activity levels, such as the number of Snaps sent.[47] The sole purpose of Snapscore—again, remember this is mostly a platform used by children and teens—is to increase product use and drive revenue.[48] Snapscores are especially important to child users because they operate as a form of social validation like an Instagram "Like." Here is what a Snapscore looks like:

Snap awards include "Charms." Charms cleverly reward users for achieving certain milestones together to leverage relationships into multiple children being on the platform. For example, if two users exchange frequent Snaps, they may unlock a "BFF (Best Friends Forever)" Charm. Conversely, Charms may be awarded to friends who are infrequently in contact to prompt both to stay on the platform:

[45] Snap for Business, *What Does Gen Z Want From Brands?* (Dec. 15, 2022), https://forbusiness.snapchat.com/en-US/blog/what-does-gen-z-want.

[46] *Id.*

[47] Snapchat Support, What is a Snapscore? ("Your Snapchat score is determined by a supersecret, special equation…") https://support.snapchat.com/en-US/a/my-score ("Your Snapchat score is determined by a super-secret, special equation…").

[48] Brad Barbz, *2020 NEW * How To Increase Snapscore By Up To 1000 Per Minute On IOS And Android - Working 2020, YouTube (Dec. 4, 2019), https://www.youtube.com/watch?v=Mo_tajuofLA.

Snapstreaks are maybe the most addictive of Snap's offerings to teens, maybe the most addicting for children of all platform inventions.[49] Two child users achieve a Snapstreak when they exchange at least one Snap in three consecutive 24-hour periods. When the "Streak" is achieved, users receive a fire emoji next to their profile avatar. For a Streak of 100 days, for example, each child receives a "100" emoji.

No less an authority on social media addiction than Facebook, in internal documents, has acknowledged how addicting Streaks are for teens, observing: "Streaks are a very important way for teens to stay connected. They are usually with your closest friends, and they are addictive." [50]

Indeed, the peer pressure not to break a Streak can be enormous. Researchers have found that losing a Streak can cause friends to feel betrayed. This is especially true of teen girls who reported "negative" feelings when losing a Streak with one of their friends.[51] In 2018, Snap conducted its own internal research on Snapstreaks, which found that over a third of users reported it was "extremely" or "very important" to keep a Streak going, and that some users reported that the stress to keep a Streak was "intolerable" or "large."[52]

Snap sends ominous notifications to child users with an hourglass emoji when Streaks are about to expire:

Unsurprisingly, one study of over 2,000 UK residents found 68% of respondents who used Snapchat reported that "the platform prevented them from sleeping."[53]

Snap Knows It Promotes "Snapchat Dysmorphia" to Teen Girls

Snap also incorporates numerous custom-designed lenses and filters, which allow users to edit and overlay augmented-reality special effects and sounds on their Snaps. Many of Snapchat's lenses and filters change users' appearance and face, creating unrealistic, idealized versions that cause

[49] *See* Cathy Becker, *Experts Warn Parents How Snapchat Can Hook in Teens with Streaks*, ABC NEWS (July 27, 2017), https://abcnews.go.com/Lifestyle/experts-warn-parents-snapchat-hookteens-streaks/story?id=48778296; Avery Hartmans, *These are the Sneaky Ways Apps Like Instagram, Facebook, Tinder Lure You in and Get You Addicted'*, BUS. INSIDER (Feb. 17, 2018), https://www.businessinsider.com/how-app-developers-keep-us-addicted-to-our-smartphones-2018-1#snapchat-uses-snapstreaks-to-keep-you-hooked-13; *see generally*, Virginia Smart & Tyana Grundig, *We're designing minds' Industry insider reveals secrets of addictive app trade*, CBC (Nov. 3, 2017), https://www.cbc.ca/news/science/marketplace-phones-1.4384876; Julian Morgans, *The Secret Ways Social Media is Built for Addiction*, VICE (May 17, 2017), https://www.vice.com/en/article/vv5jkb/the-secret-ways-social-media-is-built-for-addiction.
[50] MultiDistrict Litigation Master Complaint, citing Haugen_00008303 at 8307.
[51] Hristoya et al., "Why did we lose our snapchat streak?" Social media gamification and metacommunication. Computers in Human Behavior Reports, 5, 100172 (2022), available at https://www.sciencedirect.com/science/article/pii/S2451958822000069.
[52] MultiDistrict Litigation Master Complaint, citing SNAP0000008.
[53] Frazer Deans, *Curb Your Snapchat Addiction*, https://www.wholesome.design/advent-2018/2-curb-your-snapchat-addiction/.

profound body image issues in teenagers, especially girls. For example, in recent years, plastic surgeons have reported an increase in requests for altering surgeries that mimic Snapchat's filters. This has led researchers to coin the term "Snapchat Dysmorphia," in which the effect of Snapchat's filters triggers body dysmorphic disorder.[54]

FACEBOOK, TIKTOK, AND SNAP KNOW THEY ARE FACILITATING THE SALE OF DANGEROUS FENTANYL TO CHILDREN

Fentanyl was the cause of 77.14% of drug deaths among teenagers last year.[55]

The unprecedented spike of children dying from overdosing on fentanyl has been documented to be the fault of social media. According to, for example, *The New York Times* article titled **"Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar—** Teenagers and young adults are turning to Snapchat, TikTok and other social media apps to find Percocet, Xanax and other pills. The vast majority are laced with deadly doses of fentanyl, police say:"

- "Law enforcement authorities say an alarming portion of [fentanyl overdoses] unfolded … from counterfeit pills tainted with fentanyl that teenagers and young adults bought over social media."
- "'Social media is almost exclusively the way they get the pills," said Morgan Gire, District Attorney for Placer County, Calif., where 40 people died from fentanyl poisoning last year.
- "Overdoses are now the leading cause of preventable death among people ages 18 to 45, ahead of suicide, traffic accidents and gun violence, according to federal data.
- "**There are drug sellers on every major social media platform," one expert is quoted as saying…: As long as your child is on one of those platforms, they're going to have the potential to be exposed to drug sellers**."

Balancing Child Harm Prevention With User Engagement Doesn't Violate Section 230 of the Communications Decency Act.

First, Section 230 protects platforms in certain circumstances from being held liable for harms that are caused when they host content uploaded by third parties. But, the dopamine-hitting techniques that cause child addiction, such as "Likes" and "Streaks" and slot machine-like auto-

[54] Chen et al., Association Between Social Media and Photograph Editing Use, Self-esteem, and Cosmetic Surgery Acceptance, JAMA Facial Plastic Surgery, 2019; *See also* Nathan Smith & Allie Yang, What happens when lines blur between real and virtual beauty through filters? ABC NEWS (May 1, 2021), https://abcnews.go.com/Technology/lines-blur-real-virtual-beautyfilters/story?id=77427989.
[55] https://www.latimes.com/california/story/2022-11-12/more-teenagers-are-dying-from-fentanyl.

scrolling, as described above, are not content uploaded by third parties. They are the inventions of the platforms themselves and were, as conceded by their inventors, designed to be addictive all by themselves without reference to third party uploaded content. These are inventions of the platforms and are independently harmful and actionable apart from any content uploaded by third parties.

Second, as one of the friends of the court briefs filed *on behalf of Google* in the pending Section 230-related Supreme Court case of *Gonzalez v. Google* acknowledged, "**Where, as in a discrimination claim, the alleged basis for liability is the illegality of the platform's targeting and not the third-party content, immunity does not apply**."[56] Exactly. If this ability to hold platform's accountable for "targeting" was not the case then AI programmed in such a way as to offer products to Whites but not people of color would be cloaked by Section 230. As the Solicitor General has recently written in the same case: "Where a website operator's conduct in furthering unlawful activities goes well beyond failing to block or remove objectionable third-party content from its platform, holding the operator liable does not 'treat' it 'as the publisher or speaker of' the third party posts."[57]

As described in the red highlighted text above, when it comes to the child harm that is related to the content uploaded by third parties, some part of the harm in some cases will be attributable not to the substance of the content alone but also to ***the platform-AI's' automated decision to "target" content—whatever it might be —to children to get them to stay riveted to their products by any means necessary, no matter how utterly foreseeable the harmful consequences are to children, wholly uncaring of what the content might or might not express.***

Third, even if Section 230 could be successfully pleaded as a defense in a particular lawsuit based on the particular facts of that case, it would simply affect that particular action and not a regulation validity overall.

And fourth, in every other context, including where actors have absolute immunity, that veil can be pierced, but not so under Section 230 as the platforms would have it. They argue for the most absolute immunity found anywhere in our legal system. Consider qualified immunity, the most common kind. The doctrine of qualified sovereign immunity protects state and local officials, including law enforcement officers, from individual liability unless a reasonable person in the official's position would have known their actions were in line with clearly established legal principles.[58] In absolute immunity, even judges lose immunity when they are acting outside the role of being a judge or outside their jurisdiction as a judge.[59] Thus, even if "targeting" algorithmic recommendations were entitled to some Section 230 protection, should that extend to recommendations the platforms know are harmful to identifiable children like Molly Russell? In no other setting do we provide such immunity for knowing harms caused by a business on full purpose.

Balancing Child Harm Prevention With User Engagement Doesn't Violate Section The First Amendment.

Imagine a fully autonomous robot instructed to go out and (i) find children walking to school, (ii) roll up to them, and, (ii) using a megaphone known to blare at decibels harmful to the young, (iv) blast messages at full volume inches from the

[56] https://www.supremecourt.gov/DocketPDF/21/21-1333/252703/20230125100930536_4264_001.pdf at p. 20.
[57] https://www.supremecourt.gov/DocketPDF/21/21-1333/249441/20221207203557042_21-1333tsacUnitedStates.pdf at p. 19.
[58] *Harlow v. Fitzgerald* (1982) 457 U.S. 800.
[59] *Mireles v. Waco* (1991) 502 U.S. 9, 9-11.

ears of the children; permanently deafening some.

This is akin to what the platforms are doing. ***For the six reasons*** *below, to cause harm to children in such a fashion is not protected speech. In a lawsuit against the robot maker, the robot maker would not be able to raise a First Amendment defense to using machines in ways that the platform knows will physically deafen children -- period. That's because just because speech is part of a fact pattern of a lawsuit does not mean the lawsuit is about only that speech. Maybe the deafening content of the message could harm the child too ("Be skinnier! Eat less! Suicide is an option!") and that also might not be protected by the First Amendment. But, some part of the harm the robot caused can be attributed to the machine's conduct in targeting children and the conduct-decision to use technologies that will physically harm children.*

First, AI does not have speech rights. No 14th Amendment "person" (human or corporate) is involved in making the individual decisions or "speaking" the algorithm's output. The output produced by a recommendation algorithm is autonomous and not the product of human editorial decisions. The AI is writing the algorithms. For this reason, a regulation that protects children from single-minded user engagement is grounded in preventing harms in part caused by the operations of this autonomous, content-delivery machine does not run afoul of the First Amendment.

Second, machine learning, AI-written algorithms, and not persons, determine the content served to individual users, both for each user and all users. This targeting output from the AI is functional conduct, not expressive. Thus, in *Wisconsin v. Mitchell*,[60] the Supreme Court upheld as not violating the First Amendment, a criminal penalty enhancement statute that increased the punishment for a variety of crimes where the defendant targeted a victim because of one or more immutable characteristics, including race, religion, or ethnic background. The Court *treated the targeting at the heart of the statute* as a restriction only *on conduct*-- the selection of a victim based on his or her race, religion, or ethnic background—and not on speech.

Indeed, if causing the physical harm of addiction were protected by the First Amendment, every drug dealer would have a First Amendment right to cause drug addiction. So, too, would words that incited a physical fight be protected by the First Amendment, but they aren't. Words that have "a direct tendency to cause acts of violence by the person to whom, individually, the remark is addressed"[61]—words that are proven to cause physical harm—are not afforded blanket First Amendment protection. [62]

Third, courts have acknowledged that First Amendment rights of adults cannot be used as a rationale for endangering children. This is how child pornography—indisputably speech in the technical sense—is unprotected by the First Amendment.[63]

Fourth, a regulation balancing child harms against profit-driving "user engagement" would not be unconstitutional "on its face"; in every possible aspect or case. But the First Amendment doctrine that permits statutes to be struck down for being so overbroad as to be unenforceable in every aspect "does not apply to commercial speech."[64] And, here, even assuming AI's content

[60] (1993) 508 U.S. 476.
[61] *Gooding v. Wilson* (1972) 405 U.S. 518, 524.
[62] *Brown v. EMA* (2011) 564 U.S. 768, is thus distinguishable since the law there went after the speech itself and did not depend on the showing of any harm (i.e., conduct). Here, only algorithms that *cause* harmful addiction are proscribed. *See infra*.
[63] *New York v. Ferber* (1982) 458 U.S. 747, at https://mtsu.edu/first-amendment/article/404/new-york-v-ferber.
[64] *Village of Hoffman Estates v. Flipside*, 455 U.S. 489, 490 (2008).

delivery decisions are somehow protected speech, and even assuming commercial speech enjoyed the same protection from allegedly overbroad statutes as political speech, the supposed speech being allegedly chilled by the prospect of a regulation balancing automated targeting with child harm prevention would be speech that in court *has been proven to have physically harmed children in the awful ways.* In such a case, "there must be a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court for it to be facially challenged on overbreadth grounds."[65] Platforms will be hard-pressed to prove this.

Fifth, it is, in fact, very unlikely that if a platform were to try and invalidate a child protecting regulation just based on what it says, outside the context of an actual lawsuit brought by an actual harmed family, such a lawsuit would succeed. That is because such "facial" challenges to laws pressed outside of a lawsuit where someone is actually suing under the law are disfavored.[66]

Sixth, a child protecting regulation that would require balancing of user engagement and child is akin to a company being liable for putting a product on the street that causes harm to children. In the Ninth Circuit's recent case of *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021), an ideologically diverse panel of the Ninth Circuit permitted a negligent product design lawsuit to proceed against the social media platform Snapchat. Differentiating between expressive content uploaded by third parties and Snapchat's own inventions, the court ruled that: "The Parents thus allege a cause of action for negligent design—a common products liability tort. This type of claim rests on the premise that manufacturers have a "duty to exercise due care in supplying products that do not present an unreasonable risk of injury or harm to the public."[67] As this Committee observed last year: "The reasoning in *Lemmon v. Snap* is instructive, as liability here is not tied to content or speech, but the use of design and features that cause harm, regardless of the content underlying it. In addition, the bill furthers a compelling government interest, protecting children from addiction and emotional harm."[68]

QUESTION 4: What, if any, additional content should be included in risk assessments for processing that involves automated decisionmaking, including profiling? Why?

For the reasons set forth above, social media platforms at minimum must be required in their risk assessments to forecast harms to children from their addictive interfaces and user engagement-driven AI content targeting.

Respectfully submitted,

Ed Howard

[65] *Members of City Council of Los Angeles v. Taxpayers for Vincent* (1984) 466 U.S. 789, 801.
[66] *See*, e.g., *Wash. State Grange v. Wash. State Republican Party* (2008) 552 U.S. 442, where the Court noted that facial challenges "often rest on speculation," and it asserted that invalidating a statute before it takes effect could "short circuit the democratic process."), at https://supreme.justia.com/cases/federal/us/552/442/.
[67] *Id.* at 1092.
[68] Sen. Judic. Cmte. Analysis AB 2408 (2022) file:///C:/Users/eh4/Dropbox/Documents/Howard%20law%20offices%20and%20advocacy/CAI/2023/SKINNER%20BILL/202120220AB2408_Senate%20Judiciary.pdf at p. 17.

Senior Counsel, Children's Advocacy Institute (excerpt of recent lawsuit filed with this testimony)

EFiled: Mar 20 2023 04:59PM EDT
Transaction ID 69592713
Case No. 2023-0304-JTL

EXCERPTS IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

EMPLOYEES' RETIREMENT SYSTEM OF THE STATE OF RHODE ISLAND, KIWI INVESTMENT MANAGEMENT WHOLESALE CORE GLOBAL FUND, KIWI INVESTMENT MANAGEMENT GLOBAL QUANTITATIVE FUND, CLEVELAND BAKERS AND TEAMSTERS PENSION FUND, derivatively on behalf of META PLATFORMS, INC.,

Plaintiffs,

vs.

MARK ZUCKERBERG, SHERYL K. SANDBERG, PEGGY ALFORD, MARC L. ANDREESSEN, ANDREW W. HOUSTON, NANCY KILLEFER, ROBERT M. KIMMITT, TRACEY T. TRAVIS, TONY XU, ERSKINE B. BOWLES, KENNETH I. CHENAULT, SUSAN D. DESMOND-HELLMANN, REED HASTINGS, JAN KOUM, PETER THIEL, JEFFREY D. ZIENTS, ANDREW BOSWORTH, MIKE SCHROEPFER, CHRISTOPHER K. COX, DAVID M. WEHNER, NICK CLEGG, JENNIFER G. NEWSTEAD,

Defendants,

-and-

META PLATFORMS, INC.,

Nominal Defendant.

C.A. No. 2023-0304-JTL

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

PUBLIC VERSION DATED MARCH 20, 2023

TABLE OF CONTENTS

Page No.

GLOSSARY OF ABBREVIATIONS

Abbreviation	Description
AROC	Audit & Risk Oversight Committee
CEI	Child Exploitative/Exploitation Imagery
CNCEI	Child Nudity/Child Exploitative Images
CSAM	Child Sexual Abuse Material
DQ	Data Quality
FB	Facebook
FOSTA	Fight Online Sex Trafficking Act
GTM	Ground Truth Machine
HEx	Human Exploitation
IG	Instagram
MS	Minor Sexualization
MSGR	Facebook Messenger
SESTA	Stop Enabling Sex Traffickers Act
TVPA	Trafficking Victims Protection Act

Plaintiffs Employees' Retirement System of the State of Rhode Island, Kiwi Investment Management Wholesale Core Global Fund, Kiwi Investment Management Global Quantitative Fund, and Cleveland Bakers and Teamsters Pension Fund (collectively, "Plaintiffs"), by their undersigned attorneys, derivatively and on behalf of Nominal Defendant Meta Platforms, Inc. ("Meta" or the "Company"), file this Verified Shareholder Derivative Complaint against Defendants for breaches of fiduciary duty owed to the Company. Plaintiffs make the following allegations based upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters, based on the investigation conducted by their attorneys. This investigation included, among other things, a review of documents produced by Meta in response to books-and-records demands under 8 *Del. C.* § 220 made by Meta stockholders; the Company's conference calls, announcements and press releases; filings made by the Company with the U.S. Securities and Exchange Commission ("SEC"); whistleblower complaints filed with the SEC and published by national news media; corporate governance documents available on the Company's website; governmental and regulatory investigations of the Company and documents related thereto; judicial decisions by federal and state courts in criminal and civil lawsuits against or

discussing Meta; Congressional testimony; and news reports concerning the Company.[1]

NATURE OF THE ACTION

1. This case concerns the breaches by Meta's directors ("Board") and senior officers of their fiduciary duties with respect to the rampant and systemic sex trafficking, human trafficking, and child sexual exploitation flourishing on the Company's social media platforms, including Facebook and Instagram.

2. As described more fully below, Meta's directors and senior executives have been well aware for years that sex/human trafficking and child sexual exploitation were rampant on Facebook and Instagram. Senior officers, however, failed to exercise due care to root out these pernicious activities, and both the Company's officers and the Board failed to act in good faith to exercise oversight over the Company's social media platforms and the predatory criminal activity thriving on them.

3. In this shareholder derivative action, Plaintiffs, on behalf of Meta, seek to recover for the harm sustained by the Company as a result of the breaches of fiduciary duty by the Company's directors and officers.

[1] All emphasis herein (***bold/italics***) is added unless otherwise noted.

4. An accumulating mass of evidence shows that for the past decade, Meta's platforms have assisted, supported, and facilitated perpetrators of widespread systemic sex trafficking, human trafficking, and child sexual exploitation that has occurred on a massive scale on Meta's platforms in the United States and worldwide. The victims are Facebook and Instagram users—both minors and adults—whose lives are forever devastated. The perpetrators are often organized human trafficking "rings" that systematically use Meta's platforms to lure, recruit, exploit, and even advertise their victims for trafficking. Substantial evidence demonstrates that although the Board and management have known about this increasing trend, both management and the Board have consciously turned a blind eye to sex trafficking, human trafficking, and child sexual exploitation occurring on Meta's platforms. The conduct of Meta's Board and management is unconscionable; and in the face of this evidence, the Board's and management's utter failure to monitor or oversee this problem, to educate themselves about its scope, or even to discuss it ***in any meeting at all***—constitute breaches of their fiduciary duties to the Company and its shareholders.

5. As discussed below, evidence of widespread sex trafficking and other human trafficking on Meta's platforms, and of the Board's inadequate or nonexistent response to that trend, is overwhelming and well documented by numerous reliable sources.

6. ***First***, in October 2019, *BBC News Arabic* published the results of its undercover investigation which revealed that "[i]n Saudi Arabia, hundreds" of "women [were] being sold on Instagram, which is owned by Facebook" in what a United Nations official described as "promoting an online slave market" and "the quintessential example of modern slavery," and commented that "[i]f Facebook or any other companies are hosting apps like these, they have to be held accountable." In response, on October 23, 2019, Meta "received [a] communication from Apple" in which Apple "threatened to pull FB & IG apps from its App Store due to them identifying content promoting 'domestic servitude.'" According to Meta's internal records, management concluded that the Company had been "***underreporting this behaviour***"; suffered from an "***absence of proactive detection***"; that "***newly created and existing [domestic servitude] content [was] not captured***" which "***meant that domestic servitude content remained on the platform***"; had been "***under-enforcing on confirmed abusive activity with a nexus to the platform***"; and that internal "***investigative findings demonstrate that our platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks***. The traffickers, recruiters, and facilitators from these 'agencies' used FB profiles, IG profiles, Pages, Messenger, and WhatsApp."[2]

[2] *See* Section II.F *infra*.

7. ***Second***, a June 8, 2021 report by the Human Trafficking Institute found that the majority of online sex trafficking in 2020 occurred on Facebook and Instagram.[3] Similarly, a June 16, 2022 report by the same organization again found that the majority of sex trafficking occurs online with Facebook and Instagram together accounting for the majority of online sex trafficking in 2019, 2020, and 2021. Likewise, according to the U.S. State Department, "in 2018 trafficking gangs increasingly used social media sites, particularly Facebook, to buy and sell women and girls for sex and labor exploitation."[4]

8. ***Third***, between 2013 and 2023, U.S. federal and state courts have issued at least 70 written decisions in criminal and civil cases involving sex trafficking that occurred on Meta's platforms.[5] Between 2009 and 2022, U.S. newspapers and media outlets published at least 175 articles detailing how sex traffickers—often organized trafficking "rings"—have systematically used Meta's platforms (including Facebook, Facebook Messenger, Instagram, and WhatsApp) to commit heinous crimes.[6]

---

[3] *See* Section II.M *infra*.

[4] *See* Section II.K *infra*.

[5] *See* Section II.B *infra*. *See also* Exhibit 2.

[6] *See* Section II.A *infra*. *See also* Exhibit 1.

9. ***Fourth***, between 2012 and 2023, at least 129 federal and state courts issued written decisions in criminal and civil cases involving child sexual exploitation on Meta's platforms.[7] U.S. news and media outlets have also widely reported on the raging epidemic of child sexual exploitation occuring openly and unchecked on the Company's platforms. For example, in March 2022, a college professor described in *WIRED* magazine how her searching for "Facebook groups with names including 10, 11, or 12" concerning "the 10th, 11th, or 12th wards of the city of Pittsburgh" yielded dozens of "groups targeting children of those ages" with "over 81,000 members" openly soliciting children for sexual exploitation.[8] One 9,000-memer group appearing in the search results was named "Buscando novi@ de 9,10,11,12,13 años"—i.e., "[l]ooking for a 9-year-old girlfriend." Yet, when she "used Facebook's on-platform system" to report this group, an "automated response came back" stating "[t]he group had been reviewed and did not violate any 'specific community standards.'" And despite (or because of) her reporting this group, along with others, Facebook's AI algorithms caused "new child sexualization groups" to be "recommended to [her] as 'Groups You May Like.'"

[7] *See* Section II.C *infra*. *See also* Exhibit 3.

[8] *See* Section II.C *infra*.

10. ***Fifth***, in the midst of this trend, recent federal legislation, known as FOSTA-SESTA, clarified that internet service providers such as Meta can be held liable for intentionally facilitating sex trafficking on their platforms.[9] Indeed, a June 2021 decision by the Supreme Court of Texas held that Section 230 of the Communications Decency Act ("CDA"), 47 U.S.C. § 230, did not bar claims against Facebook by victims of sex trafficking under the Texas human trafficking statute.[10] The U.S. Supreme Court denied Facebook's petition for writ of certiorari on March 7, 2022.[11]

11. ***Sixth***, during 2018, 2019, and 2020, Mark Zuckerberg ("Zuckerberg")—Meta's co-founder, Chairman, Chief Executive Officer ("CEO"), and controlling shareholder—repeatedly testified before Congress and publicly discussed the subject of sex trafficking connected to Meta. The Company (and its Board) thus has been well aware of the increasing use of its platforms by sex traffickers and the devastating consequences for victims.[12]

---

[9] *See* Section I.C *infra*.

[10] *See* Section II.P *infra*.

[11] *See Doe v. Facebook, Inc.*, ("*Facebook Cert.*"), 142 S. Ct. 1087 (2022) (Thomas, J).

[12] *See* Sections II.D, II.E, II.G *infra*.

12. ***Seventh***, on September 16, 2021, *The Wall Street Journal* reported that "[s]cores of internal Facebook documents" revealed that although Facebook employees had flagged human traffickers using its network, the Company's response had been "[w]eak," "inadequate or ***nothing at all***."[13] For example, said employees concluded that "Facebook products facilitated each step" of a "bustling human-trafficking trade in the Middle East," which "criminal networks recruit[ed] people from poor countries, coordinat[ed] their travel and pu[t] them into . . . forced sex work in the United Arab Emirates and other Persian Gulf countries." In another example, Facebook employees discovered a large sex trafficking "ring that used the site to recruit women from Thailand and other countries. They were held captive, denied access to food and forced to perform sex acts in Dubai massage parlors, according to an internal investigation report. Facebook removed the posts but didn't alert local law enforcement."

13. ***Eighth***, on October 3, 2021, former Facebook employee Frances Haugen appeared on the broadcast *60 Minutes*. On October 4, 2021, CBS's *60 Minutes* published eight whistleblower complaints that Ms. Haugen filed with the SEC, one of which alleged that Meta "misled investors and the public about its promotion of human trafficking / slavery / servitude."[14] One of the internal

[13] *See* Section II.Q *infra*.

[14] *See* Section II.R *infra*.

documents that Ms. Haugen provided to the SEC, dated October 2019, discussed "human trafficking" occurring on Meta's various platforms in the form of "domestic servitude" and "human exploitation."

14. ***Ninth***, in response to Plaintiffs' books-and-records demands pursuant to 8 *Del. C.* §220, Meta produced Board-level documents revealing, among other things, that the Board has acknowledged [redacted] as one of the [redacted] the Company did not yet [redacted] and for which [redacted] but did not [redacted] [15]

15. ***Tenth***, despite publicly stating that "[w]e deploy technology across all of our platforms to proactively surface illegal child exploitative content as we can, including through detection technology, machine learning and artificial intelligence techniques,"[16] Meta's documents reveal that it internally acknowledged to the Board that the [redacted]

[15] *See* Part III *infra*.

[16] *See* Section II.J *infra*.

[17] *See* Section III.J *infra*.

[redacted]

16. ***Eleventh***, in response to Plaintiffs' books-and-records demands pursuant to 8 *Del. C.* § 220, Meta agreed to "search for materials provided to the Board ***and Board minutes*** since January 1, 2017 relating to the two topics of (i) sex and human trafficking and (ii) teen health, including excerpts of minutes of meetings of the Board (or committees of the Board) that reflect discussion of those two subjects" and to "produce … any non-privileged materials and information identified as a result of that search."[19] Meta also "certifie[d]" in writing to Plaintiffs that its "production" of the "materials that Meta agreed to produce" was "now complete."[20] Yet, despite producing other Board-level documents relating to these topics (which are discussed herein), Defendants conspicuously ***failed to produce any minutes whatsoever*** of any meeting of either the Board, the Audit Committee, or any other committee of the Board. The obvious—and only—inference is that neither the

[18] *See* Section III.M *infra*.

[19] Letter from David E. Ross to William S. Norton (Dec. 14, 2021) at 4.

[20] Letter from David E. Ross to Christine M. Mackintosh (May 20, 2022) at 1.

Board nor the Audit Committee have ever even discussed these topics at all—or at least to an extent that merited noting the discussion in any meeting's minutes.

17. ***Twelfth***, while Meta did produce some Board-level documents discussing the Company's [redacted]—conspicuously absent from Meta's § 220 document production was any material evidence or discussion of what, if anything, the Board, its committees, or Meta's management have done to detect, prevent, deter, or address ***sex trafficking*** or ***human trafficking*** as such on the Company's platforms, or what oversight the Board performed as to these mission-critical risks.

18. Rather, Meta's documents suggest it has consciously chosen to avoid defining "human trafficking" as comprising "sex trafficking." Meta's 2021 "Anti-Slavery and Human Trafficking Statement" does not even mention "sex trafficking." And whereas Meta's 2020 "Anti-Slavery and Human Trafficking Statement" had stated that "[w]e define human trafficking as the exploitation of humans in order to force them to engage in commercial sex, labor, or other activities against their will," and claimed that "we remove content on Facebook that facilitates or coordinates the exploitation of humans, including human trafficking"—Meta's Board approved and ***deleted*** this very same language from similar 2021 and 2022 statements. Clearly, the Board gave up even claiming to remove content relating to or discussing sex trafficking.

19. In sum, when the overwhelming evidence of criminal sex/human trafficking on Meta's platforms is considered together with Meta's failure to produce any Board (or committee) minutes discussing sex/human trafficking, alongside Meta's failure to produce any Board-level documents discussing whether or how the Company has sought to detect, disrupt, prevent, or address sex/human trafficking on its platforms—the only logical inference is that the Board has consciously decided to permit Meta's platforms to promote and facilitate sex/human trafficking.

20. A critical tenet of Delaware corporate law is that Delaware corporations may only pursue "lawful business" by "lawful acts." 8 *Del. C.* §§ 101(b), 102.[21] In passing FOSTA-SESTA, Congress reaffirmed that online service providers such as Meta cannot consciously promote or facilitate unlawful sex trafficking, human trafficking, or child sexual exploitation on their interactive computer platforms without themselves breaking the law. And a Delaware fiduciary cannot be loyal to a Delaware company while causing it to break the law—particularly when the category of crimes being facilitated involves commercial sex acts induced by force,

[21] "Delaware law does not charter law breakers. Delaware law allows corporations to pursue diverse means to make a profit, subject to a critical statutory floor, which is the requirement that Delaware corporations only pursue 'lawful business' by 'lawful acts.' As a result, a fiduciary of a Delaware corporation cannot be loyal to a Delaware corporation by knowingly causing it to seek profit by violating the law." *In re Massey Energy Co. Derivative & Class Action Litig.*, 2011 WL 2176479, at *20 (Del. Ch. May 31, 2011) (quoting Del. Code § 101(b) and § 102).

fraud, coercion, and abuse—both of adults and minors; involuntary servitude, peonage, debt bondage, slavery; and child sexual exploitation—all on a mass scale. Meta's Board and management have utterly failed to act in good faith to assure the existence of a functioning Board-level system of monitoring and reporting to prevent such heinous conduct, and by consciously failing to monitor or oversee whether management was addressing the endemic scourge of sex trafficking and human trafficking that has lived *and grown* for years on Meta's platforms.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to 10 *Del. C.* § 341 and has personal jurisdiction over Defendants, who are current or former directors and officers of Meta, pursuant to 10 *Del. C.* § 3114. This Court also has jurisdiction over Nominal Defendant Meta, a Delaware corporation, pursuant to 10 *Del. C.* § 3111.

PARTIES

A. Plaintiffs

22. Plaintiff Employees' Retirement System of the State of Rhode Island is a Meta shareholder and has continuously owned shares of the Company's common stock since March 31, 2017.

23. Plaintiff Cleveland Bakers and Teamsters Pension Fund is a Meta shareholder and has continuously owned shares of the Company's common stock since October 10, 2016.

24. Plaintiff Kiwi Investment Management Wholesale Core Global Fund is a Meta shareholder and has continuously owned shares of the Company's common stock since July 18, 2017.

25. Plaintiff Kiwi Investment Management Global Quantitative Fund is a Meta shareholder and has continuously owned shares of the Company's common stock since October 25, 2018.

B. Nominal Defendant

26. Nominal Defendant Meta is a Delaware corporation with its principal executive offices located at 1601 Willow Road, Menlo Park, California. Meta's common stock is traded on the NASDAQ exchange under the ticker symbol "META." The Company operates various technology and social media products, including Facebook, Instagram, and WhatsApp.

C. Current Company Director Defendants

27. Defendant Zuckerberg is Meta's founder and has served as its CEO since 2004 and as Chairman of the Board since 2012. As CEO, Zuckerberg is responsible for Meta's day-to-day operations, overall direction and company strategy. Zuckerberg is also Meta's controlling stockholder; specifically, as of

March 31, 2022, Zuckerberg controlled 54.4% of Meta's "Total Voting Power" through his ownership of 84.7% of Meta's Class B shares.[22]

28. Defendant Sheryl K. Sandberg ("Sandberg") served as the Company's Chief Operating Officer from March 2008 until August 2022. Sandberg has served as a Company director since June 2012.

29. Defendant Peggy Alford ("Alford") has served as a Company director since May 2019. Alford has been a member of the Board's Audit Committee[23] since April 2020, chairman of the Board's Compensation Committee[24] since May 2022, and a member of the Board's Privacy Committee from May 2020 until May 2022.

30. Defendant Marc L. Andreessen ("Andreessen") has served as a Company director since June 2008. Andreessen has been a member of the Board's Compensation Committee at all times relevant to the Complaint, and the Board's Audit Committee from at least 2013 until February 2021.

---

[22] Meta, Proxy Statement (Form DEF 14A) at 62 (Apr. 8, 2022).

[23] In June 2018, the Board amended the charter of the Audit Committee and renamed it as the "Audit & Risk Oversight Committee." References to the "Audit Committee" include the Audit & Risk Oversight Committee after June 2018.

[24] In October 2019, the Board amended the charter of the Compensation & Governance Committee and renamed it as the "Compensation, Nominating & Governance Committee." References to the "Compensation Committee" include the Compensation Nominating & Governance Committee after October 2019 and the Compensation & Governance Committee prior to October 2019.

31. Defendant Andrew W. Houston ("Houston") has served as a Company director since February 2020. Houston has served as a member of the Board's Compensation Committee since April 2020.

32. Defendant Nancy Killefer ("Killefer") has served as a Company director since March 2020. Killefer has served as chairman of the Board's Privacy Committee since May 2020, and as a member of the Board's Audit Committee since February 2021.

33. Defendant Robert M. Kimmitt ("Kimmitt") has served as a Company director since March 2020. Kimmitt has served as a member of the Board's Privacy Committee since May 2020.

34. Defendant Tracey T. Travis ("Travis") has served as a Company director since March 2020. Travis has been a member of the Board's Audit Committee since March 2020, and chairman of that committee since at least May 2021.

35. Defendant Tony Xu ("Xu") has served as a Company director since January 2022. Xu has been a member of the Board's Compensation Committee since February 2022.

36. Zuckerberg, Sandberg, Alford, Andreessen, Houston, Killefer, Kimmitt, Travis, and Xu are referred to collectively as "Director Defendants" and the "Demand Board."

D. Former-Director Defendants

37. Defendant Erskine B. Bowles ("Bowles") served as a Company director from September 2011 to May 2019. Bowles was chairman of the Board's Audit Committee until May 2019.

38. Defendant Kenneth I. Chenault ("Chenault") served as a Company director from February 2018 to May 2020. Chenault was a member of the Board's Audit Committee from May 2018 until May 2020.

39. Defendant Susan D. Desmond-Hellmann ("Desmond-Hellmann") served as a Company director from March 2013 to October 2019. Desmond-Hellmann served on the Board's Audit Committee from 2014 until May 2019, and as chairman of the Board's Compensation Committee from May 2019 to October 2019.

40. Defendant Reed Hastings ("Hastings") served as a Company director from June 2011 to May 2019. Hastings was chairman of the Board's Compensation Committee from 2016 to May 2019.

41. Defendant Jan Koum ("Koum") is the co-founder and former CEO of WhatsApp, and served as a Company director from October 2014 until April 2018.

42. Defendant Peter Thiel ("Thiel") served as a Company director from April 2005 until May 2022. Thiel served as a member of the Board's Compensation

Committee from 2015 until October 2019, and as that committee's chairman from October 2019 until May 2022.

43. Defendant Jeffrey D. Zients ("Zients") served as a Company director from May 2018 to May 2020. Zients was chairman of the Board's Audit Committee from May 2019 to May 2020.

44. Bowles, Chenault, Desmond-Hellmann, Hastings, Koum, Thiel, and Zients are referred to herein as the "Former-Director Defendants."

E. Executive Officer Defendants

45. Defendant Andrew Bosworth ("Bosworth") has been the Company's Chief Technology Officer ("CTO") since March 2022. Bosworth has been with the Company since 2006 when he created Facebook's News Feed. He served as the Company's Vice President for Reality Labs, overseeing the Company's augmented reality, virtual reality, and artificial intelligence products from 2017 until he became CTO in March 2022.

46. Defendant Mike Schroepfer ("Schroepfer") served as the Company's CTO from 2013 until March 2022.

47. Defendant Nick Clegg ("Clegg") is the Company's President of Global Affairs. Clegg joined the Company in October 2018 as Vice President of Global Affairs and Communications and was promoted to his current position in February 2022. Clegg was heavily involved in creating the Company's content oversight

board, and now leads the Meta's efforts on all policy matters and government interactions on policy implementation, according to Zuckerberg's Facebook post announcing Clegg's 2022 promotion.

48. Defendant Christopher K. Cox ("Cox") has served as the Company's Chief Product Officer from 2014 to March 2019 before stepping away to explore various climate change initiatives and contribute to several political causes. Cox resumed his role as Chief Product Officer in June 2020.[25]

49. Defendant Jennifer G. Newstead ("Newstead") has served as the Company's Chief Legal Officer since April 2019.

50. Defendant David M. Wehner ("Wehner") served as the Company's Chief Financial Officer from June 2014 until November 1, 2022, when he became the Chief Strategy Officer.

51. Defendants Bosworth, Schroepfer, Clegg, Cox, Newstead, and Wehner are referred to herein as "Officer Defendants." The term "Officer Defendants" includes Defendants Zuckerberg and Sandberg for purposes of claims asserted against the Officer Defendants, as Defendants Zuckerberg and Sandberg breached fiduciary duties both in their capacities as directors and in their capacities as officers of Meta.

[25] Cox left the Company to pursue other interests in March 2019 and resumed his role as Chief Product Officer in June 2020.

PLAINTIFFS' DEMAND TO INSPECT META'S BOOKS AND RECORDS

52. As part of Plaintiffs' thorough pre-suit investigation, Plaintiffs each sought inspection of certain books and records of the Company pursuant to 8 *Del. C*. § 220 ("Section 220").

53. On December 7, 2021, ERSRI served Meta with a demand for the inspection of books and records relating to, *inter alia*, sex trafficking, human trafficking, and content harmful to children and teenagers occurring on Meta's social media platforms.

54. In response to ERSRI's books-and-records demand pursuant to Section 220, Meta agreed by letter dated December 14, 2021, to produce any non-privileged materials and information identified in their search for "materials provided to the Board and Board minutes since January 1, 2017 relating to the two topics of (i) sex and human trafficking and (ii) teen health, including excerpts of minutes of meetings of the Board (or committees of the Board) that reflect discussion of those two subjects "[26]

55. On May 26, 2022, the Kiwi Funds served Meta with a demand for the inspection of books and records relating to the use of the Company's social media platforms for human trafficking and sex trafficking. Meta agreed to produce to the

[26] *See* Letter from David E. Ross to William S. Norton, *supra* note19, at 4.

Kiwi Funds the same documents as it had provided to ERSRI. By letter dated June 8, 2022, Meta certified that "its production of the non-privileged materials that Meta agreed to produce [to the Kiwi Funds] is ***now complete***."

56. On January 23, 2023, Cleveland Bakers served Meta with a demand for the inspection of books and records relating to the use of the Company's social media platforms for human trafficking and sex trafficking.

57. In response to Cleveland Bakers' books-and-records demand pursuant to Section 220, Meta agreed, by letter dated January 30, 2023, to produce the same materials it had agreed to produce to ERSRI.

58. By letter dated May 20, 2022, Meta certified that "its production of the non-privileged materials that Meta agreed to produce [to ERSRI] is ***now complete***."[27]

59. The Company's own documents—and the lack thereof—show that the Board, including each of its committees, failed to discuss (even once) the use of the Company's social media platforms for sex trafficking and human trafficking. The Board and its committees also failed to discuss the issue of child sexual exploitation occurring on Meta's platforms. These failures were despite global awareness and

[27] *See* Letter from R. Garrett Rice to Christine M. Mackintosh, *supra* note 20, at 1.

concern with these issues as detailed in Plaintiffs' 220 demands, shareholder proposals detailed in Meta's proxy statements, and as alleged herein.

60. Meta's books and records, along with other information obtained by Plaintiffs through their investigation, evidence the fact that Meta's Board failed to engage in any meaningful oversight relating to the harm to the victims of human and sex trafficking through the use of the Company's social media platforms, or the risk to the Company created by such use of its platforms.

SUBSTANTIVE ALLEGATIONS

I. LEGAL BACKGROUND ON SEX/HUMAN TRAFFICKING

A. The Trafficking Victims Protection Act of 2000

61. Sex trafficking and human trafficking are crimes under U.S. federal and state law. The Trafficking Victims Protection Act of 2000 ("TVPA") and its subsequent reauthorizations define two primary forms of human trafficking: "sex trafficking" and "forced labor":

- Sex trafficking is the recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a person for the purpose of a commercial sex act in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age. (22 U.S.C. § 7102(11)(A)).

- Forced labor is the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery. (22 U.S.C. § 7102(11)(B)).

62. To strengthen penalties for those who engage in sex trafficking, the TVPA created 18 U.S.C. § 1591, which makes "sex trafficking" a crime and defines the offense as follows:

> (a) Whoever knowingly—
>
> > (1) in or affecting interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, recruits, entices, harbors, transports, provides, obtains, advertises, maintains, patronizes, or solicits by any means a person; or
> >
> > (2) benefits, financially or by receiving anything of value, from participation in a venture which has engaged in an act described in violation of paragraph (1),
> >
> > > knowing, or, except where the act constituting the violation of paragraph (1) is advertising, in reckless disregard of the fact, that means of force, threats of force, fraud, coercion described in subsection e(2), or any combination of such means will be used to cause the person to engage in a commercial sex act, or that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act, shall be punished as provided in subsection (b).

18 U.S.C. § 1591(a). A violator of Section 1591 is subject to a statutory fine and a term of imprisonment ranging from "not less than 10 years" to "for life." 18 U.S.C. § 1591(b). In 2003, Congress authorized victims of sex trafficking to file civil actions. 18 U.S.C. § 1595.

63. The U.S. Department of Justice ("DOJ") has described human trafficking (as defined in the TVPA) as "a crime involving the exploitation of a person for labor, services, or commercial sex."[28]

64. The U.S. Department of State (the "State Department") has decried human trafficking as "a grave crime and a human rights abuse":

> Human trafficking, also called trafficking in persons, has no place in our world. As both a grave crime and a human rights abuse, it compromises national and economic security, undermines the rule of law, and harms the well-being of individuals and communities everywhere. It is a crime of exploitation; traffickers profit at the expense of their victims by compelling them to perform labor or to engage in commercial sex in every region of the United States and around the world. With an estimated 24.9 million victims worldwide at any given time, human traffickers prey on adults and children of all ages, backgrounds, and nationalities, exploiting them for their own profit.[29]

65. The U.S. Department of Defense ("DOD") states that "[t]raffickers prey on victims with little or no social safety net." Particular vulnerabilities associated with trafficking victims, according to the DOD, include "poverty or economic hardship, political instability or armed conflict, natural disasters, childhood abuse or neglect, children in foster care, runaway and homeless youth, victims of violence, migrant workers, undocumented immigrants, racial, ethnic, and

---

[28] https://www.justice.gov/humantrafficking.

[29] https://www.state.gov/humantrafficking-about-human-trafficking/.

other minorities, physical or cognitive abilities, history of substance abuse, and LGBTQ individuals."[30]

66. The U.S. Department of Homeland Security ("DHS") describes human trafficking as conduct involving "the use of force, fraud, or coercion to obtain some type of labor or commercial sex act."[31] The DHS states that traffickers may use the following methods to lure victims into trafficking situations: violence, manipulation, false promises of well-paying jobs, and romantic relationships.

B. Section 230 of the Communications Decency Act

67. Since its enactment in 1996, Section 230 of the CDA has often been used by social media companies to avoid liability for the conduct of third parties occurring on its platforms. Section 230 states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (47 U.S.C. § 230). However, Section 230 does ***not*** protect providers from criminal liability if their content violated criminal laws concerning "sex trafficking" or "sexual exploitation of children":

> **(e) EFFECT ON OTHER LAWS**
>
> **(1) NO EFFECT ON CRIMINAL LAW**

[30] https://ctip.defense.gov/What-is-TIP/.

[31] https://www.dhs.gov/blue-campaign/what-human-trafficking.

> Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.
>
> ***
>
> **(5) NO EFFECT ON SEX TRAFFICKING LAW**
>
> Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit –
>
> > **(A)** any claim in a civil action brought under section 1595 of title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title;
> >
> > **(B)** any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of title 18; or
> >
> > **(C)** any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

47 U.S.C. § 230(e)(1) and (5); *see also* 18 U.S.C. Chapter 110 (18 U.S.C. §§ 2251-2260A) (Sexual Exploitation and Other Abuse of Children); 18 U.S.C. §§ 1591, 1595.

C. FOSTA-SESTA (April 11, 2018)

68. On April 11, 2018, the President signed the Fight Online Sex Trafficking Act[32] ("FOSTA") and the Stop Enabling Sex Traffickers Act[33] ("SESTA") (together "FOSTA-SESTA"), which clarified the country's sex trafficking laws by making it illegal to knowingly assist, support, or facilitate sex trafficking. FOSTA-SESTA made changes to three statutory schemes: the CDA, the TVPA (discussed above); and the Mann Act, 18 U.S.C. § 2421 *et seq*.

69. ***First***, the law amended the safe harbor provisions of Section 230 of the CDA, 47 U.S.C. § 230—which courts had previously interpreted as giving internet service providers (like Meta) immunity from civil liability for the actions of their users—to exclude the enforcement of federal or state sex trafficking laws from Section 230's safe harbors.

70. Section 2 of both acts provides, in part, that "[S]ection 230 was never intended to provide legal protection to websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[34] Congress

---

[32] Pub. L. No. 115-164, 132 Stat. 1253 (2018).

[33] S. 1693, 115th Cong. (2018).

[34] FOSTA, § 2(1); S. 1693 § 2. In passing FOSTA, Congress "narrow[ed] Section 230's scope and provide[d] prosecutors with new tools to combat the sex trafficking of ***both minors and adults***." *Woodhull Freedom Found. v. United States*, 948 F.3d 363, 368 (D.C. Cir. 2020).

clarified and amended Section 230 to ensure that it does not "provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[35] FOSTA-SESTA amended Section 230 by adding that "[n]othing in [Section 230] (other than subsection (c)(2)(A)) shall be construed to impair or limit any claim in a civil action brought under section 1595 of title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title." 47 U.S.C. § 230(5). *See* § I.B *supra* (quoting full text of 47 U.S.C. § 230(5)).

71. ***Second***, as to the Mann Act, FOSTA proscribed "own[ing], manag[ing], or operat[ing] an interactive computer service with the intent to promote or facilitate the prostitution of another person," as punishable by a fine and imprisonment for not more than ten years. FOSTA, § 3(a), 132 Stat. at 1253–54 (codified at 18 U.S.C. § 2421A(a)). This provision adopts the definition of "interactive computer service" in Section 230(f) of the CDA. 18 U.S.C. § 2421A(a). When the underlying conduct "promotes or facilitates the prostitution of 5 or more persons" or when the person "acts in reckless disregard of the fact that such conduct contributed to sex trafficking," there is an enhanced penalty of imprisonment for not more than twenty-five years. *Id.* § 2421A(b). An individual injured by such an

[35] FOSTA, § 2(1).

aggravated violation may sue for money damages. *Id.* § 2421A(c). Specifically, 18 U.S.C. § 2421A provides:

IN GENERAL.—

> **(a)** Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, ***owns, manages, or operates an interactive computer service*** (as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f))), ***or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person*** shall be fined under this title, imprisoned for not more than 10 years, or both.
>
> **(b) AGGRAVATED VIOLATION.**—Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, ***owns, manages, or operates an interactive computer service*** (as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f))), ***or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person and—***
>
> > **(1)** ***promotes or facilitates the prostitution of 5 or more persons***; ***or***
> >
> > **(2)** ***acts in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of [section] 1591(a),***
>
> ***shall be fined under this title, imprisoned for not more than 25 years, or both***.
>
> **(c) CIVIL RECOVERY.—**
> Any person injured by reason of a violation of section 2421A(b) may recover damages and reasonable attorneys' fees in an action before any appropriate United States district court.
>
> **(d) MANDATORY RESTITUTION.—**
> Notwithstanding sections 3663 or 3663A and in addition to any other civil or criminal penalties authorized by law, the court shall order restitution for any violation of subsection (b)(2). The scope and nature of such restitution shall be consistent with section 2327(b).

18 U.S.C. § 2421A.

72. ***Third***, with respect to the TVPA, FOSTA-SESTA added a provision to 18 U.S.C. § 1595 authorizing state attorneys general to bring *parens patriae* civil actions against any person who violates section 1591. Specifically, 18 U.S.C. § 1595 provides:

> **(a)** An individual who is a victim of a violation of this chapter may bring a civil action against the perpetrator (or whoever knowingly benefits, financially or by receiving anything of value from participation in a venture which that person knew or should have known has engaged in an act in violation of this chapter) in an appropriate district court of the United States and may recover damages and reasonable attorneys fees.
>
> **(b)**
>
> > **(1)** Any civil action filed under subsection (a) shall be stayed during the pendency of any criminal action arising out of the same occurrence in which the claimant is the victim.
> >
> > **(2)** In this subsection, a "criminal action" includes investigation and prosecution and is pending until final adjudication in the trial court.
>
> **(c)** No action may be maintained under subsection (a) unless it is commenced not later than the later of—
>
> > **(1)** 10 years after the cause of action arose; or
> >
> > **(2)** 10 years after the victim reaches 18 years of age, if the victim was a minor at the time of the alleged offense.
>
> **(d)** ***In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates section 1591, the attorney general of the State, as parens patriae, may bring a civil action against such person on behalf of the residents of the State in an appropriate district court of the United States to obtain appropriate relief.***

18 U.S.C. § 1595.

73. Along with revising section 1595, Section 230(e)(5)(A) of the CDA now provides that nothing within the CDA shall be construed to limit or impair "any claim in a civil action brought under section 1595 of [the TVPA] if the conduct underlying the claim constitutes a violation of section 1591 of that title." 47 U.S.C. § 230(e)(5).

D. 11 *Del. C.* § 787(b)(2) (Trafficking an Individual)

74. In addition to being a federal crime, "trafficking an individual" is also a crime under the laws of the state of Delaware. *See* 11 *Del. C.* § 787(b)(2). "A person is guilty of trafficking an individual if the person knowingly recruits, transports, harbors, receives, provides, obtains, isolates, maintains, advertises, solicits, or entices an individual in furtherance of ***forced labor*** in violation of paragraph (b)(2) of this section or ***sexual servitude*** in violation of paragraph (b)(3) of this section." 11 *Del. C.* § 787(b).[36]

[36] *See also* 11 *Del. C.* § 787(b)(2) ("A person is guilty of ***forced labor*** if the person knowingly uses coercion to compel an individual to provide labor or services, except where such conduct is permissible under federal law or law of this State other than 79 Del. Laws, c. 276."); 11 *Del. C.* § 787(b)(3) ("Sexual servitude. — a. A person commits the offense of ***sexual servitude*** if the person knowingly: 1. Maintains or makes available a minor for the purpose of engaging the minor in commercial sexual activity; or 2. Uses coercion or deception to compel an adult to engage in commercial sexual activity.").

II. META HAS FACILITATED AND ENABLED WIDESPREAD SEX TRAFFICKING AND HUMAN TRAFFICKING

A. 2009-2022 – Reports of Sex/Human Trafficking and Exploitation on Meta's Platforms Permeate the U.S. News

75. Meta's widespread and ubiquitous facilitation of sex trafficking and human trafficking have been reported in more than 175 articles published in U.S. newspapers and other media outlets between 2009 and 2022. This non-exhaustive selection of news articles is summarized (in chronological order) in Exhibit 1. These articles reported how human traffickers have repeatedly used Meta's platforms to commit their crimes against hundreds (and most likely thousands) of victims in the United States alone, and innumerable more victims worldwide. In several articles, Meta's spokespersons commented on these reports of sex trafficking and human trafficking.

76. For example, on October 29, 2012, *The Associated Press* reported that "***[s]o far this year, 27 of the 129 children reported missing to Indonesia's National Commission for Child Protection are believed to have been abducted after meeting their captors on Facebook***" and that "***[t]he 27 Facebook-related abductions reported to the commission this year in Indonesia have already exceed[ed] 18 similar cases it received in all of 2011***."[37] The article described how these "Facebook-related abductions" are committed by "sexual predators" involved in

[37] *See* Exhibit 1 at 5.

"child sex tourism" in which children as young as 14 or 15 are subjected to "kidnap and rape" and are "forced into prostitution." This same article quoted a Facebook "spokesman Andrew Noyes" who "said in an email" that "[w]e take human trafficking very seriously and a number of measures are in place to counter this activity," but Mr. Noyes "declined to give any details on Facebook's involvement in trafficking cases reported in Indonesia or elsewhere."[38]

77. Similarly, on January 8, 2015, the *Grand Forks Herald* reported on "a sex trafficking conference" at which an "Assistant U.S. Attorney" described a case regarding "a Minnesota man now serving 12 years in federal prison" who "engaged in 800 Facebook chat conversations with, most of the time, 14-to 17-year-old girls" with the intent to "sexually exploit them."[39] The same article quoted "Facebook's Monika Bickert" who "acknowledged how sites like hers can be attractive to pimps for recruiting victims and then threatening or coercing them, or to arrange transactions." The article further noted that "Bickert, head of global policy management with [Facebook]" acknowledged that such criminals "feel the Internet is a really powerful tool for them."

[38] *Id.*

[39] *Connect In A Click*, GRAND FORKS HERALD (Jan. 8, 2015).

78. On October 25, 2021, *Tampa Bay Times* published an article reporting that "[a]fter publicly promising to crack down, Facebook acknowledged in internal documents obtained by The Associated Press that it was 'under-enforcing on confirmed abusive activity.'"[40] The author further states that "[e]ven today, a quick search for 'khadima,' or 'maids' in Arabic, will bring up accounts featuring posed photographs of Africans and South Asians with ages and prices listed next to their images." The author further notes that "[i]n the documents seen by the AP, Facebook acknowledges being aware of both the exploitative conditions of foreign workers and the use of Instagram to buy and trade maids online [but] Facebook acknowledged it only scratched the surface of the problem and that 'domestic servitude content remained on the platform.'"

79. On October 28, 2021, *USA Today* published an article stating that an internal Facebook report uncovered "a U.S. sex trafficking network recruiting women from overseas and advertising illegal sexual services in domestic massage parlors."[41] The article reported that certain individuals "***used dozens of Facebook***

[40] Associated Press, *Apple once threatened Facebook ban over Mideast maid abuse; Facebook acknowledged some countries across the region have 'especially egregious' human rights issues when it comes to laborers' protection*, TAMPA BAY TIMES (Oct. 25, 2021), available at https://www.tampabay.com/news/nation-world/2021/10/25/apple-once-threatened-facebook-ban-over-mideast-maid-abuse/.

[41] Cara Kelly, *Facebook failed to rid site of sex trafficking; Papers show company knew it was profiting from illicit spas*, USA Today (Oct. 28, 2021).

pages and accounts to promote [sex work] parlors and relied on two marketing firms, one in the U.S. and one in India, to buy Facebook ads filled with keywords for potential sexual services." The author quotes Maggy Krell, who worked on sex trafficking cases as a supervising deputy attorney general in California, who said "'Facebook can't stick its head in the sand,' '[o]nce on notice that its site is being used to traffic someone, they must act.'" The article further states that "***[a] review of the internal documents reveals Facebook has known its products were part of the life cycle of human trafficking for more than three years***," but that Meta "focused" on "'soft actions,' or anything short of moving content from Facebook platforms."

80. On August 30, 2022, *FOX – 4 WDAF* in Kansas City, Missouri, published an article reporting that "[a]n alleged sex-trafficker may have preyed upon hundreds of fellow women over the course of a decade," and that "[d]uring their investigation, agents discovered more than 1,600 online ads associated with Gomez allegedly promoting prostitution" on Facebook, dating back ten years.[42]

B. 2013-2022 – Criminal/Civil Cases Involving Sex/Human Trafficking on Meta's Platforms Are Routine in U.S. Courts

81. Between 2013 and 2023, at least 70 federal and state courts issued written decisions in criminal and civil cases involving sex trafficking and human

[42] Aaron Feis, *Alleged sex-trafficker may have hundreds of victims, FBI says*, FOX–4 WDAF (Aug. 30, 2022).

trafficking on Meta's platforms. These decisions are listed in reverse chronological order and summarized in Exhibit 2. While these selected cases are believed to be merely a sample of the larger number of incidents of sex trafficking and human trafficking facilitated by Meta's platforms, including a larger number of criminal prosecutions involving sex trafficking linked to the Company, it is clear that such cases have occurred with increasing frequency in recent years. More appear each week.

82. In several cases, courts found that the evidence supported probable cause to issue search warrants to search the Facebook accounts of defendants and/or victims for evidence of sex trafficking occurring on Meta's platforms.[43]

---

[43] *See, e.g.*, *United States v. Wilkins*, No. CR 19-390 (RC), 2021 WL 1894990, at *22, *28 (D.D.C. May 11, 2021) (denying motion to suppress evidence obtained from a "warrant issued to Facebook for [an] Instagram account" and finding "that probable cause existed to search the account for evidence of sex trafficking"); *People v. McGraw*, No. F078342, 2020 WL 5569579, at *1 (Cal. Ct. App. Sept. 17, 2020) (finding "evidence . . . was sufficient to establish probable cause that defendant committed human trafficking" where criminal investigator's "testimony . . . was based primarily on text messages and Facebook communications," including "several Facebook profiles linked to defendant"); *United States v. Vines*, No. 1:17-CR-00160-JRS-TAB, 2018 WL 5634361, at *1, *4, *5 (S.D. Ind. Oct. 31, 2018) (following "indictment charging [defendant] with sex trafficking of a child," denying motion to suppress search warrant; finding "probable cause for search of [defendant's] Facebook" account; and noting that "[t]he government routinely checks social media in sex trafficking cases"); *United States v. Mathis*, No. 18-CR-18(1) (DWF/LIB), 2018 WL 4473529, at *1, *9 (D. Minn. July 17, 2018), report and recommendation adopted, No. CR 18-18(1) (DWF/LIB), 2018 WL 4062741 (D. Minn. Aug. 27, 2018) (denying motion to suppress evidence and finding that search warrant was supported by probable cause where search warrant "affidavit set forth

83. Also in several cases, courts admitted the expert testimony of law enforcement officials describing how sex traffickers frequently use Facebook to recruit victims, communicate with victims and co-conspirators, and facilitate their criminal activities.[44]

---

that [minor victim] had been trafficked by [defendant], that [minor victim] communicated through facebook with [another minor victim], that [defendant] had a facebook account, and that [minor victim] appeared to be looking for [defendant] through facebook connections. Further, the affidavit set forth [investigator's] professional experience that sex traffickers and the individuals they traffic . . . often communicate through facebook."); *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017) (finding probable cause to search Facebook account linked to the sex-trafficking conspiracy).

[44] *See, e.g.*, *United States v. Lagrone*, No. 4:17-CR-00264-O, 2018 WL 10447374, at *3 (N.D. Tex. Mar. 23, 2018) (admitting expert testimony by detective who "explained that he has extensive experience using Backpage.com as an investigative tool and frequently uses Facebook and other social media sites in a similar manner"; "find[ing] that the law enforcement witnesses are qualified and demonstrate a level of expertise in how criminals use Facebook, Backpage.com, and other websites to run their enterprises and recruit victims"; and noting that "[t]his testimony is admissible because it will be helpful to the jury to understand how these sites are used in sex trafficking organizations "); *United States v. Jackson*, No. 2:16-CR-00054-DCN, 2017 WL 2362351, at *1 (D.S.C. May 31, 2017) (denying motion to exclude "expert testimony regarding sex trafficking" where defendants "were indicted on multiple counts of trafficking a minor for sex and of sex trafficking by force, fraud, and coercion in connection with a conspiracy to commit sex trafficking," and "indictment charge[d] that the defendants conspired to recruit young women, some of whom were less than 18 years old, to work as prostitutes," and "used Facebook to recruit victims as well as to communicate with other co-conspirators"); *United States v. Brinson*, 772 F.3d 1314, 1319, 1327 (10th Cir. 2014) (affirming conviction for conspiracy to engage in sex trafficking, sex trafficking of children, and attempted sex trafficking of children and finding that court acted within its discretion by allowing "detective qualified as an expert" to testify regarding "how pimps and prostitutes use the internet, including websites such as Facebook.com";

84. Many judicial opinions by federal and state courts in the last several years have discussed how Meta's platforms are used by sex traffickers to recruit and exploit their victims. *See* Ex. 2. For example, in *United States v. Comer*, 5 F.4th 535 (4th Cir. 2021), the defendant "lured women into prostitution via social media and, in at least one case, attempted to use Facebook to force a young woman who had left her trafficking ring to return." *Id.* at 539. The court concluded that the defendant "***indisputably weaponized social networks like Facebook*** to commit her underlying offense" and that these social networks "were the crucial instrumentalities through which she recruited others into prostitution and, at least in the case of [one victim], tried to prevent them from leaving." *Id.* at 546.

85. Similarly, in *United States v. Porter*, No. 2:20-CR-95, 2022 WL 3021646, at *1 (S.D. Ohio July 29, 2022), the court charged the defendant with child sex trafficking conspiracy and sex trafficking by force conspiracy, noting the defendant's use of Facebook and Facebook messenger. *Id.* The court further noted that the defendant communicated with his coconspirators about his crimes on Facebook. *Id.*

---

and that "the jury could have relied on the Facebook.com exchange between [defendant] and [minor victim]" and "[f]rom that exchange, the jury could reasonably infer that [defendant] was using the internet to knowingly entice [a minor victim] into the prostitution trade").

C. 2012-2022 – U.S. Courts and U.S. News Media Report Rampant Child Sexual Exploitation Taking Place on Meta's Platforms

86. Between 2012 and 2023, at least 129 federal and state courts issued written decisions in criminal and civil cases involving cases of child sexual exploitation on Meta's platforms. These decisions—which are merely a sample of a larger trend in which new cases are filed every few days—are summarized in Exhibit 3.

87. A review of merely a few such cases conveys the real-world harm that that has resulted from the Board's failure to provide any meaningful oversight of this growing problem even as Meta's management has abysmally failed to detect, prevent, or slow down the rampant child sexual exploitation that occurs on a daily basis on Meta's platforms. For example:

- *Commonwealth v. Howland*, No. 61 MDA 2022, 2022 WL 16832489, at *1 (Pa. Super. Ct. Nov. 9, 2022) (defendant convicted of "kidnapping and sexual abuse of a 13-year-old child admitted communicating with the child by . . . Facebook").

- *Commonwealth v. Escabal*, No. 1928 EDA 2021, 2022 WL 6643947, at *1 (Pa. Super. Ct. Oct. 11, 2022) (defendant "admitted using Facebook Messenger to disseminate images of child pornography" and that his "Facebook account [was] used to disseminate the pornographic images").

- *United States v. Elliott*, No. 1:19-CR-00152-TWP-MJD, 2022 WL 2046342, at *1 (S.D. Ind. June 7, 2022) (defendant "possessed Child Sexual Abuse Material ('CSAM') of Minor Victim 1 and distributed it on Facebook, thereafter, he attempted to hire a hitman . . . to kill Minor Victim 1 and Witness Victim 1 to prevent them from testifying against him in various state and federal cases").

- *United States v. Isip*, No. CR 19-64-RGA, 2022 WL 1120111, at *2 (D. Del. Apr. 14, 2022) ("Defendant knowingly received a sexually explicit picture from the [minor] victim via Facebook Messenger.").

- *United States v. Ashmore*, No. ACM 40036, 2022 WL 678895, at *1 (A.F. Ct. Crim. App. Mar. 8, 2022) (defendant "used 16 different Instagram accounts" and "5 Facebook accounts" that were "populat[ed] . . . with photos" of "his [minor] victims").

- *Cuddihe v. United States*, No. 17-CR-04091-SRB-1, 2021 WL 1972208, at *1-2 (W.D. Mo. May 17, 2021) (defendant exchanged "pictures and videos via Facebook Messenger" and used "Facebook" and "Facebook Messenger" to "converse[] with over 150 people, many of whom appeared to be minors between the ages of eleven and fifteen").

- *United States v. Galvan*, No. 3:20-CR-00019, 2020 WL 4604502, at *1, *3, *5 (S.D. Tex. Aug. 11, 2020) (defendant "arrested and charged in state court with three counts of possession of child pornography" after "posing as a 13-year-old boy on Instagram" and authorities discovered "over 8,000 pages of Instagram conversations during the approximate month-and-a-half period the Instagram account was active," and "[a] review of the less-than-two-month-old Instagram account revealed 8,185 pages of conversations, including sexually explicit messages between [defendant] and at least ten separate minor victims").

- *United States v. Bjerknes*, No. 17-CR-0234 (WMW), 2020 WL 1989393, at *1 (D. Minn. Apr. 27, 2020) ("[Defendant's] convictions arise from his scheme, executed between 2014 and 2017, to use 'various social media applications, including Facebook to solicit images and videos constituting child pornography from minor females, engage in sexually explicit conversations with minor females, and distribute sexually explicit images and videos to minor females and males.' [Defendant's] scheme involved at least 55 minors.").

88. U.S. news media has similarly reported on the ubiquitous, openly occurring, and unchecked child sexual exploitation that occurs every day on Meta's

platforms and which currently has no end in sight. For example, on March 13, 2022, *WIRED*, an online and print magazine, published an article by Professor Lara Putnam, a history professor at the University of Pittsburg, titled "Facebook Has a Child Predation Problem."[45] In the article, Professor Putnam recounted how her attempt to research "the 10th, 11th, or 12th wards of the city of Pittsburgh" on Facebook quickly led her to dozens of Facebook "groups targeting children of those ages" with "over 81,000 members" who openly solicited children for sexual exploitation.[46]

89. For example, one such "group [was] named 'Buscando novi@ de 9,10,11,12,13 años'" [i.e., "[l]ooking for a 9-year-old girlfriend"] and had "7,900 members."[47] Yet, when Professor Putnam "used Facebook's on-platform system" to "tag[] it as containing 'nudity or sexual activity' which 'involves a child,'" an "automated response came back days later" (by which time the group had grown to "9,000" members) saying that "[t]he group had been reviewed and did not violate any 'specific community standards'" and that if Professor Putnam "continued to encounter content 'offensive or distasteful' [she] should report that specific content,

[45] Lara Putnam, *Facebook Has a Child Predation Problem*, WIRED (Mar. 13, 2022), available at https://www.wired.com/story/facebook-has-a-child-predation-problem/.

[46] *Id.*

[47] *Id.*

not the group as a whole."[48] And despite her repeated efforts to report these groups to Facebook, due to Facebook's implacable "AI-driven algorithms," "new child sexualization groups began getting recommended to [her] as 'Groups You May Like.'" A partial excerpt of the article states as follows:

> WHILE TRYING TO map the extent and impact of place-based Facebook groups where QAnon and allied disinformation spread, I went looking for Facebook groups with names including 10, 11, or 12. This was part of my work with the Pitt Disinformation Lab, and ***I was thinking of the 10th, 11th, or 12th wards of the city of Pittsburgh. What appeared instead was a group named "Buscando novi@ de 9,10,11,12,13 años." Looking for a 9-year-old girlfriend? What?***
>
> The page's aesthetic was cartoon cute: oversized eyes with long lashes, hearts, and pastels. The posts that made explicit references to photographed genitalia were gamified and spangled with emoticons: "See your age in this list? Type it into the replies and I'll show 'it' to you."
>
> Most often posts were just doorways to connection, the real danger offstage. "Looking for a perverted girlfriend of 11," read one post, with purple background and heart emojis. Replies asked for friend requests to continue via Messenger, or offered entry to private groups or WhatsApp chats—away from the eyes of even a digital passerby.
>
> This was not some outlaw 8Chan message board. ***It was cheerfully findable on Facebook***. And, I began discovering in alarm, it was not the only one. ***Indeed, as late as January 2022—three months into my efforts to get action taken against them—if I searched 11, 12, 13 on the platform, 23 of the first 30 results were groups targeting children of those ages, with group names that included the words boyfriend/girlfriend, novio/a, or niños/niñas, sometimes along with 'pervertidos,' 'hot,' etc. They totaled over 81,000 members***.
>
> ***

[48] *Id.*

Surely due diligence would dictate proactive steps to prevent the creation of such groups, backed up by quick action to remove any that get through once they are flagged and reported. I would have thought so. Until I stumbled into these groups and began, with rising disbelief, to find it ***impossible to get them taken down***.

***

OF COURSE I reported the group I had accidentally uncovered. I used Facebook's on-platform system, tagging it as containing "nudity or sexual activity" which (next menu) "involves a child." An automated response came back days later. The group had been reviewed and did not violate any "specific community standards." If I continued to encounter content "offensive or distasteful to you"—was my taste the problem here?—I should report that specific content, not the group as a whole.

"Buscando novi@ de 9,10,11,12,13 años" had 7,900 members when I reported it. By the time Facebook replied that it did not violate community standards, it had 9,000.

So I tweeted at Facebook and the Facebook newsroom. I DMed [i.e., Direct Messaged] people I didn't know but thought might have access to people inside Facebook. I tagged journalists. And ***I reported through the platform's protocol a dozen more groups, some with thousands of users***: groups I found not through sexually explicit search terms but just by typing "11 12 13" into the Groups search bar.

What became ever clearer as I struggled to get action is that technology's limits were not the problem. ***The full power of AI-driven algorithms was on display, but it was working to expand, not reduce, child endangerment***. ***Because even as reply after reply hit my inbox denying grounds for action, new child sexualization groups began getting recommended to me as "Groups You May Like."***

D. April 10, 2018 – Zuckerberg Testifies Before the U.S. Senate Regarding Sex/Human Trafficking on Meta's Platforms

90. On at least three separate occasions, Zuckerberg has testified before Congress and publicly discussed the subject of sex trafficking tied to Facebook. His

testimony makes clear that Facebook, its Board, and Zuckerberg specifically, have been put on notice for years that more had to be done to address the improper facilitation of sex trafficking on Meta's platforms.

91. On April 10, 2018, Zuckerberg testified for the first time before Congress, appearing before the U.S. Senate Committee on the Judiciary and the U.S. Senate Committee on Commerce, Science and Transportation. Below are excerpted comments that U.S. Senators John Thune and Ben Sasse made to Zuckerberg during that hearing.

> [**Senator Thune:**] Just last month, in overwhelming bipartisan fashion, ***Congress voted to make it easier for prosecutors and victims to go after websites that knowingly facilitate sex trafficking. This should be a wake-up call for the tech community***. We want to hear more, without delay, about what Facebook and other companies plan to do to take greater responsibility for what happens on their platforms (p. 3)
>
> ***
>
> [**Senator Sasse:**] I think violence has no place on your platform. ***Sex traffickers and human traffickers have no place on your platform***. (p. 103)

E. October 23, 2019 – Zuckerberg Testifies Before the House Regarding Sex Trafficking and Exploitation on Meta's Platforms

92. On October 23, 2019, Zuckerberg testified before the U.S. House Financial Services Committee. Below are excerpted comments that U.S. Congresswoman Ann Wagner made to Zuckerberg during that hearing, and certain of his responses.

[**Congresswoman Wagner:**] So, let me move on to something that is near and dear to my heart. As you may know, I wrote and passed HR 1865, the Fight Online Sex Trafficking Act. Together with the Senate's Stop Enabling Sex Traffickers Act, the package is widely known as FOSTA-SESTA. I am committed to rooting out online sex trafficking, and I believe that what is illegal offline should, indeed, be illegal online.

[**Congresswoman Wagner:**] Three weeks ago, the New York Times ran a report entitled, "The Internet is Overrun with Images of Child Sex Abuse." And I would like this submitted for the record.

***

[**Congresswoman Wagner:**] 16.8 million, as confirmed by the Department of Justice, of the 18.4 million worldwide reports of child sexual abuse material are on Facebook. 16.8 of the 18.4 million. These 18.4 million reports from last year included a record 45 million photos and videos. These are absolutely shocking numbers. Moreover, it is estimated that 70 percent of Facebook's valuable reporting to NCMEC, the National Center on Missing and Exploited Children, would be lost if Facebook implements its end to end encryption proposal. Mr. Zuckerberg, how much is this figure growing year after year, and if you enact end – to - end encryption, what will become of the children who will be harmed as a result that they are not reported?

[**Zuckerberg:**] Congresswoman, thanks. Child exploitation is one of the most serious threats that we focus on.

[**Congresswoman Wagner:**] What is Facebook doing? Sixteen–point–eight of the 18.4 million.

[**Zuckerberg:**] Congresswoman, those reports come from Facebook. The reason why the vast majority come from Facebook is because I think we work harder than any other company to identify this behavior and report it to NCMEC and the FBI.

[**Congresswoman Wagner:**] ***What are you doing to shut this down? These accounts peddle horrific illegal content that exploits women and children. What are you doing, Mr. Zuckerburg, to shut this down?***

[**Zuckerberg:**] ***Congresswoman, we build sophisticated systems to find this behavior.***

[**Congresswoman Wagner:**] Sixteen–point–eight million and growing of the 18.4 images?

[**Zuckerberg:**] Absolutely. Congresswoman, I don't think Facebook is the only place on the internet where this behavior is happening. I think the fact that the vast majority of those reports come from us reflects the fact that we actually do a better job than everyone else at finding it and acting on it. And you are right that in an end–to–end encrypted world, one of the risks that I am worried about, among others, to safety is that it will be harder to find some of this behavior.

[**Congresswoman Wagner:**] But you have said you want end–to–end encryption. What is going to happen to these children? They won't be reported then. And you are responsible. Facebook is responsible for 16.8 million of the 18.4 million that are out there last year alone.

[**Zuckerberg:**] Congresswoman, again I believe that there are probably a lot more than 18 million out there, and I think we're doing a good job of finding this, but I think you're right that an end to–

[**Congresswoman Wagner:**] ***What are you going to do to shut it down, Mister Zuckerberg?***

[**Zuckerberg:**] ***We are working with law enforcement and building technical systems to identify and report this hard before it–***

[**Congresswoman Wagner:**] ***Well, you are not working hard enough, sir, …***

F. October 2019 – BBC Reports "Hundreds of Women Being Sold" in "Slave Markets" on "Instagram"; Apple Threatens to Pull Meta from the App Store; and Meta Internally Admits "Our Platform Enables All Three Stages of the Human Exploitation Life Cycle"

93. On October 31, 2019, *BBC News Arabic* published an article detailing "[a]n undercover investigation" revealing that "[i]n Saudi Arabia, ***hundreds of***

women [were] being sold on Instagram, which is owned by Facebook."[49] The article stated that "at the time of publication, ***hundreds of domestic workers were still being traded on Instagram*** which the BBC [British Broadcasting Company] has seen."[50] *BBC* quoted "Urmila Bhoola, the UN special rapporteur on contemporary forms of slavery," who said, "***[t]his is the quintessential example of modern slavery***[.]"[51] "***What they are doing is promoting an online slave market***," Ms. Bhoola said, "If Facebook or any other companies are hosting apps like these, they have to be held accountable."[52]

94. On October 23, 2019, according to internal documents,[53] Meta "received [a] communication from Apple" in which Apple "threatened to pull

---

[49] *See* Owen Pinnell & Jess Kelly, *Slave markets found on Instagram and other apps*," BBC NEWS ARABIC (Oct. 31, 2019), available at https://www.bbc.com/news/technology-50228549.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Apple's confrontation with Meta was revealed in internal documents obtained by Frances Haugen and filed with her whistleblower complaints to the SEC, which were published in *60 Minutes'* website. *See* Keith Zubrow, Maria Gavrilovic, and Alex Ortiz, Whistleblower's SEC Complaint: Facebook Knew Platform Was Used to "Promote Human Trafficking and Domestic Servitude," 60 MINUTES (Oct. 4, 2021), available at https://www.cbsnews.com/news/facebook-whistleblower-sec-complaint-60-minutes-2021-10-04/ ("[Meta's] failure to solve human trafficking and servitude on its platforms threatened its distribution on the Apple App Store."). *60 Minutes* posted Haugen's SEC complaint concerning trafficking at: https://drive.google.com/file/d/1ItiZR_n1_xB3gzkJZ9uvd6pUOYRMGIex/view.

[Facebook and Instagram] apps from its App Store due to [Apple's] identifying content promoting 'domestic servitude'" on Facebook and Instagram. "Apple['s] escalation was linked to the findings of the BBC investigation into Domestic Servitude content on [Instagram and Facebook], which identified [Meta's] apps (and Apple's platform, Apps Store) being used to buy and sell domestic workers in the Gulf Region."[54]

95. In response to this "Apple escalation," Meta undertook a "Deep Dive" on "Domestic Servitude and Tracking in the Middle East," and as a result, internally acknowledged that it had been "***underreporting this behaviour***"; suffered from an "***absence of proactive detection***"; that "***newly created and existing [domestic servitude] content [was] not captured***" which "***meant that domestic servitude content remained on the platform***"; Meta had been "***under-enforcing on confirmed abusive activity with a nexus to the platform***"; and that Meta's own "***investigative findings demonstrate that our platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks***."[55] Specifically, Meta's internal documents stated:[56]

---

[54] *Id.*

[55] *Id.*

[56] *Id.* (quoting "Internal Facebook documents" titled "Apple Escalation – How we made it through this SEV," "Domestic Servitude and Tracking in the Middle East – a SEV Deep Dive," and "Domestic Servitude") (internal footnotes and citations omitted).

"On 23rd October [2019] ***we received communication from Apple where the company threatened to pull FB & IG apps from its App Store due to them identifying content promoting 'domestic servitude'***

Apple escalation was linked to the findings of the BBC investigation into Domestic Servitude content on IG & FB, which identified our apps (and Apple's platform, Apps Store) being used to buy and sell domestic workers in the Gulf Region. At the time, BBC approached Facebook in relation to the investigation prior to the Apple escalation and shared violating hashtags . . .

However, due to the underreporting of this behaviour and absence of proactive detection, newly created and existing content not captured in the IG [i.e., Instagram] sweep meant that domestic servitude content remained on the platform.*"*

"***Was this issue known to Facebook before BBC enquiry and Apple escalation? Yes***."

"[W]e found users did discover the IG domestic servitude accounts using Search currently we aren't logging the information to determine how users found the IG accounts."

"***FB is the primary vehicle that domestic workers from the Philippines - - probably the most significant source country - - use to communicate with recruitment agencies about off-platform exploitation . . . 89% . . . were undetectable for scaled review***. . . Our best opportunity to reduce this type of human exploitation on the platform is a preventive educational campaign . . . We also propose several recommendations to improve our enforcement . . . by using our current approach, ***we are under-enforcing on confirmed abusive activity with a nexus to the platform.***"

"***Our investigative findings demonstrate that our platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks. The traffickers, recruiters and facilitators from these 'agencies' used FB profiles, IG profiles, Pages, Messenger and WhatsApp***."

"Human Trafficking Unresolved model for investigative flows led to ambiguity on responsibilities . . . Understand exercise for Hex [human exploitation] deprioritized." "***encryption will preclude investigators'***

> ***access to inboxes and potentially make it impossible to accurately evaluate the violating status of recruitment-related agencies*** . . . [but a] preventative approach could lead to a significant reduction in real-world domestic servitude abuse via the Facebook platform.

96. In the same internal documents (as quoted in a September 16, 2021 article by *The Wall Street Journal*[57]), Meta internally acknowledged in that "***domestic servitude manifests on our platform across its entire life cycle: recruitment, facilitation, and exploitation***," and "***recognised the risks resulting from mitigation strategy based on user reports: similarly to other human exploitation abuses, domestic servitude has been highly underreported by the platform users***."[58]

G. November 17, 2020 – Zuckerberg Testifies Before U.S. Senate Regarding Human Trafficking on Meta's Platforms

97. On November 17, 2020, Zuckerberg testified before the U.S. Senate Committee on the Judiciary. Below are excerpted comments that Senator Richard Blumenthal made to Zuckerberg during that hearing.

> [**Senator Blumenthal:**] There are real harms and real victims here. And in some ways, this hearing is a betrayal of those real harms and the real victims of them. Those harms have been caused by big tech because you have failed your responsibility as have others in this industry. ***I want to see real reform that will enable these abuses to be reformed***

---

[57] Justin Scheck, Newley Purnell, Jeff Horwitz, *Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show*, THE WALL STREET JOURNAL (Sept. 16, 2021), available at https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953?mod=article_inline.

[58] *Id.*

because your platforms have embraced abuse and weaponized child predators, violent white supremacists and human traffickers.

H. 2020 – Polaris – "Human Trafficking Trends in 2020"

98. The Polaris Project is a nonprofit that was founded in 2002 that has operated the U.S. National Human Trafficking Hotline, which provides 24/7 support and a variety of options for survivors of human trafficking to get connected to help and stay safe. Polaris released its report – Human Trafficking Trends in 2020 – detailing an analysis of data obtained from the U.S. National Human Trafficking Hotline.[59]

99. The investigation found that "[o]nline recruitment increased a significant 22%. During the lockdowns, as the proportion of victims from common recruitment sites such as strip clubs (-46%), foster homes (-70%) and schools (-38%) went down drastically, the Internet was reported as the top recruitment location for all forms of trafficking."[60]

100. Notably, "the analysis found a significant increase in the proportion of potential victims for whom Facebook and Instagram were the sites for recruitment into trafficking." There was a "125% increase in reports of recruitment on Facebook

[59] https://polarisproject.org/2020-us-national-human-trafficking-hotline-statistics/.

[60] https://polarisproject.org/wp-content/uploads/2022/01/Human-Trafficking-Trends-in-2020-by-Polaris.pdf.

over the previous year" and a "95% increase in reports of recruitment on Instagram over the previous year."[61]

I. March 3, 2020 – Tech Transparency Project – "Broken Promises: Sexual Exploitation of Children on Facebook"

101. In March of 2020, the Tech Transparency Project ("TTP") published its analysis which found hundreds of U.S. cases in which suspected pedophiles used Facebook to groom minors and trade images of their sexual abuse.[62]

102. The review identified 366 federal criminal cases over seven years that featured suspects using Facebook for child exploitation. TTP's report also found such cases are becoming more frequent, from as many as 10 per quarter in 2013 to as many as 23 per quarter in 2019.

103. The report further concluded that Facebook's systems are failing to eliminate such abuse. In the vast majority of cases, Facebook did not provide the initial tip-off to authorities, despite this conduct occurring on its platforms. In fact, "[o]nly 9% of the cases were initiated because Facebook or the National Center for Missing and Exploited Children (which receives cyber tips from Facebook) reported them to authorities, raising questions about the effectiveness of Facebook's

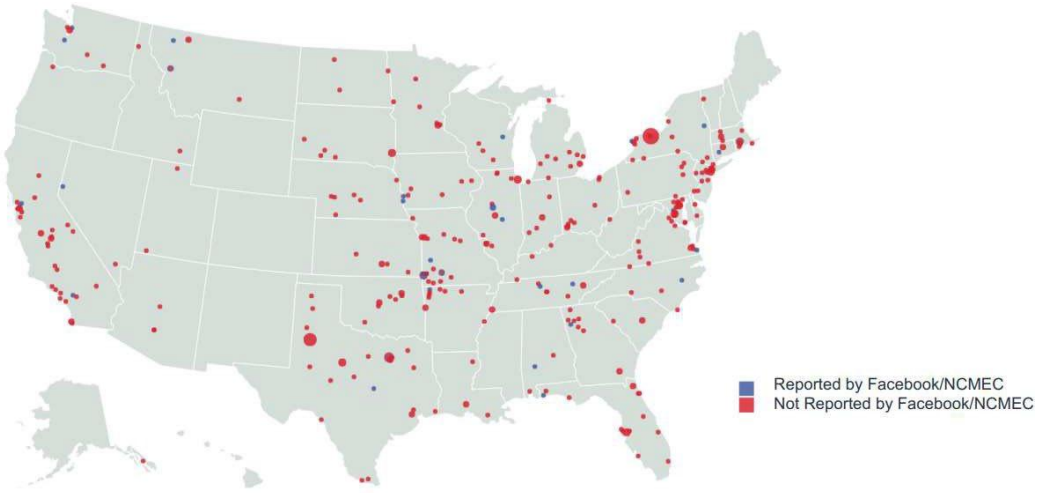
---

[61] *Id.*

[62] https://www.techtransparencyproject.org/articles/sexual-exploitation-children-facebook.

monitoring of criminal activity targeting children."[63] The report concluded therefore that "[t]he cases reviewed represent the tip of the iceberg of a far larger problem that remains unsolved by Facebook in the U.S. and around the world."[64]

104. The TTP report also emphasized how Zuckerberg told lawmakers in October 2019 that Facebook "build[s] sophisticated systems to find this behavior," yet the map below illustrates how Meta has failed to detect and/or report the vast majority of cases:



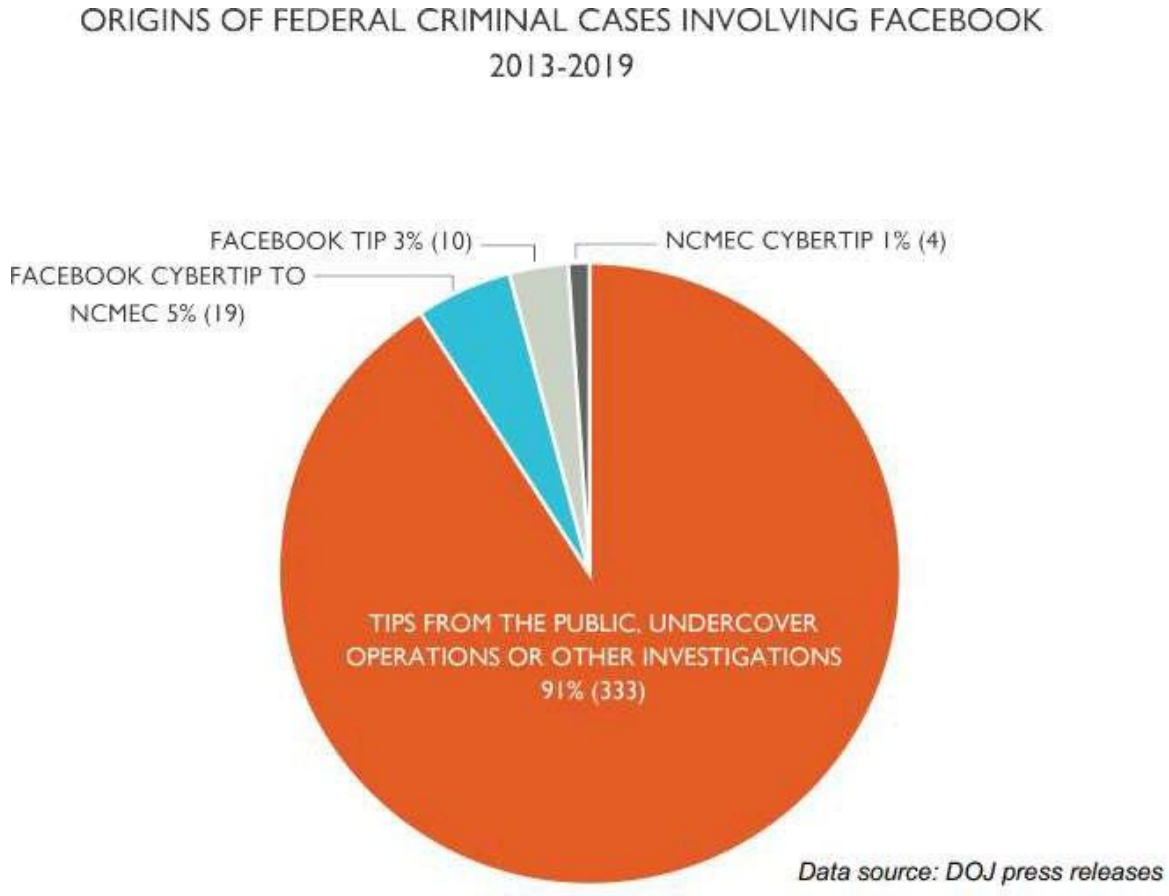
Federal criminal cases across the country have shown suspected pedophiles targeting or abusing children on Facebook. Facebook reported the activity to authorities in less than 10 percent of the cases.

105. The report further stated that "[a]ll of the examples of suspects using Facebook for child exploitation fell into 366 cases (which sometimes covered

[63] https://www.techtransparencyproject.org/sites/default/files/Facebook-Child-Exploitation.pdf.

[64] *Id.*

multiple defendants). The Justice Department's press releases on those cases included information on how the investigation was initiated. The majority of the cases (91%) were initiated by tips from the public, undercover operations or information obtained in ongoing investigations. The remaining 9% state that investigations were the result of cyber tips from Facebook or NCMEC."[65]



106. TTP's report further explains that "[a]fter [FOSTA-SESTA's] final passage, however, the press releases show child exploitation cases involving

[65] *Id.*

Facebook began to increase, as did Facebook and NCMEC's reporting of such activity to authorities."[66]

107. "In the five years before the passage of FOSTA-SESTA, Facebook and NCMEC averaged less than one cyber tip per quarter, according to the TTP analysis. Since the bill was passed in March 2018, they have averaged more than three reports per quarter. In total, they reported more cases in the nearly two years since FOSTA-SESTA than they did in the prior five years combined."[67]

108. "Th[is] trend … suggests the threat of legal liability under FOSTA-SESTA may be motivating Facebook to increase tips to authorities. But even with the upswing, ***the number of Facebook tips detailed in the DOJ press releases remains relatively low, and they're limited to child sexual abuse images.***"[68]

J. April 10, 2020 – Meta's Board Opposes a "Stockholder Proposal Regarding Child Exploitation" by Making False Statements

109. On April 10, 2020, Meta filed its annual proxy statement in which it published a "Stockholder Proposal Regarding Child Exploitation" which stated, among other things, that "Facebook [was] being sued in a Texas court for facilitating

---

[66] *Id.*

[67] *Id.*

[68] *Id.*

sex trafficking of minors," and that "Instagram [was] being linked to 'rampant sex trafficking'":[69]

> Facebook and its subsidiaries have faced other recent controversies of child sexual exploitation, including:
>
> - ***Facebook being sued in a Texas court for facilitating sex trafficking of minors***;[70]
>
> - ***Instagram being linked to "rampant sex trafficking***, child sexual abuse grooming, as well as adult fetishization of young girls…," "sexually graphic comments on minor's photos," and allowing strangers to "direct message minors";[71] and
>
> - Pedophiles "sharing Dropbox links to child porn via Instagram[.]"[72]

110. Based on these and other observations, the "Shareholders request[ed] that the Board of Directors issue a report by February 2021 assessing the risk of increased sexual exploitation of children as the Company develops and offers additional privacy tools such as end-to-end encryption."[73]

---

[69] Meta, Proxy Statement (Schedule 14A) at 77 (Apr. 10, 2020).

[70] https://www.nytimes.com/2019/12/03/technology/facebook-lawsuit-section-230.html.

[71] https://endsexualexploitation.org/articles/statement-instagram-is-predators-paradise-says-international-groupof-human-rights-ngos/; https://endsexualexploitation.org/articles/senate-hearing-uncovers-sexploitation-in-appsand-social-media/

[72] https://www.dailymail.co.uk/news/article-6574015/How-pedophiles-using-Instagram-secret-portal-apparentnetwork-child-porn.html

[73] Meta, Proxy Statement (Schedule 14A) at 77 (Apr. 10, 2020).

111. Meta's Board opposed this request and "**recommend[ed] a vote AGAINST the stockholder proposal**."[74] In its "Opposing Statement," Meta claimed that "[w]e use sophisticated technology and other techniques not only to detect child exploitation imagery and remove it, but also to detect and prevent grooming or potentially inappropriate interactions between a minor and an adult," and told shareholders that "[w]e deploy technology across all of our platforms to proactively surface as much illegal child exploitative content as we can, including through detection technology, machine learning and artificial intelligence techniques, and open-sourcing photo- and video-matching technology."[75] As discussed below, Meta's statements in opposing this stockholder proposal were materially misleading because in fact Meta did not use its "machine learning" technology [redacted] Furthermore, although Meta was ***publicly*** claiming that it could successfully "detect child exploitation imagery and remove it" and "detect and prevent grooming or potentially inappropriate interactions between a minor and an adult"—***internally*** Meta was acknowledging that [redacted]

[74] *Id.* at 79.

[75] *Id.*

[redacted]

K. June 2020 – 2020 Trafficking in Persons Report

112. In June 2020, the U.S. Department of State published its Trafficking in Persons Report (June 2020, 20th Ed.).[76] The report notes how "[t]he media reported in 2018 that trafficking gangs increasingly used social media sites, particularly Facebook, to buy and sell women and girls for sex and labor exploitation." *Id*. at 269. The report further notes that "[t]raffickers use social media websites, including dating apps, online forums and chat rooms, and Facebook groups, to exploit girls in sex trafficking." *Id.* at 275.

L. April 9, 2021 – Meta's Board Opposes a "Shareholder Proposal Regarding Child Exploitation" by Making False Statements

113. On April 9, 2021, Meta filed its annual proxy statement in which it published a "Shareholder Proposal Regarding Child Exploitation" which stated, among other things, that "[c]hild sexual exploitation online (and Child Sexual Abuse Material—CSAM) is an escalating threat to children worldwide. The exponential growth of CSAM is directly tied to the growth of social media and the increasing number of children online. In 2019, the National Center for Missing and Exploited

[76] https://www.state.gov/reports/2020-trafficking-in-persons-report/.

Children (NCMEC) received nearly 17 million reports of CSAM. Of these, nearly 16 million reports–or ***94 percent–stem from Facebook and its platforms, including Messenger and Instagram***."[77]

114. Just as they had in 2020, the "Shareholders request[ed] that the Board of Directors issue a report by February 2022 assessing the risk of increased sexual exploitation of children as the Company develops and offers additional privacy tools such as end-to-end encryption."[78]

115. As it had in 2020, Meta's Board opposed this request and "**recommend[ed] a vote AGAINST the shareholder proposal**."[79] In its "Opposing Statement," Meta claimed to have "dedicated teams to help ***find and remove more harmful content - increasingly before people even see it***"; touted "***our progress and effectiveness in combating these issues***"; and stated that "[w]e deploy technology across all of our platforms to proactively surface illegal child exploitative content and activity, including through detection technology, ***machine learning*** and artificial intelligence techniques."[80]

---

[77] Meta, Proxy Statement (Schedule 14A) at 74 (Apr. 9, 2021).

[78] *Id.*

[79] *Id*. at 76.

[80] *Id.* at 75.

116. As discussed below, Meta's statements in opposing this shareholder proposal were materially misleading because in fact Meta did not use its "machine" learning technology [redacted] *See* Section II.L *supra*. And although Meta was ***publicly*** touting its "progress and effectiveness in combating these issues" and how it could "find and remove more harmful content - increasingly before people even see it"—***internally*** Meta was acknowledging that [redacted] *See* Section II.L *supra*.

M. June 8, 2021 – 2020 Federal Human Trafficking Report

117. On June 8, 2021, the Human Trafficking Institute published its 2020 Federal Human Trafficking Report.[81] The report provided numerous statistics concerning human trafficking in the United States and internationally. One of the "key takeaways from 2020" was that 59% of online victim recruitment (and 65% of

[81] https://traffickinginstitute.org/wp-content/uploads/2022/01/2020-Federal-Human-Trafficking-Report-Low-Res.pdf.

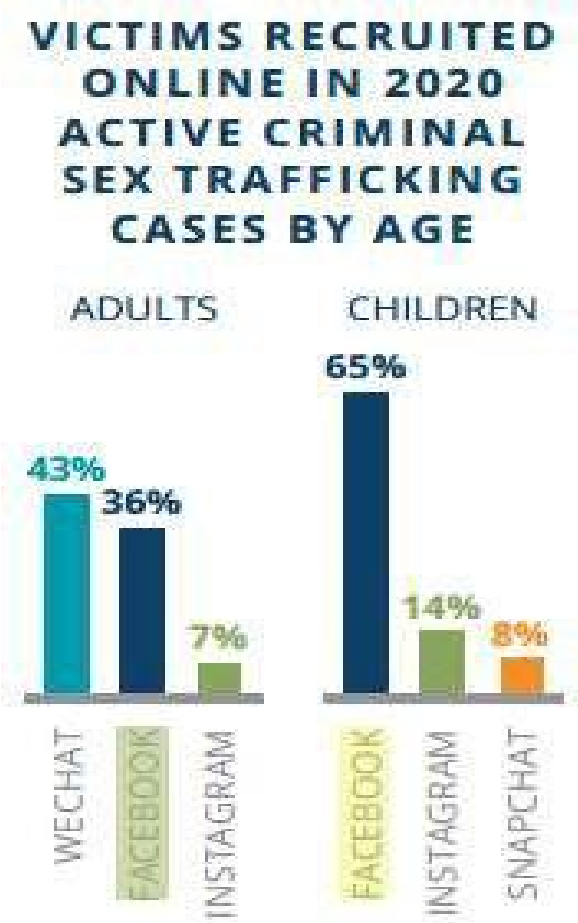
child victim recruitment) in active sex trafficking cases occurred on the Facebook and Instagram social media platforms:

> Although traffickers in 2020 active cases recruited their victims from a variety of physical locations, the internet was the most common (41%, 244) location for recruitment, as has been the case every year since 2013. ***In 2020, 59% (78) of online victim recruitment in active sex trafficking cases occurred on Facebook, making [Facebook] by far the most frequently referenced website or app in public sources connected with these prosecutions, which was also true in 2019***.
>
> Surprisingly, despite Facebook's reputation as a less popular platform among teenagers, it was a more common platform for recruiting child victims than adult victims in 2020 active sex trafficking cases. In fact, ***65% (68) of child victims recruited on social media were recruited through Facebook*** compared to just 36% (10) of adults. After Facebook, Instagram and Snapchat were the most frequently cited social media platforms for recruiting child victims, accounting for 14% (15) and 8% (8) of child recruitment, respectively. Among adults, other top platforms were WeChat (43%, 12) and Instagram (7%, 2). Overall, when examining websites and apps used to recruit victims irrespective of age, the most common sites in active sex trafficking cases—after Facebook—were Instagram (13%, 17), WeChat (9%, 12), and SnapChat (7%, 9).

Id. at 44 (emphases added) (internal citations omitted).

118. The report depicted the percentages of "active criminal sex trafficking cases by age" which involved Facebook or one of Meta's other platforms, Instagram, as follows: [82]

[82] *Id.*



119. Thus, in 2020, 79% of child victims in active criminal sex trafficking cases were recruited by their predators from Facebook and Instagram.

N. June 2021 – 2021 Trafficking in Persons Report

120. In June 2021, the State Department publicly released its annual Trafficking in Persons Report.[83] The State Department reported that COVID-19 mitigation efforts forced many people to shift online, including human traffickers. Online grooming and recruitment of children has increased, and reports from several

[83] https://www.state.gov/reports/2021-trafficking-in-persons-report/.

different countries demonstrated drastic increases in online commercial sexual exploitation and sex trafficking, including online sexual exploitation of children (OSEC), and demand for distribution of child sexual exploitation material (CSEM), including content that involved human trafficking victims. The report noted that in Israel, women, transgender adults, and children were vulnerable to sex trafficking, and that traffickers "use social media websites, including dating apps, online forums and chat rooms, and Facebook groups, to exploit girls in sex trafficking."[84] The report further noted that "[i]n cases of sexual exploitation of children, WhatsApp chats . . . are used to attract children and exploit them."[85]

O. June 10, 2021 – Meta Falsely Tells *CBS* that It "Take[s] Down Any Content that Violates [Its] Rules" Against "Sex Trafficking and Child Exploitation"

121. On June 10, 2021, Meta issued a statement to *CBS News*, claiming that it "take[s] down any content that violates" the Company's rules prohibiting "sex trafficking and child exploitation" on its platforms:

> ***Sex trafficking and child exploitation are abhorrent and we don't allow them on Facebook. We have policies and technology to prevent these types of abuses and take down any content that violates our rules***. We also work with safety groups, anti-trafficking organizations and other technology companies to address this and we report all apparent instances of child sexual exploitation to the National Center for Missing and Exploited Children.

[84] *Id.* at 310.

[85] *Id.* at 216.

122. Meta's statement above to *CBS News* on June 10, 2021, was materially false and misleading because although Meta claimed to "take down any content that violates" it rules against "[s]ex trafficking and child exploitation"—Meta had already internally acknowledged in December 2020 that (1) [redacted]; (2) [redacted]; (3) the [redacted] and that the [redacted]; and (4) the Company lacked [redacted][86]

123. Indeed, Meta failed to "fix[] the systems that allowed" traffickers to operate despite having extensive information concerning their activities and opportunities to remove that content. For example, as *The Wall Street Journal* reported on September 16, 2021, a Meta team spent more than one year in 2018/2019 investigating human trafficking on its platforms in the Middle East, and therefore already knew it had an unresolved problem with human trafficking before the issue was raised by *BBC* and Apple. Yet, an internal document warned the Company to be cautious with statements against human trafficking in order to not "alienate

[86] META220_0006468 and META220_0006471.

buyers" of enslaved domestic workers who used Meta's platforms. As *The Wall Street Journal* reported, and Meta's internal documents noted, Meta was often more concerned with retaining users and "placating authoritarian governments" than it was with preventing human trafficking on its platforms.[87]

P. June 25, 2021 – the Texas Supreme Court Upholds a Lawsuit Against Meta by Victims of Sex Trafficking Despite Section 230

124. On June 25, 2021, the Supreme Court of Texas issued an opinion in *In re Facebook, Inc.*,[88] which held that Section 230 of the CDA, 47 U.S.C. § 230, did not bar claims against Meta by three victims of sex trafficking under the Texas human trafficking statute.[89] In so holding, the court reviewed these victims' allegations that Facebook engaged in "overt acts" that "encourag[ed] the use of [the Company's] platforms for sex trafficking" including that:

> Facebook "creat[ed] a breeding ground for sex traffickers to stalk and entrap survivors"; that "Facebook . . . knowingly aided, facilitated and assisted sex traffickers, including the sex trafficker[s] who recruited [Plaintiffs] from Facebook" and "knowingly benefitted" from rendering such assistance; that "Facebook has assisted and facilitated the trafficking of [Plaintiffs] and other minors on Facebook"; and that Facebook "uses the detailed information it collects and buys on its users to direct users to persons they likely want to meet" and, "[i]n doing so,

[87] https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953.

[88] No. 20-0434, 2021 WL 2603687 (Tex. June 25, 2021).

[89] Tex. Civ. Prac. & Rem. Code Ann. § 98.002(a).

. . . facilitates human trafficking by identifying potential targets, like [Plaintiffs], and connecting traffickers with those individuals."[90]

125. The court found that "[r]ead liberally in Plaintiffs' favor, these statements may be taken as alleging affirmative acts by Facebook to encourage unlawful conduct on its platforms."[91] The court concluded that "[t]he available precedent indicates that Facebook enjoys no CDA immunity from claims founded on such allegations" and therefore held that "[t]he plaintiffs' statutory human-trafficking claims may proceed "[92]

126. In the same case, on March 7, 2022, the U.S. Supreme Court denied Meta's petition for writ of certiorari. *See Facebook Cert.,* 142 S. Ct. 1087 (2022). In his concurring opinion, Justice Thomas wrote that "***Facebook allegedly 'knows its system facilitates human traffickers in identifying and cultivating victims,' but has nonetheless 'failed to take any reasonable steps to mitigate the use of Facebook by human traffickers' because doing so would cost the company users and the advertising revenue those users generate***." *Id.* at 1088. Justice Thomas observed that "[i]t is hard to see why the protection of § 230(c)(1) grants publishers against being held strictly liable for third parties' content should protect Facebook from liability for its own 'acts and omissions.'" *Id.*

---

[90] *In re Facebook*, 2021 WL 2603687, at *13.

[91] *Id.*

[92] *Id.* at *13, *1.

Q. September 16, 2021 – *The Wall Street Journal* Reports that Meta "Allow[s] Users to Post … Advertisements for Human Trafficking" and "Treats Harm" as the "Cost of Doing Business"

127. In September 2021, *The Wall Street Journal* began publishing a series of articles that the newspaper dubbed its "Facebook Files Investigation." The articles were based on "internal documents," many provided by Frances Haugen, and "interviews with dozens of current and former employees" of Facebook.[93]

128. Of particular relevance to this case, on September 16, 2021, *The Wall Street Journal* published an article titled "***Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show***."[94] The article stated that "[s]cores of internal Facebook documents reviewed by The Wall Street Journal show employees raising alarms about how its platforms are used in some developing countries, where its user base is already huge and expanding. They also show the company's response, which in many instances is inadequate or

---

[93] Jeff Horwitz, *Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt*, THE WALL STREET JOURNAL (Sept. 13, 2021), available at https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353?mod=article_inline.

[94] Justin Scheck, Newley Purnell, Jeff Horwitz, *Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show*, THE WALL STREET JOURNAL (Sept. 16, 2021), available at https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953.

nothing at all."[95] Rather, "[w]hen problems have surfaced publicly, Facebook has said it addressed them by taking down offending posts. But it hasn't fixed the systems that allowed offenders to repeat the bad behavior."[96] Much of the misconduct reported in the article to which Meta exhibited an inadequate or nonexistent response involved sex trafficking, human trafficking, and human exploitation on Meta's platforms. Among other things, the article stated:

> Scores of internal Facebook documents reviewed by The Wall Street Journal show employees raising alarms about how its platforms are used in some developing countries, where its user base is already huge and expanding. They also show ***the company's response***, which in many instances ***is inadequate or nothing at all***.
>
> ***Employees flagged that human traffickers in the Middle East used the site to lure women into abusive employment situations in which they were treated like slaves or forced to perform sex work***.
>
> Facebook removes some pages, though ***many more operate openly***, according to the documents.
>
> In some countries where Facebook operates, it has few or no people who speak the dialects needed to identify dangerous or criminal uses of the platform, the documents show.
>
> When problems have surfaced publicly, Facebook has said it addressed them by taking down offending posts. But ***it hasn't fixed the systems that allowed offenders to repeat the bad behavior. Instead, priority is given to retaining users, helping business partners and at times placating authoritarian governments***, whose support Facebook sometimes needs to operate within their borders, the documents show.

---

[95] *Id.*

[96] *Id.*

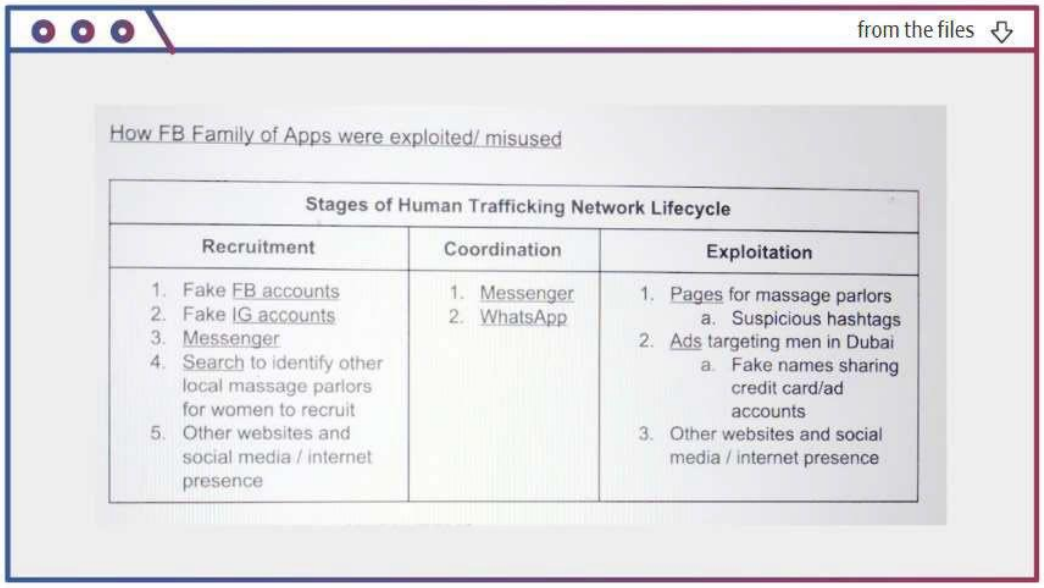
Facebook treats harm in developing countries as "simply the cost of doing business" in those places, said Brian Boland, a former Facebook vice president who oversaw partnerships with internet providers in Africa and Asia before resigning at the end of last year.

"There is very rarely a significant, concerted effort to invest in fixing those areas," he said.

***

The documents reviewed by the Journal are reports from employees who are studying the use of Facebook around the world, including ***human exploitation*** and other abuses of the platform. ***They write about their embarrassment and frustration, citing decisions that allow users to post . . . advertisements for human trafficking***.

***



Source: 2019 'Case Briefs and Insights report' on how human traffickers and criminal networks use Facebook platforms

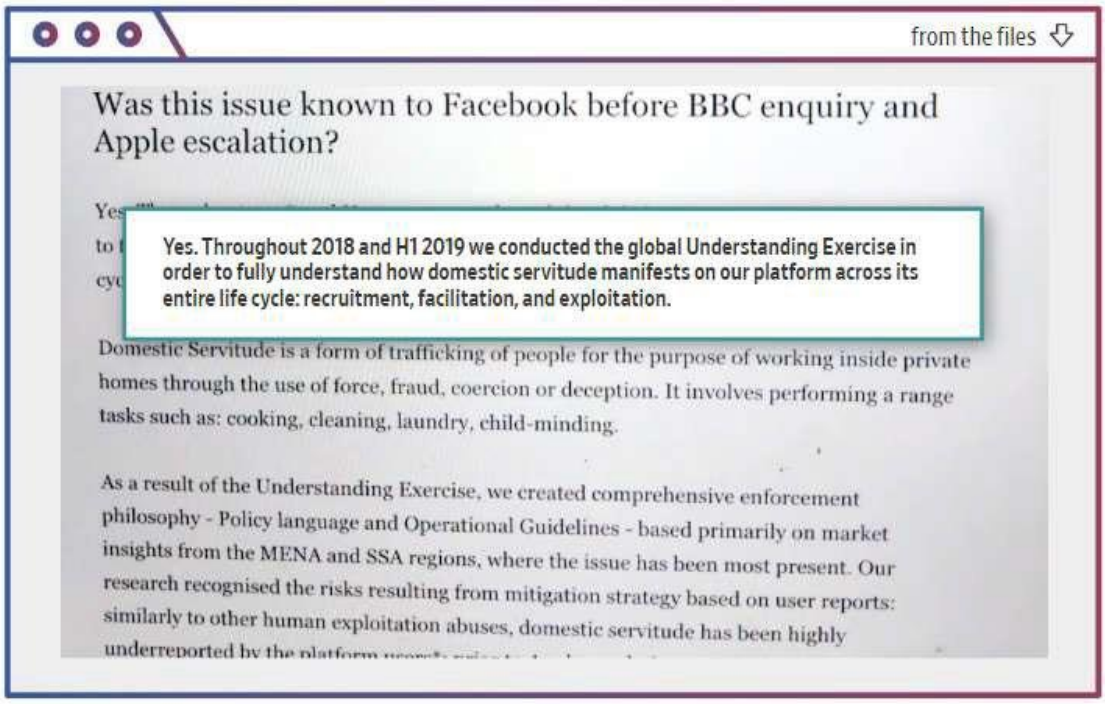
The investigation team spent more than a year documenting a bustling human-trafficking trade in the Middle East taking place on its services. On Facebook and Instagram, unscrupulous employment agencies advertised workers they could supply under coercive terms, using their photos and describing their skills and personal details.

The practice of signing people to restrictive domestic employment contracts and then selling the contracts is widely abused and has been defined as human trafficking by the U.S. State Department.

The company took down some offending pages, but ***took only limited action to try to shut down the activity until Apple Inc. threatened to remove Facebook's products from the App Store unless it cracked down on the practice. The threat was in response to a BBC story on maids for sale***.

In an internal summary about the episode, a Facebook researcher wrote: ***"Was this issue known to Facebook before BBC enquiry and Apple escalation?"***

The next paragraph begins: "Yes."



Source: 2019 internal report titled 'Apple Escalation on Domestic Servitude - how we made it through this SEV'

One document from earlier this year suggested the company should use a light touch with Arabic-language warnings about human trafficking so as not to "alienate buyers"—meaning Facebook users who buy the domestic laborers' contracts, often in situations akin to slavery.

***

Language gap

The company's internal communications show it doesn't have enough employees who speak some of the relevant languages to help monitor the situation. For some languages, Facebook also failed to build automated systems, called classifiers, that could weed out the worst abuses. ***Artificial-intelligence systems that form the backbone of Facebook's enforcement don't cover most of the languages used on the site***.

***

Facebook's team of human-exploitation investigators, which in addition to the former police officer included a Polish financial expert who previously investigated trafficking finances at HSBC bank and a Moroccan refugee expert who formerly worked at the United Nations High Commissioner for Refugees, ***gathered evidence of human trafficking***.

By looking across Facebook products, they found criminal networks recruiting people from poor countries, coordinating their travel and putting them into domestic servitude or into forced sex work in the United Arab Emirates and other Persian Gulf countries. Facebook products facilitated each step, and the investigators followed communications across platforms to identify perpetrators and victims.

Facebook in 2018 didn't have a protocol for dealing with recruiting posts for domestic servitude. In March 2018, employees found Instagram profiles dedicated to trafficking domestic servants in Saudi Arabia. An internal memo says they were allowed to remain on the site because the company's policies "did not acknowledge the violation."

The investigation team identified multiple trafficking groups in operation, including one with at least 20 victims, and organizers who spent at least $152,000 on Facebook ads for massage parlors.

The former police officer recommended that Facebook disable WhatsApp numbers associated with the rings, put in new policies about ads purchased anonymously and improve its artificial intelligence to better root out posts related to human trafficking, according to the

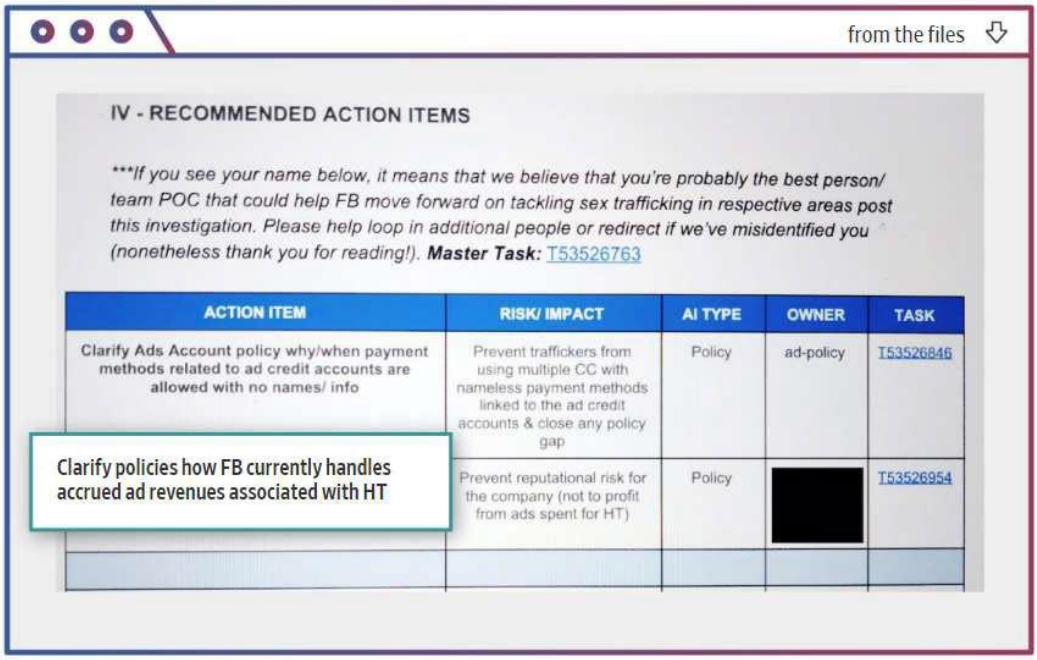
documents. He added that ***Facebook should develop a network to prevent trafficking*** by sharing findings with other tech companies.

In another memo, the Polish trafficking expert wrote that ***18 months after it first identified the problem, Facebook hadn't implemented systems to find and remove the trafficking posts***.

The BBC and Apple flagged concerns in 2019. With the threat posing ***"potentially severe consequences to the business,"*** the trafficking expert wrote, Facebook began moving faster. A proactive sweep using the investigation team's prior research found more than 300,000 instances of potential violations and disabled more than 1,000 accounts.

The team continued finding posts of human trafficking, and Facebook struggled to put effective policies in place. One document says ***Facebook delayed a project meant to improve understanding of human trafficking***.

Another memo notes: "***We know we don't want to accept/profit from human exploitation. How do we want to calculate these numbers and what do we want to do with this money?***"



Note: Names have been redacted on this document.
Source: 2019 'Case Briefs and Insights report' on how human traffickers and criminal networks use Facebook platforms

At the end of 2020, following three months in which Facebook investigated a dozen networks suspected of human trafficking, a system for detecting it was deactivated. The trafficking investigators said that hurt their efforts, according to the documents.

"We found content violating our domestic servitude policy that should have been detected automatically" by a software tool called the Civic Integrity Detection pipeline, wrote an employee in a document titled "***Domestic Servitude: This Shouldn't Happen on FB and How We Can Fix It***." She recommended the company reactivate that pipeline.

***

The investigation team also struggled to curb sex trafficking. In 2019, they discovered a prostitution ring operating out of massage parlors in the U.S. Facebook gave the information to police, who made arrests.

Facebook discovered a much larger ring that used the site to recruit women from Thailand and other countries. They were held captive, denied access to food and forced to perform sex acts in Dubai massage parlors, according to an internal investigation report.

Facebook removed the posts but ***didn't alert local law enforcement***. The investigation found traffickers bribed the local police to look away, according to the report.

R. October 3-4, 2021 – Former Meta Employee Frances Haugen Appears on *60 Minutes* and Publishes Her Complaints to the SEC

129. On October 3, 2021, Frances Haugen, one of the key sources of information for *The Wall Street Journal's* series of September 2021 news articles, appeared on *60 Minutes*. In the broadcast, *60 Minutes* reported that "[l]ast month, Haugen's lawyers filed at least 8 complaints with the [SEC] which enforces the law in financial markets."[97] Ms. Haugen's disclosures to the SEC included some of the

[97] Scott Pelley, *Whistleblower: Facebook Is Misleading the Public on Progress*

"tens of thousands of pages of Facebook internal research" that Ms. Haugen "secretly copied" while an employee at Facebook. *Id.*[98]

130. The next day, on October 4, 2021, *60 Minutes* published on its website each of Ms. Haugen's eight complaints to the SEC.[99] One of Ms. Haugen's complaints to the SEC was titled "Facebook misled investors and the public about its promotion of human trafficking / slavery / servitude."[100] This complaint quoted an internal Meta document titled "28/27 Domestic Servitude Global Analysis document" which stated that "***[w]e have observed increasing number*** [*sic*] ***of***

Against Hate Speech, Violence, Misinformation, 60 MINUTES (Oct. 4, 2021), available at https://www.cbsnews.com/news/facebook-whistleblower-frances-haugen-misinformation-public-60-minutes-2021-10-03/.

[98] The "thousands of documents" that Ms. Haugen obtained were available on Facebook's intra-company network called "Facebook Workplace," and included "presentations to Chief Executive Mark Zuckerberg – sometimes in draft form, with notes from top company executives included" and which "[v]irtually any of Facebook's more than 60,000 employees could have accessed." Jeff Horwitz, "*The Facebook Whistleblower, Frances Haugen, Says She Wants to Fix the Company, Not Harm It*," THE WALL STREET JOURNAL (Oct. 3, 2021), available at https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122.

[99] *See* Keith Zubrow, Maria Gavrilovic, and Alex Ortiz, Whistleblower's SEC Complaint: Facebook Knew Platform Was Used to "Promote Human Trafficking and Domestic Servitude," 60 MINUTES (Oct. 4, 2021), available at https://www.cbsnews.com/news/facebook-whistleblower-sec-complaint-60-minutes-2021-10-04/.

[100] Available at https://drive.google.com/file/d/1ItiZR_n1_xB3gzkJZ9uvd6pUOYRMGIex/view.

reported content that indicates that the platform is being used to coordinate and promote domestic servitude … real world harm caused by domestic servitude as well as risk to the business due to potential PR [i.e., public relations] … fires."[101]

131. The same complaint quoted further internal Meta documents which stated (as noted above in Section II.F) that: "***[D]ue to the underreporting of this behaviour and absence of proactive detection, newly created and existing content not captured in the IG [i.e., Instagram] sweep meant that domestic servitude content remained on the platform***"; "***we are under-enforcing on confirmed abusive activity with a nexus to the platform***"; and "***[o]ur investigative findings demonstrate that … our platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks… The traffickers, recruiters, and facilitators from these 'agencies' used FB profiles, IG profiles, Pages, Messenger, and WhatsApp***…."[102]

S. October 5, 2021 – Ms. Haugen Testifies Before Congress that Meta's "AI Systems Only Catch a Very Tiny Minority of Offending Content" and Explains that the Company "Has No Oversight"

132. On October 5, 2021, Ms. Haugen testified before the U.S. Senate's Sub-Committee on Consumer Protection, Product Safety, and Data Security. In her

[101] *Id.* at 3.

[102] *Id.* at 4-5.

written statement, Ms. Haugen testified that Facebook's "leadership keeps vital information from the public, the U.S. government, its shareholders, and governments around the world. The documents I have provided prove that ***Facebook has repeatedly misled us about what its own research reveals about the safety of children***, its role in spreading hateful and polarizing messages, and so much more."[103] Ms. Haugen further testified that "***Facebook's closed design means it has no oversight—even from its own Oversight Board, which is as blind as the public***." *Id.*

133. During the hearing, Senator Marsha Blackburn stated that "***Facebook also turned a blind eye toward blatant human exploitation taking place on its platform - trafficking, forced labor cartels, the worst possible things one can imagine***."[104]

134. Furthermore, during the hearing, Senator Mike Lee brought up prior testimony of a different witness who testified before the committee (Ms. Davis) claiming that Facebook has sexually suggestive ads that are targeted to children. Ms.

---

[103] Statement of Frances Haugen (Oct. 4, 2021), available at https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49.

[104] Marsha Blackburn, *Blackburn Asks Whistleblower To Detail Facebook's Practice of Endangering Children Online*, (2021), available at https://www.blackburn.senate.gov/2021/10/blackburn-asks-whistleblower-to-detail-facebook-s-practice-of-endangering-children-online.

Haugen responded that "It is very possible that none of those ads were seen by a human. The reality is that we've seen from repeated documents within my disclosures is that ***Facebook's AI systems only catch a very tiny minority of offending content*** … [i]t's likely if they rely on computers and not humans, they will also likely never get more than 10 to 20% of those ads."[105]

T. October 25, 2021 – Ms. Haugen Testifies Before the U.K. Parliament

135. On October 25, 2021, Frances Haugen testified before the Parliament of the United Kingdom to discuss her concerns about Facebook's monitoring of the conduct on its platform.

136. In particular, Ms. Haugen pointed out Facebook's deficiencies in moderating online posts written in languages other than English, saying "I want to be clear: bad actors have already tested Facebook. They have tried to hit the rate limits. They have tried experiments with content. They know Facebook's limitations. The only ones who do not know Facebook's limitations are good actors. Facebook needs to disclose what its integrity systems are and which languages it works in, and the performance per language or per dialect, because I guarantee you

[105] Clare Duffy, et al., *Facebook whistleblower testifies in Congress*, (Oct. 5, 2021), https://www.rev.com/blog/transcripts/facebook-whistleblower-frances-haugen-testifies-on-children-social-media-use-full-senate-hearing-transcript.

that, safety systems designed for English probably do not work as well on UK English versus American English."[106]

U. April 8, 2022 – Meta's Board Opposes a "Shareholder Proposal Regarding Child Exploitation" by Making False Statements

137. On April 8, 2022, Meta filed its annual proxy statement in which it published a "Shareholder Proposal Regarding Child Sexual Exploitation Online" which stated, among other things, that "[i]n 2020, 79 percent of U.S. underage sex trafficking victims recruited online were recruited through Facebook or Instagram."[107]

138. Just as they had in 2020 and 2021, the "Shareholders request[ed] that the Board of Directors issue a report by February 2023 assessing the risk of increased sexual exploitation of children as the Company develops and offers additional privacy tools such as end-to-end encryption."[108]

139. As it had in 2020 and 2021, Meta's Board "**recommend[ed] a vote AGAINST the shareholder proposal**."[109] In support of its recommendation, Meta claimed that "[f]or years ***we have been tackling this issue*** using the most advanced technologies"; "[w]e continue to increase our investment in people and technology

---

[106] Available at https://committees.parliament.uk/oralevidence/2884/pdf/ at 19.

[107] Meta, Proxy Statement (Schedule 14A) at 80 (Apr. 8, 2022).

[108] *Id*.

[109] *Id*. at 83.

with ***dedicated teams to help find and remove more harmful content – increasingly before people even see it***"; and that "***[w]e deploy technology to proactively surface illegal child exploitative content and activity***, including through detection technology, ***machine learning*** and artificial intelligence techniques."[110]

140. As discussed below, Meta's statements to shareholders in its April 8, 2022 proxy were materially misleading because in fact Meta did not use its "machine learning" technology [redacted] *See* Section II.U *supra*. And while Meta ***publicly*** claimed to have been "tackling this issue" for "years" including by "remov[ing] more harmful content – increasingly before people even see it"—***internally*** Meta was acknowledging that [redacted] *See* Section II.U *supra*.

[110] *Id.* at 82.

V. July 2022 – 2022 Trafficking in Persons Report

141. In July 2022, the State Department again released its annual Trafficking in Persons Report.[111] This report states that more than 175 nations have ratified or acceded to the UN TIP Protocol, which defines trafficking in persons and contains obligations to prevent and combat the crime. The TVPA and the UN TIP Protocol contain similar definitions of human trafficking. The elements of both definitions can be described using a three-element framework focused on the trafficker's 1) acts; 2) means; and 3) purpose. It is also important to note that neither U.S. nor international law requires that a trafficker or victim move across a border for a human trafficking offense to take place.

142. The 2022 Trafficking in Persons Report stated that "[t]raffickers have increasingly lured potential victims through social media, including Facebook, Instagram, TikTok, and mobile messages," and that "[t]he media [in Iraq, Iran, and Syria reported] trafficking gangs increasingly use social media sites, particularly Facebook, to buy and sell women and girls for sex and labor exploitation." The report also noted that in Israel, "[t]raffickers use social media websites, including dating apps, online forums and chat rooms, and Facebook groups to exploit girls in sex trafficking." Furthermore, in Kuwait, reports of "employers allegedly selling

[111] https://www.state.gov/reports/2022-trafficking-in-persons-report/.

their workers to other employers on social media and online platforms like Instagram, Twitter, Facebook … increased."

W. June 16, 2022 – 2021 Federal Human Trafficking Report

143. On June 16, 2022, the Human Trafficking Institute publicly released the 2021 Human Trafficking Report ("2021 HTI Report").[112] The 2021 HTI Report found that since 2000, traffickers have recruited 55% of sex trafficking victims online, usually through social media platforms, web-based messaging apps, online chat rooms, classified advertisements, or job boards. Defendants in federal sex trafficking cases used the internet as their primary method of soliciting buyers in 85% of the cases filed in 2021.

144. The 2021 HTI Report further found that when an online platform was used to recruit victims for criminal sex trafficking in new cases filed in 2019, 2020, and 2021, Facebook was used in 41% of the cases (more than twice as much than any other platform) and Instagram was used in 15% of the cases. In other words, based on these statistics the 2021 HTI Report concluded that more sex trafficking has occurred on Meta's two largest platforms ***than on every other platform in the world combined***.

[112] https://traffickinginstitute.org/2021-fhtr-is-now-available/.

PLATFORMS USED IN RECRUITMENT OF SEX TRAFFICKING VICTIMS SINCE 2019[111]

III. BOARD-LEVEL DOCUMENTS CONFIRM THAT THE BOARD HAS KNOWN THAT META HAS UTTERLY FAILED TO PREVENT, DETECT, OR RESPOND TO RAMPANT SEX TRAFFICKING ON ITS PLATFORMS—YET FAILED TO EXERCIZE OVERSIGHT

145. Despite committing to Plaintiffs that they would produce Board minutes, including committee minutes, related to sex and human trafficking and teen health, there was a complete lack of Board minutes produced by Defendants. The materials presented to the Board, however, demonstrate that the Board knew about Meta's problems with trafficking and related issues.[113] Defendants woefully

[113] *See, e.g.*, 1850 ([redacted]), 2229 (same), 2671 (same), 2726 ([redacted]), 3134 ([redacted]); *see also* 5069 (noting [redacted] to address [redacted] and [redacted] including [redacted]), 5919 (noting a [redacted]).

neglected their duty to respond to and address human trafficking on Meta's platforms.

146. As background, when Meta identifies a [redacted][114] The materials provided to the Board on February 14, 2019 indicate the Board was [redacted][115] In addressing problems, Meta stated, [redacted][116] Meta also has stated that [redacted][117]

147. In the same document, Meta [redacted]

[114] META220_0003179.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[redacted] respectively. *Id.* Hence, Meta [redacted]

[redacted]

A. December 2017 – the Board Acknowledges the [redacted]

148. On December 7, 2017, the Board received a presentation titled "Board Updates & Approvals" for "*Directors Only*"[118] which discussed Meta's "2017 DECEMBER – POLICY RISKS & OPPORTUNITIES."[119] The presentation reported the following:


[redacted]
120

B. March 2018 – the Board Is Informed that [redacted]

149. On March 1, 2018, the Board received a presentation on [redacted] and was specifically warned that [redacted] and noted that

[118] META220_0003014.

[119] META220_0003132.

[120] META220_0003134.

such [redacted][121]

C. 2019 – the Board Acknowledges [redacted] and Admits that [redacted] in Addressing [redacted]

150. A [redacted] recognizes that Meta's [redacted][122]

151. In evaluating [redacted][123] As to Meta's progress in addressing these problems, Meta coded [redacted][124] Meta noted that its [redacted] included [redacted][125]

D. February 2019 – the Board Acknowledges [redacted]

[121] META220_0002955

[122] META220_0002885.

[123] *Id.*

[124] *Id.*

[125] META220_0002890.

[redacted]—Yet Does Not Prioritize Solving It

152. On February 13, 2019, the Audit Committee held a meeting during which it received a presentation which discussed "Law Enforcement Compliance."[126] The presentation further discussed the [redacted] [.]"[127]

153. On February 14, 2019, the Board received a "H1 2019 Board Update"[128] for the Facebook Board of Directors[129] which stated that Meta needed to [redacted] regarding [redacted]; noted that [redacted]; and set forth the [redacted] of Meta's [redacted] regarding the [redacted][130] The update categorized Meta's progress as [redacted]

[126] META220_0006220, 6233.

[127] META220_0006233.

[128] META220_0003172.

[129] *Id.*

[130] META220_0003178.

[redacted]—and again noted that [redacted] [redacted][131]

154. The update stated that Meta's progress addressing [redacted] [redacted][132]

155. The update also stated that Meta's progress in addressing [redacted] However, the update did not even mention sex/human trafficking as being an issue that Meta was even trying to address, nor did it state whether Meta had made any progress (or if it was even trying to make progress) addressing sex/human trafficking.

[131] *Id.*

[132] *Id.*

156. Next, the update reviewed Meta's [redacted] [133] In that regard, the update predicted that [redacted] [134] Regarding how Meta classified the [redacted] the update included a [redacted] [135]

[133] META220_0003179.

[134] *Id.*

[135] *Id.* (emphasis in original).

157. The update stated that Meta's [redacted][136] Thus, because Meta's [redacted], as of the date of this update (December 2018), Meta had only [redacted] to address this problem.

158. In contrast, the update stated that Meta's [redacted][137] In other words, Meta's [redacted] Stated differently, whereas Meta at least sought to [redacted]

[136] *Id.*

[137] *Id.*

[redacted] Meta was content in ***not*** making any progress [redacted]

[redacted]

159. On another page, the update stated, [redacted] and listed purported [redacted] [redacted][138] Yet, noticeably absent from this page is any reference to Meta

[138] META220_0003181. Inexplicably, Meta had no [redacted] *Id.*

using its [redacted][139] This is despite the fact that, just pages earlier, Meta had acknowledged that it had only [redacted][140] on [redacted], had also acknowledged that this problem would [redacted], and had made clear that it had no [redacted][141]

[139] *Id.*

[140] META220_0003178.

[141] META220_0003179.

E. May 2019 – Meta Fails to Remove "Posts of Sexually Explicit or Exploitative Content" Despite Alerts from the BBC and Opposes a Shareholder Proposal for a Report Regarding Child Exploitation

160. On May 30, 2019, Meta held its Annual Meeting of Shareholders. In connection with this meeting, the Board met and received a "PROXY PAPER"[142] from Glass, Lewis & Co., LLC ("Glass Lewis"), a proxy advisory firm, which recommended that Company shareholders vote "FOR" a shareholder proposal "[t]hat the Company report on the efficacy of its content policy enforcement."[143] Glass Lewis reasoned that "[a]dditional disclosure of financial and reputational risks

[142] META220_0000754.

[143] META220_0000785.

on account of recent content management controversies is warranted" and noted that "we believe support for this proposal would provide disclosure of an important area that we do not believe is being satisfactorily addressed by the Company[.]"[144] As support, the paper detailed how in 2016, Facebook had failed to remove "posts of sexually explicit or exploitative content" despite repeated reports and notifications regarding that content by the BBC:[145]

> In 2016, ***the BBC reported that the Company's platform contained posts of sexually explicit or exploitative content and images, as well as "secret" groups used by pedophiles to connect and interchange images***. In response to these reports, the Company stated that it had improved its reporting and take-down measures. However, to test these claims, the *BBC* subsequently used the Company's reporting mechanisms to alert it to 100 images which appeared to violate the Company's guidelines. ***Of these 100 images of what appeared to be child pornography, only 18 were removed***. The Company claimed the others had not violated its Community Standards. The *BBC* also discovered five accounts maintained by convicted sex offenders, specifically pedophiles, despite the Company's rules which deny access to its platform by these individuals. The *BBC* notified the Company of the accounts via its platform's notification system, but ***none were disabled***. Pursuant to a follow-up investigation by the *BBC* one year later, the Company recognized the nature of the content and stated that it removed the items from its platform and reported them to the Child Exploitation & Online Protection Centre (Angus Crawford. 'Facebook Failed to Remove Sexualised Images of Children." *BBC*. March 7, 2017).

[144] *Id.*

[145] META220_0000789.

F. September 2019 – the Board Receives a [redacted]

161. On September 5, 2019, the Board received a presentation titled "Board Approvals & Updates" for "*Directors Only*" which discussed "Political Narratives and Our Response" and noted that one such narrative was that [redacted] and that [redacted][146]

[redacted]

162. Later in the same presentation, Meta stated that [redacted]

[redacted]

[146] META220_0003252, 3364, 3366-67.

[redacted][147]

163. Yet noticeably absent from the above statement was any mention of any policy against sex/human trafficking or any effort or progress in identifying or taking down content related to sex/human trafficking, or any ability of Meta (including its [redacted]) to [redacted] or take down content related to either child exploitation, prostitution, sexual solicitation, or sex/human trafficking.[148]

164. A presentation dated December 5, 2019, noted that [redacted] . . .”[149]

[147] META220_0003376.

[148] *Id.*

[149] META220_0003508.

G. 2020 – Meta Acknowledges that It Lacks [redacted] and that Meta [redacted]

165. A document titled "Policy 2020 H1/H2 Strategy"[150] discussed Meta's [redacted] and detailed certain [redacted][151] This [redacted] [.]"[152] The document stated that [redacted][153] The document stated that [redacted][154] The document further noted that [redacted]

[150] META220_0003006.

[151] META220_0003011.

[152] META220_0003012.

[153] *Id.*

[154] *Id.*

[redacted][155]

166. Importantly, by acknowledging that [redacted][157]—Meta was simultaneously acknowledging that such [redacted] that Meta's [redacted][158] The document further acknowledged that [redacted][159]

H. February 2020 – the Board Opposes a "Stockholder Proposal Regarding Child Exploitation" Warning that "Instagram" Is "Linked to 'Rampant Sex Trafficking" and "Child Sexual Abuse"

167. On February 13, 2020, a presentation to the Board's Compensation Committee[160] attached a "Stockholder Proposal Regarding Child Exploitation" that

[155] *Id.*

[156] *Id.*

[157] META220_0003011.

[158] META220_0003012.

[159] META220_0003011.

[160] META220_0001663.

noted that "Facebook [is] being sued in a Texas court for facilitating sex trafficking of minors"; that "Instagram [is] being linked to 'rampant sex trafficking [and] child sexual abuse grooming'"; and that "Facebook may face significant regulatory risk if it cannot curb child sexual abuse on existing platforms":[161]

> Facebook and its subsidiaries have faced other recent controversies of child sexual exploitation, including:
>
> - Facebook being sued in a Texas court for ***facilitating sex trafficking of minors***;[162]
> - Instagram being linked to "***rampant sex trafficking***, ***child sexual abuse grooming***, as well as adult fetishization of young girls...", "sexually graphic comments on minor's photos" and allowing strangers to "direct message minors."[163]
> - Pedophiles "sharing Dropbox links to child porn via Instagram";[164]
>
> Facebook may face significant regulatory risk if it cannot curb child sexual abuse on existing platforms or on encrypted messaging. Senate Judiciary Committee member Marsha Blackburn stated in a December 2019 hearing that Facebook and peers need to "get your act together, or

---

[161] META220_0001850-1851.

[162] https://www.nytimes.com/2019/12/03/technology/facebook-lawsuit-section-230.html.

[163] https://endsexualexploitation.org/articles/statement-instagram-is-predators-paradise-says-international-group-of-human-rights-ngos/; https://endsexualexploitation.org/articles/senate-hearing-uncovers-sexploitation-in-apps-and-social-media/.

[164] https://www.dailymail.co.uk/news/article-6574015/How-pedophiles-using-Instagram-secret-portal-apparentnetwork-child-porn.html.

we will gladly get your act together for you.[165] Most of the Committee supported that sentiment.[166]

168. The presentation noted that this stockholder proposal "[r]equest[ed] that the Board issue a report by February 2021 assessing the risk of increased sexual exploitation of children as the company develops and offers additional privacy tools such as end-to-end encryption."[167] The same proposal was discussed in another presentation on the same day (February 13, 2020) titled "Board Updates & Approvals" for *"Directors Only*."[168]

I. May 2020 – Glass Lewis Recommends Voting "FOR" the Shareholder Proposal and Notes that "366 Federal Criminal Cases Over Seven Years Featured Suspects Using Facebook for Child Exploitation"

169. On May 27, 2020, Meta held its Annual Meeting of Shareholders. In connection with this meeting, the Board met and reviewed the "Proxy Analysis & Benchmark Policy Voting Recommendations" by Institutional Shareholder Services Inc. ("ISS"), a proxy advisory firm, in which ISS discussed the above-referenced stockholder proposal for a "Report on Online Child Sexual Exploitation" and ISS

---

[165] https://www.politico.com/news/2019/12/10/tech-companies-bipartisan-congress-encryption-080704.

[166] https://www.judiciary.senate.gov/meetings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy.

[167] META220_0001690.

[168] META220_0000001, META220_0000016.

recommended that the Board vote "FOR" the proposal and stated that "[a] vote FOR this proposal is warranted, as additional information on risks related to potential sexual exploitation of children through the company's platforms would give shareholders more information on how well the company is managing related risks."[169] ISS noted that "the board states that the requested report is unnecessary and recommends that stockholders vote against it."[170] However, ISS noted that in March 2020, the TTP had released a study identifying "366 federal criminal cases over seven years that featured suspects using Facebook for child exploitation":[171]

> In March 2020, the not-for-profit investigative group Tech Transparency Project [(TTP)] released a study called "Broken Promises: Sexual Exploitation of Children on Facebook." Results of the study have been published in The Guardian and elsewhere. By analyzing Department of Justice news releases from January 2013 through December 2019, the study finds that Facebook failed to catch hundreds of cases of child exploitation on its platform. The "top findings" section of the analysis states:
>
> - "The review identified ***366 federal criminal cases over seven years that featured suspects using Facebook for child exploitation***.
> - Only 9 percent of the cases were initiated because Facebook or the National Center for Missing and Exploited Children (which receives cyber tips from Facebook) reported them to authorities,

[169] META220_0002627, 2671.

[170] META220_0002672.

[171] META220_0002674.

> raising questions about the effectiveness of Facebook's monitoring of criminal activity targeting children."

170. Based on the above, ISS stated that "the company has experienced some recent controversy related to its alleged failure to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019."[172] Accordingly, ISS concluded that "[g]iven the potential financial and reputational impacts of potential controversies related to child exploitation on the company's platforms, shareholders would benefit from additional information on how the company is managing the risks related to child sexual exploitation, including risks associated with end-to-end encryption technologies. Therefore, this proposal merits shareholder support."[173]

171. Also in connection with the Board's May 27, 2020 Annual Meeting, Glass Lewis similarly recommended that the Board vote "FOR" the same shareholder proposal "[t]hat the Company report on the risk of increased sexual exploitation of children due to end-to-end encryption."[174] As it had in May of 2019 (*see* § III.I *supra*), Glass Lewis reminded the Board that the *BBC* had alerted Meta that "the Company's platform contained posts of sexually explicit or exploitative

---

[172] *Id.*

[173] *Id.*

[174] META220_0002725.

content and images" and "accounts maintained by convicted sex offenders, specifically pedophiles," and that of "100 images" reported, "only 18 were removed" and "none" of the "pedophiles[']" accounts "were disabled."[175] Glass Lewis also reminded the Board—like ISS's May 14, 2020 report—of the TTP's March 2020 report which "review identified 366 federal criminal cases over seven years that featured suspects using [Meta's] platform for child exploitation."[176] Glass Lewis further reminded the Board that the "passage of the FOSTA-SESTA law, which for the first time made [Meta] liable to civil penalties for sex trafficking on its platform," created "the potential for litigation." [177]

172. Glass Lewis noted how "[i]n October 2018, the Company announced work that it had done over the prior year to develop new technology to fight child exploitation, including photo-matching technology, and ***artificial intelligence and machine learning*** to proactively detect child nudity and previously unknown child exploitative content when it is uploaded."[178]

173. Glass Lewis further noted that "recent regulation has increased the level of legal and reputational risk related to this issue. Further, numerous investigations

---

[175] META220_0002728.

[176] *Id.*

[177] META220_0002729.

[178] *Id.*

by the media have demonstrated the wide extent of this problem on the platforms maintained by the largest tech companies, including the Company. As such, management of this issue is of critical importance for companies involved in the distribution of digital media and messaging over the internet."[179]

174. Glass Lewis concluded: "Accordingly, we do not believe that [Meta] has provided sufficient disclosure to demonstrate to shareholders that these risks will be managed as [Meta] expands its encrypted messaging services, nor do we have any reason to be assured that [Meta] will act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services." [180]

175. On May 28, 2020, the Board received a presentation titled "Board Updates & Approvals" for "*Directors Only*," which reviewed "Investor Feedback re: Governance Matters" and stated that "Investors were also interested i[n] . . . . Proposal 10 (Child Exploitation)."[181]

---

[179] *Id.*

[180] META220_0002729-30.

[181] META220_0000159, 0252.

J. December 2020 – the Audit Committee Learns that [redacted]

176. On December 2, 2020, the Board's Audit Committee held a meeting at which they received an "Agenda" presentation that informed them of several [redacted][182]

[182] META220_0006395, 6468, 6471, 6599, 6672, 6675.

177. As noted above, one [redacted] and in particular that the [redacted]

[redacted][184] In other words, despite frequently touting Meta's technological capabilities to use artificial intelligence ("AI") to detect harmful content,[185] the Company internally acknowledged to the Audit Committee that fo[redacted] Even worse, the Company also acknowledged that [redacted]

[183] Meta's website defines "ground truth data" as "***the foundation upon which we build models, generate inferences, and make decisions***. What is ground truth data? We define it as a dataset that contains the values we want to infer for a particular population of interest (the data could be human labels, survey data, behavioral data, etc.). Whether it is modeling user characteristics to ensure appropriate and personalized user experiences, ***detecting and removing harmful misinformation and hate speech***, or executing other data-driven tasks, the underlying ***machine learning processes*** rely on models trained and validated on some ground truth data." *See* https://research.facebook.com/blog/2022/8/-introducing-the-ground-truth-maturity-framework-for-assessing-and-improving-ground-truth-data-quality/.

[184] META220_0006468.

[185] *See, e.g.*, "F8 2018: Using Technology to Remove the Bad Stuff Before It's Even Reported" (May 2, 2018), available at https://about.fb.com/news/2018/05/removing-content-using-ai/; "Community Standards report" (Nov. 13, 2019) ("We have been making consistent progress in increasing the effectiveness of our AI systems to detect harmful content."), available at https://ai.facebook.com/blog/community-standards-report/; "Our New AI System to Help Tackle Harmful Content" (Dec. 8, 2021), available at https://about.fb.com/news/2021/12/metas-new-ai-system-tackles-harmful-content/.

[redacted][186]

178. Confronted with their utter failure to [redacted] communicated to the Audit Committee that [redacted][187]

179. Simply put, not only did Meta not use its [redacted] to address [redacted] but it did not use [redacted] This appears to be the same failure that was eventually revealed and corroborated on October 25, 2021, by *USA Today*, which reported that "[i]n at least one case, Facebook deactivated a tool that was proactively detecting exploitation, according to internal documents."[188]

---

[186] META220_0006468.

[187] *Id.*

[188] Terry Collins et al., *Live updates: Facebook papers whistleblower Frances Haugen testifies at Parliament*, USA TODAY (Oct. 25, 2021), available at https://www.usatoday.com/story/tech/2021/10/25/facebook-papers-whistleblower-testimony-frances-haugen/6120082001/.

180. Meta's internal admission to the Audit Committee that it did not [redacted] is remarkable given that the Company's 2020, 2021, and 2022 proxy statements, in recommending that shareholders vote "against"[189] the shareholder proposal for a report on Meta's "detection technologies and strategies" to prevent "sexual exploitation of children,"[190] the Company repeatedly claimed that "[w]e deploy technology across all of our platforms to proactively surface as much illegal child exploitative content as we can, including through detection technology, ***machine learning and artificial intelligence techniques***"[191]

181. The same presentation identified a further [redacted] with respect to Meta's [redacted][192]

[redacted]

[189] *See* Meta, Proxy Statement (DEF 14A) at 79 (Apr. 10, 2020); Meta, Proxy Statement (DEF 14A) at 76 (Apr. 9, 2021); Meta, Proxy Statement (DEF 14A) at 83 (Apr. 8, 2022).

[190] *See* Meta, Proxy Statement (DEF 14A) at 77 (Apr. 10, 2020); Meta, Proxy Statement (DEF 14A) at 74 (Apr. 9, 2021); Meta, Proxy Statement (DEF 14A) at 80 (Apr. 8, 2022).

[191] *See* Meta, Proxy Statement (DEF 14A) at 79 (Apr. 10, 2020); Meta, Proxy Statement (DEF 14A) at 75 (Apr. 9, 2021); Meta, Proxy Statement (DEF 14A) at 82 (Apr. 8, 2022).

[192] META220_0006471, 6675.

[redacted]

182. Specifically, the Audit Committee was informed that [redacted][193] [redacted][194] In other words, Meta's management [redacted] were unable to [redacted] and therefore they had been unable to [redacted]

[193] *Id.*

[194] *Id.*

[redacted][195] And Meta's management lacked [redacted]

[redacted][196]

183. On December 3, 2020, the Board received a presentation titled "Board Updates & Approvals" for "*Directors Only*"[197] which attached a letter from Harrington Investments Inc.,[198] regarding a "Shareholder Proposal Follow-up."[199] The letter stated that "Facebook is the world's #1 hub of reported child sexual abuse material" and that "94 percent" of online material "came from the Facebook platform":[200]

> ***Facebook is the world's #1 hub of reported child sexual abuse material (CSAM). In 2019, there were more than 16.9 million reports***

---

[195] *Id.*

[196] *Id.*

[197] META220_0000344.

[198] Harrington Investments, Inc., describe themselves as "a leader in Socially Responsible Investing and Shareholder Advocacy since 1982, dedicated to managing portfolios for individuals, foundations, non-profits, and family trusts to maximize financial, social and environmental performance." https://www.harringtoninvestments.com/.

[199] META220_0000467-0471.

[200] META220_0000469. The letter appears to have quoted statements made by shareholders in support of the shareholder resolutions that ISS and Glass Lewis recommended in May 2020 that the Board support. *See, e.g.*, https://www.iccr.org/shareholders-raise-alarm-facebook-agm-failure-address-encryption-concerns-will-boost-child-sexual#:~:text=They%20noted%20that%20Facebook%20is,came%20from%20the%20Facebook%20platform.

> ***of child sexual abuse material online and, of that, 15.8 million — or 94 percent — came from the Facebook platform***.....Reported incidents of child sexual exploitation and grooming.....increased dramatically from year to year over the past decade. The bottom line is that Facebook's efforts are not stopping these crimes against children -- including infants and toddlers -- on its platforms.

K. February 2021 – the Board Opposes the Renewed Stockholder Proposal and Learns that the Supreme Court Had Declined to Hear Meta's Appeal of the Texas Lawsuit by Victims of Trafficking

184. On February 11, 2021, the Board's Compensation Committee received a presentation regarding Meta's "2021 Annual Meeting of Stockholders Agenda."[201] The presentation attached and discussed a "Stockholder Proposal" which "[r]equest[ed] that the Board issue a report by February 2022 assessing the risk of increased sexual exploitation of children as the company develops and offers additional privacy tools such as end-to-end encryption. The report should address potential adverse impacts to children (18 years and younger) and to the company's reputation or social license and assess the impact of limits to detection technologies and strategies."[202] The shareholder proposal stated that "[t]he Facebook brand has been diminished in recent years due to the platform's use as a tool for gross disinformation, hate speech, and to incite racial violence. What was envisioned as a tool to connect people has led to many instances of human suffering and death.

[201] META220_0001010, 1063.

[202] META220_0001068; *see also* META220_0001156.

Management and the board have failed to take effective action to stem these abuses, which has resulted in a series of negative impacts including: . . . [o]ver 45 million images of child pornography and torture made public."[203]

185. The same presentation also attached a [redacted] dated February 5, 2021, by [redacted][204] The [redacted] informed the Committee that [redacted][205]

186. The same [redacted] further informed the Committee that [redacted][206]

[203] META220_0001162.

[204] META220_0001219.

[205] *Id.*

[206] META220_0001319.

187. Also on February 11, 2021, the Board received a presentation titled "Board Updates & Approvals" for "*Directors Only*"[207] that informed the Board of the same "Stockholder Proposal" discussed above requesting "that the Board issue a report by February 2022 assessing the risk of increased sexual exploitation of children as the company develops and offers additional privacy tools such as end-to-end encryption."[208] The same presentation set forth a [redacted] which stated:[209]

[redacted]

[207] META220_0004201.

[208] META220_0004214.

[209] *Id.*

[redacted]

188. Yet, as discussed herein, Meta's supposed [redacted] were not necessarily being used for [redacted] and therefore this statement was misleading to investors. *See supra* Section II.U; *see also infra* Section III.O.

189. The same February 11, 2021 presentation included a section titled [redacted] which acknowledged that Meta [redacted] and that its [redacted] in that regard [redacted].[210]

[redacted]

[210] META220_0004246.

L. May 2021 – the Board Learns that "Shareholder Proposals" Regarding "Child Exploitation" Had "Garnered the Most Attention" and Meta Issues a "2021 Anti-Slavery and Human Trafficking Statement" that Fails to Mention Sex Trafficking

190. On May 26, 2021, Meta held its Annual Meeting of Shareholders. In connection with the meeting, the Board met and reviewed a shareholder proposal similar to one it had received in 2020 seeking the Company to issue a report concerning child exploitation on Meta's platforms and providing supporting facts. The Board also reviewed similar recommendations by ISS and Glass Lewis, proxy advisors who each recommended (as they had in 2020) that shareholders vote "FOR" the proposal.[211]

191. On May 27, 2021, the Board received a presentation titled "Board Updates & Approvals" for "*Directors Only*"[212] which discussed "Investor Feedback re: Governance Matters" and noted that "Shareholder proposals that garnered the most attention were: Proposals 6 (Child Exploitation)."[213]

192. Also on May 27, 2021, the Compensation Committee received a presentation that similarly discussed "Investor Feedback re: Governance Matters"

---

[211] META220_0000885-886, 897, 916-920, 923-924, 926-927, 933, 938, 962-968, 991.

[212] META220_0003530.

[213] META220_0003595.

which noted that "Shareholder proposals ..... that garnered the most attention were: Proposals 6 (Child Exploitation)."[214]

193. The May 27, 2021 "Board Updates & Approvals" presentation included a discussion of "Key Policies Applicable to Directors" which listed Meta's "Anti-Slavery and Human Trafficking Statement" and noted that "[c]hanges/updates to policies marked in RED are being proposed for approval at the 5/26 [Audit Committee] meeting or 5/27 [Compensation Committee] meeting. Redlined versions of these policies have been included in the following slides for reference."[215] As indicated, the presentation included a "redlined" version of "Facebook's Anti-Slavery and Human Trafficking Statement," in which deletions were indicated in red in strikethrough font and additions were indicated in blue underlined font.[216]

194. Meta's 2021 Anti-Slavery and Human Trafficking Statement was also notable in that it ***did not*** discuss, focus on, or even comment on whether sex trafficking or sexual exploitation had been occurring on Meta's platforms. Instead, this statement focused on whether "modern slavery and human trafficking" were

[214] META220_0001380, 1385.

[215] META220_0003530, 3605.

[216] META220_0003625-30.

occurring within Meta's own business operations or in Meta's supply chains.[217] In this latter regard, Meta concluded, "[w]e consider the risks of modern slavery and human trafficking to be ***relatively low*** in our direct business operations as our direct workforce is largely comprised of professionally qualified or skilled personnel. However, we are aware that inherent and potential risks of modern slavery and human trafficking could be present in our supply chains."[218]

195. Meta's 2021 "Anti-Slavery and Human Trafficking Statement" is perhaps most noticeable in the language that the Board approved to be deleted and which had been in the earlier 2020 version of that statement. Specifically, Meta deleted the portion of language which stated that they remove content related to human trafficking:[219]

> ~~In an effort to disrupt and prevent harm, ***we remove content on Facebook that facilitates or coordinates the exploitation of humans, including human trafficking. We define human trafficking in our Community Standards as the business of depriving someone of liberty for profit. It is the exploitation of humans in order to force them to engage in commercial sex, labor, or other activities against their will***. It relies on deception, force and coercion, and degrades humans by depriving them of their freedom while economically or materially benefiting others.~~

[217] *Id.*

[218] META220_0003625.

[219] META220_0003629.

196. The final, published versions of Meta's 2020, 2021, and 2022 "Anti-Slavery and Human Trafficking Statement" remain available online and reflect Meta's deletions of the above language from the 2021 and 2022 versions.[220]

M. September 2021 – the Audit Committee Learns that [redacted] Including a [redacted] and [redacted]

197. On September 1, 2021, the Audit Committee held a "Zoom Meeting" during which the Board reviewed a presentation reviewing several [redacted] which concluded, among other things, that [redacted][221]

[redacted]

[220] Neither Meta's 2021 or 2022 Anti-Slavery and Human Trafficking Statements make any mention of "sex trafficking" or provide any attempt to define or refer to human trafficking as involving commercial sex or sexual exploitation. Instead, Meta blithely noted that "[w]e consider the risks of modern slavery and human trafficking to be relatively low in our direct business operations as our direct workforce is largely comprised of professionally qualified or skilled personnel." *See* ANTI-SLAVERY AND HUMAN TRAFFICKING STATEMENT 2021 available at https://s21.q4cdn.com/399680738/files/doc_downloads/2021/06/2021-Facebook's-Anti-Slavery-and-Human-Trafficking-Statement.pdf; ANTI-SLAVERY AND HUMAN TRAFFICKING STATEMENT 2022 available at https://s21.q4cdn.com/399680738/files/doc_downloads/2022/06/30/2022-Anti-Slavery-and-Human-Trafficking-Statement.pdf.

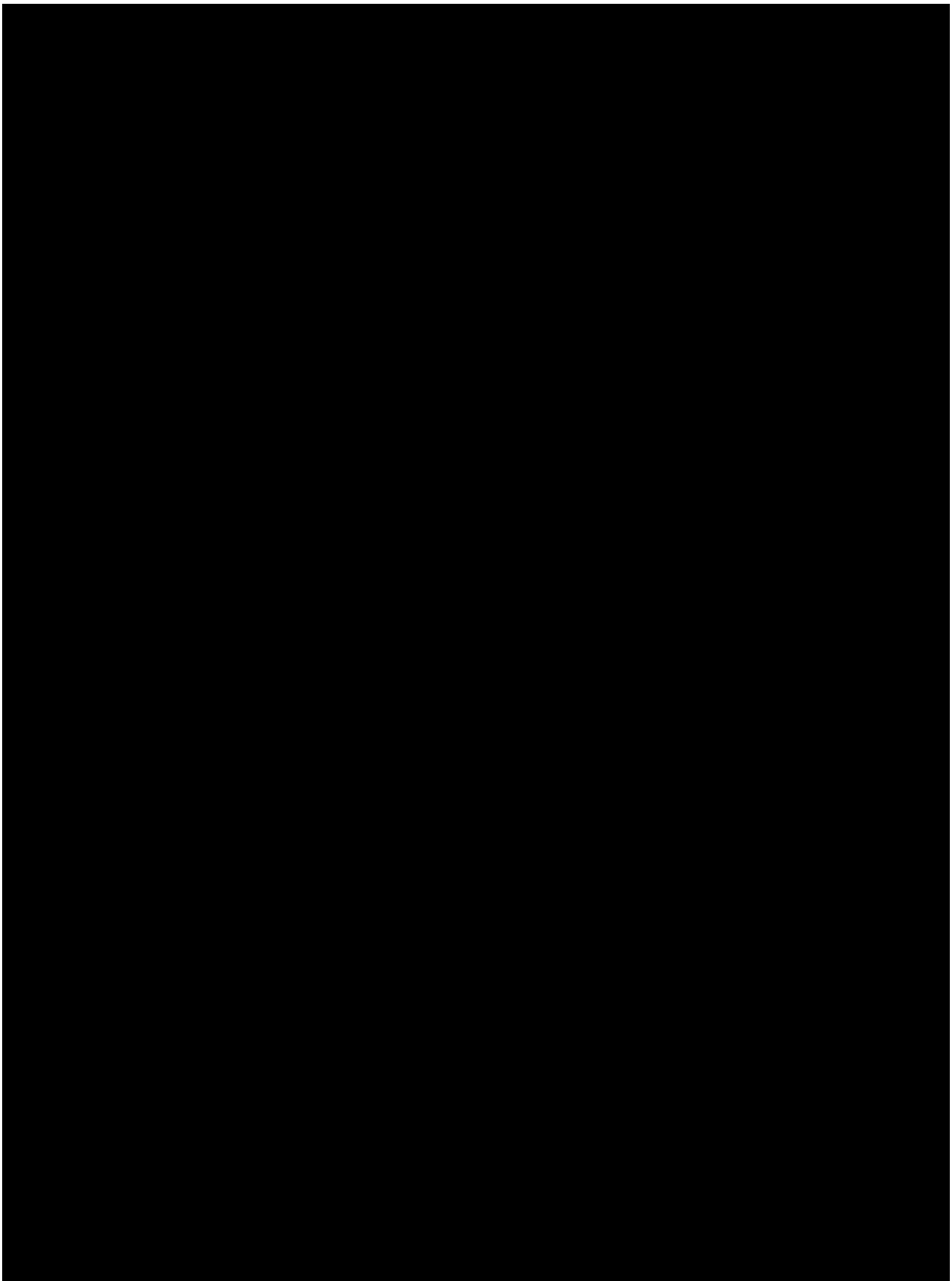
[221] META220_0004766, 4867; *see also* META220_0004968, 5069.

[redacted]

198. On another slide, the presentation identified several [redacted], including that [redacted]:[222]

[redacted]

[222] META220_0004907.



[redacted]

199. On another slide, the presentation identified the additional [redacted]:[223]

[redacted]

[223] META220_0004908.

200. On September 2, 2021, the Board received a presentation titled "Board Updates & Approvals" for "*Directors Only*."[224] The documents attached to the September 2, 2021 Board update included a letter dated May 25, 2021, from Matt Crossman of Rathbone Investment Management Ltd. to Defendant Zuckerberg.[225] In the letter, Mr. Crossman wrote:[226]

> With regard to the AGM [i.e., annual general meeting] planned for the 26th May 2021, we wish to formally notify the board of our intention to

[224] META220_0004350.

[225] META220_0004433-34.

[226] *Id.*

> voting against the recommendation of management on the following items:
>
> ***
>
> - Item 6: Report on Online Child Sexual Exploitation: We have determined to vote FOR this resolution.
>
> ***
>
> With regard to item 6, we have determined to vote against management by providing our support for the request that the company report on risks related to the sexual exploitation of children as it develops additional privacy tools, such as end-to-end encryption. Additional information on risks related to potential sexual exploitation of children through the company's platforms would give shareholders more information on how well the company is managing related risks, and we are generally in favour of improved disclosure.

201. Also on September 2, 2021, the Compensation Committee received a presentation[227] attaching the "ISS Proxy Analysis & Benchmark Policy Voting Recommendations" in which ISS stated, "[s]upport for the shareholder proposal requesting a report assessing risks related to the potential sexual exploitation of children through the company's platforms (Item 6) is warranted, as additional information would aid investors in assessing the company's management of related risks."[228]

[227] META220_0000813.

[228] META220_0000885.

N. December 2021 – the Board Learns that Meta's [redacted] and Meta Is "Wracked by Management Missteps and Lack of Board Oversight" and "Subject to Unparalleled Regulatory Scrutiny"

202. On December 8, 2021, the Audit Committee received a presentation [redacted][229]

[redacted]

203. The presentation stated that [redacted] and that [redacted][230] The presentation also noted that [redacted][231] The presentation further noted that [redacted][232]

[229] META220_0005477, 5529.

[230] META220_0005529.

[231] *Id.*

[232] *Id.*

204. On December 9, 2021, the Board received a presentation marked for "DIRECTORS ONLY"[233] that included a shareholder proposal stating that "***[t]he Meta (formerly Facebook) brand has continued to be wracked by management missteps and lack of Board oversight, resulting in continued harm by its platform including . . . . [l]ack of cooperation with authorities to prevent and detect child exploitation and abuse***."[234]

205. The proposal also told the Board that "[a] whistleblower complaint filed with the SEC argues that the Company has failed to adequately warn investors about the material risks of dangerous and criminal behavior . . . on its sites," and that Meta's "failure to control these activities reflects a grave lack of oversight by management and the board."[235]

206. The proposal also criticized and sought information regarding "the effectiveness of Meta's algorithms to locate and eliminate content that violates the Community Standards" and "the effectiveness of Meta's staff and contractors in locating and eliminating content that violates the Community Standards[.]"[236]

---

[233] META220_0004573.

[234] META220_0004673 (citing https://www.theguardian.com/technology/2021/jan/21/facebook-admits-encryption-will-harm-efforts-to-prevent-child-exploitation).

[235] META220_004673 (citing https://www.washingtonpost.com/technology/2021/10/22/facebook-new-whistleblower-complaint/).

[236] META220_0004674.

207. The proposal concluded that Meta's "enforcement of 'Community Standards' . . . has proven ineffective at controlling the dissemination of user content that . . . incites violence and/or harm to public health or personal safety."[237]

O. February 2022 – the Audit Committee Learns that Meta's [redacted] Have [redacted] and that [redacted]

208. On February 9, 2022, the Audit Committee held a meeting and reviewed a presentation titled "Audit & Risk Oversight Committee Agenda."[238] The presentation discussed Meta's [redacted][239] and, as part of that discussion, reviewed [redacted][.][240] One such [redacted] concerned Meta's [redacted] and found that Meta had [redacted][241]

209. In the same presentation, another [redacted] concerning Meta's [redacted] found that Meta had [redacted][.]"[242]

---

[237] META220_0004673.

[238] META220_0005786.

[239] META220_0005902.

[240] META220_0005919-5920, 5922.

[241] META220_0005919.

[242] META220_0005920.

210. Yet another [redacted] concerning Meta's [redacted] found, among other things, that (1) Meta's [redacted]; (2) Meta had an [redacted]; (3) [redacted]; and (4) [redacted][.]"[243]

211. With regard to [redacted], the presentation stated that [redacted][244] In other words, Meta internally acknowledged to the Audit Committee not only that [redacted]," but that at the same time, Meta did not have any [redacted] system that it could use for [redacted]. And while Meta was [redacted]

[243] META220_0005922.

[244] *Id.*

[redacted][245]

212. With regard to [redacted], the presentation stated that [redacted][246] In other words, Meta internally acknowledged to the Audit Committee that a [redacted]" but that this [redacted][.]"[247] Even worse, while Meta had developed a [redacted] Meta had not yet even [redacted][248]

[245] *Id.*

[246] *Id.*

[247] *Id.*

[248] *Id.*

213. Meta's acknowledgement to the Audit Committee that as of January 20, 2022, the Company did not yet have [redacted][249] is notable when considered alongside Meta's prior acknowledgement to the Audit Committee that as of December 2, 2020, the Company did not yet have a [redacted] to [redacted][250] Hence, in December 2020, Meta could not [redacted], and in January of 2022, Meta had no [redacted]—and apparently as a consequence, Meta had a [redacted]

214. On February 10, 2022, the Board held a "Q1 2022 Board of Directors Meeting"[251] during which the Board reviewed a presentation which described a "Shareholder Proposal" the Board had received and a [redacted]

[249] *Id.*

[250] META220_0006395, 6468.

[251] META220_0000481.

[redacted][252] On the same day, the Compensation Committee received the same slide, which is recreated below.[253]

Shareholder Proposals (cont.)

Shareholder Proposal	[redacted]
Report on child exploitation: Requests that the Board prepare a report assessing the risk of increased sexual exploitation of children as we implement privacy such as E2EE [i.e., end-to-end encryption].	[redacted]

215. The February 10, 2022 Board presentation also contained the text of the 2022 Shareholder Proposal regarding "Child Sexual Exploitation Online"[254] and the [redacted][255] In its [redacted] the

[252] META220_0000535.

[253] META220_0006803, 6848.

[254] META220_0000608-0609.

[255] META220_0000610-0612.

Board stated, [redacted][256]

IV. FIDUCIARY DUTIES OF THE DEFENDANTS

A. Defendants' Fiduciary Duties Under *Caremark*

216. By reason of their positions as directors, officers, and/or fiduciaries of Meta and because of their ability to control the business and corporate affairs of Meta, Defendants at all relevant times owed fiduciary duties to Meta and its stockholders, including the duties of care, loyalty, and good faith.

217. Under *Caremark* and its progeny, a board of directors of a Delaware corporation, as well as its officers, have the specific fiduciary duties to: (a) implement an information and reporting system and controls of compliance; and (b) oversee and monitor the operations of that information and reporting system.[257] Under the second prong of *Caremark*, directors and officers breach their fiduciary duty of loyalty if, having implemented a reporting and information system and

[256] META220_0000611.

[257] *In re Caremark Int'l. Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

controls, they consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.[258]

218. The *Caremark* duty is especially heightened with respect to the monitoring of fraudulent or criminal conduct, as opposed to other, more general business risks. As the Delaware Court of Chancery has stated, "[d]irectors should, indeed must under Delaware law, ensure that reasonable information and reporting systems exist that would put them on notice of fraudulent or criminal conduct within the company. Such oversight programs allow directors to intervene and prevent frauds or other wrongdoing that could expose the company to risk of loss as a result of such conduct."[259]

219. Moreover, the Delaware Court of Chancery has recently confirmed that *Caremark* duties extend to corporate officers. As Vice Chancellor Laster noted, "[t]he same policies that motivated Chancellor Allen to recognize the duty of oversight for directors apply equally, if not to a greater degree, to officers. The Delaware Supreme Court has held that under Delaware law, corporate officers owe

[258] *Stone v. Ritter*, C.A. No. 1570-N, 2006 WL 302558, at *1-2 (Del. Ch. 2006), *aff'd sub nom. Stone ex rel. AmSouth Bancorporation v. Ritter*, 911 A.2d 362, 370, (Del. 2006).

[259] *In re Citigroup Inc. S'holder Deriv. Litig.*, 964 A.2d 106, 131 (Del. Ch. 2009).

the same fiduciary duties as corporate directors, which logically include a duty of oversight."[260]

220. As noted above, it is an axiomatic tenet of Delaware corporate law that Delaware corporations may only pursue "lawful business" by "lawful acts." 8 *Del. C.* §§ 101(b), 102(a)(3). "Delaware law does not charter law breakers. Delaware law allows corporations to pursue diverse means to make a profit, subject to a critical statutory floor, which is the requirement that Delaware corporations only pursue 'lawful business' by 'lawful acts.' As a result, a fiduciary of a Delaware corporation cannot be loyal to a Delaware corporation by knowingly causing it to seek profit by violating the law."[261]

221. Here, one of the most significant risks Meta faced was legal and regulatory compliance. Defendants were well aware that Meta was at a heightened risk for running afoul of these requirements because of multiple governmental departments' keen focus on sex/human trafficking and child exploitation on Meta's online platforms and those platforms' roles in promoting and facilitating the recruitment of trafficking victims. Accordingly, Defendants were required to be

---

[260] *In re McDonald's Corp. S'holder Deriv. Litig.*, --- A.3d ---, 2023 WL 407668, at *1 (Del. Ch. Jan. 26, 2023).

[261] *In re Massey Energy Co. Derivative & Class Action Litig.*, C.A. No. 5430-VCS, 2011 WL 2176479, at *20 (Del. Ch. May 31, 2011) (quoting 8 *Del. C.* §§ 101(b), 102(a)(3), (b)(7)).

especially vigilant that the proper systems were in place to detect and deter such illegal conduct.

222. As set forth in greater detail below, Defendants breached their fiduciary duties by both failing to implement any adequate information reporting systems or controls to detect, prevent, and address sex/human trafficking and child exploitation (under the first prong of *Caremark*); and, to the extent any such ostensible systems or controls may have existed (if only nominally), by failing to oversee and monitor such systems or controls (under the second prong of *Caremark*). As alleged in Sections IV.A to IV.C *infra*, Defendants owed very specific responsibilities to monitor their information and reporting systems for fraudulent and criminal conduct and to ensure that the Company's business practices complied with all legal and regulatory requirements. Moreover, these responsibilities indisputably were known by Defendants. In conscious disregard of these responsibilities, Defendants failed to monitor or oversee the operations of Meta's information and reporting system, thereby disabling themselves from being informed of the non-compliance and fraudulent/unlawful sales practices. By failing to act in the face of a known duty to act, and by demonstrating a conscious disregard for their responsibilities, Defendants failed to act in good faith and breached their fiduciary duty of loyalty.

B. The Audit Committee's Charter Gave the Audit Committee Defendants the Specific Duty to Oversee Legal and Regulatory Compliance, Community Safety and Security, and Content Governance

223. In June 2018, Facebook announced that it changed its Audit Committee Charter to cover risk oversight responsibilities like data privacy, community safety, and cybersecurity. Defendant Bowles, Chair of the Audit Committee at that time, made the statement that "Facebook has grown significantly since going public, and so has the role of the audit committee, especially its role managing risk oversight. To reflect this, the Board updated the Audit Committee's charter to clarify how its role has grown, as well as to address other evolving issues, particularly in the areas of privacy and data use, community safety and security, and cyber-security."[262] At that time, the Audit Committee was renamed the Audit & Risk Oversight Committee (which is referred to herein as the "Audit Committee").

224. The Charter of the new Audit Committee (effective June 14, 2018) (the "2018 Charter") stated that the purpose of the Audit Committee was "to oversee (A) the independence, qualifications, and performance of the independent auditor, (B) the accounting and financial reporting processes of the Company and the audits of the financial statements of the Company, (C) the Company's internal audit function, and (D) certain risk exposures of the Company." Because the

[262] https://www.axios.com/2018/06/14/facebooks-board-expands-role-of-a-1529004696.

responsibilities and duties of the Audit Committee are set forth in its Charter, the members of the Board indisputably were aware of these duties.

225. The Audit Committee is required to meet no less frequently than once each quarter, "or more frequently, as determined appropriate by the Committee." Furthermore, the Committee, "in discharging its responsibilities, may conduct, direct, supervise or authorize studies of, or investigations into, any matter that the Committee deems appropriate, with full and unrestricted access to all books, records, documents, facilities and personnel of the Company." Further, the Committee "has the sole authority and right, at the expense of the Company, to retain legal and other consultants, accountants, experts and advisers of its choice to assist the Committee in connection with its functions, including any studies or investigations." In other words, the Audit Committee is provided the necessary access to management and to the internal auditor in order to fulfill the Committee's responsibilities.

226. Among its responsibilities, the Audit Committee is required to oversee the internal audit function. As part of this responsibility, the Audit Committee is required to "oversee the activities of the Company's internal audit function, including review of any process of appointment and/or replacement of the senior employee in charge of the internal audit function." Further, the "Committee will periodically meet separately with the internal audit function out of the presence of the Company's management."

227. A key responsibility assigned to the Audit Committee under the 2018 Charter is to oversee risk. As part of this responsibility, the Audit Committee is responsible for overseeing the management of the below major risk exposures set forth in the 2018 Charter:

1. *Financial and Enterprise Risk*. The Committee will review with management, at least annually, the Company's major financial risk and enterprise exposures and the steps management has taken to monitor or mitigate such exposures, including the Company's procedures and any related policies with respect to risk assessment and risk management.

2. **Legal and Regulatory Compliance.** ***The Committee will review with management, at least annually, (a) the Company's program for promoting and monitoring compliance with applicable legal and regulatory requirements, and (b) the Company's major legal and regulatory compliance risk exposures and the steps management has taken to monitor or mitigate such exposures, including the Company's procedures and any related policies with respect to risk assessment and risk management.***

3. *Privacy and Data Use*. The Committee will review with management, at least annually, (a) the Company's privacy program, (b) the Company's compliance with its consent order with the U.S. Federal Trade Commission, as well as the laws, and (c) the Company's major privacy and data use risk exposures and the steps the Company has taken to monitor or mitigate such exposures, including the Company's procedures and any related policies with respect to risk assessment and risk management.

4. **Community Safety and Security.** ***The Committee will review with management, at least annually, the Company's assessment of the major ways in which its services can be used to facilitate harm or undermine public safety or the public interest, as well as the steps the Company has taken to monitor or mitigate such abuse, including the Company's procedures and any related policies with risk to risk assessment and risk management.***

5. *Cybersecurity*. The Committee will review with management, at least annually, the Company's cybersecurity risk exposures and the steps the Company has taken to monitor or mitigate such exposures, including the Company's procedures and any related policies with respect to risk assessment and risk management.

6. *Other Risk Oversight*. The Committee will periodically review with management the Company's risk exposures in other areas, as the Committee deems necessary or appropriate from time to time.

228. In December 2020, section *(d) Community Safety and Security* was amended to reference Meta's monitoring of "content": "The Committee will review with management, at least annually, the Company's assessment of the major ways in which its services can be used to facilitate harm or undermine public safety or the public interest, ***including through the sharing of content on its services that violate the Company's policies***, as well as the steps the Company has taken to monitor, mitigate, and prevent such abuse."

229. In 2021, Meta changed the title of this section from "Community Safety and Security" to "Social Responsibility," stating that:

> The Committee will review with management, (a) at least annually, the Company's assessment of the major ways in which its services can be used to facilitate harm or undermine public safety or the public interest, including through the sharing of content on its services that violate the Company's policies, as well as the steps the Company has taken to monitor, mitigate, and prevent such abuse, and (b) from time to time, such other program, policies, and risk exposures related to social responsibility as the Committee deems necessary or appropriate.

230. These responsibilities are affirmed in Meta's proxy statement disclosures. According to Meta's 2022 Annual Proxy Statement filed with the SEC

on April 8, 2022,[263] the "Principal Responsibilities" of the Audit Committee include "[r]eviewing our program for promoting and monitoring compliance with applicable legal and regulatory requirements," and "[o]verseeing our major risk exposures (including in the areas of financial and enterprise risk, legal and regulatory compliance, environmental sustainability, social responsibility (including content governance, community safety and security, human rights, and civil rights), and cybersecurity) and the steps management has taken to monitor and control such exposures, and assisting our board of directors in overseeing the risk management of our company."[264]

231. Under the Audit & Risk Oversight Committee Charter, effective as of September 8, 2022 ("2022 Charter"),[265] one of the Audit Committee's principal duties is to monitor the Company's financial statements and disclosures. As part of this responsibility, the Audit Committee is required to:[266]

a. Meet to review and discuss with the independent auditor and the Company's management the Company's quarterly financial statements and annual audited financial statements, including the Company's specific disclosures under "Management's Discussion and Analysis of Financial Condition and Results of Operations."

---

[263] https://www.sec.gov/Archives/edgar/data/1326801/000132680122000043/meta2022definitiveproxysta.htm.

[264] *Id.* at 21.

[265] https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2022/09/Audit-and-Risk-Oversight-Committee-Charter-(9.8.2022).pdf.

[266] *Id.* at 3-4.

b. The Committee will be responsible for recommending to the Board whether the annual audited financial statements should be included in the Company's annual report on Form 10-K.

c. The Committee will cause to be prepared and review a report to the Company's stockholders for inclusion in the Company's proxy statement as required by the Commission Rules.

d. The Committee will discuss with the independent auditors and they Company's management any items appropriate or required to be discussed in accordance with applicable PCAOB standards in connection with the preparation of financial statements of the Company.

232. The responsibilities set forth above in the 2022 Charter, and affirmed in the Company's proxy statement disclosures, clearly encompass oversight of the Company's compliance with criminal laws, regulatory compliance, and community safety and security.

C. Additional Duties Imposed by Meta's Corporate Governance Guidelines and Code of Conduct

233. All of the Director Defendants became fully aware of their responsibilities and duties to oversee and monitor the Company for compliance risks when they joined the Board. Meta's Corporate Governance Guidelines state that "these Corporate Governance Guidelines . . . reflect the Board's strong commitment to sound corporate governance practices and . . . encourage effective policy and decision making at both the Board and management level, with a view to enhancing long-term value for Meta shareholders."[267] The Corporate Governance Guidelines

[267] Meta, Corporate Governance Guidelines (Amended as of Apr. 3, 2022) at 1,

also provide that "[e]ach member of the Board is expected to spend the time and effort necessary to properly discharge such director's responsibilities." *Id.*

234. According to the Company's Code of Conduct one of the five principles that guide Meta's work includes "[k]eep[ing] people safe and protect[ing] privacy—we are committed to protecting our communities from harm."[268] The Code of Conduct specifically applies to "[m]embers of the Board of Directors, officers, and employees of Meta, as well as contingent workers (including vendor workers, contractors and independent contractors)[.]"[269]

235. The Code of Conduct specifically exhorts employees to:

- Consider a broad range of potential impacts on people, communities and society, looking across different dimensions of responsibility, such as inclusion, safety, privacy and others[.]
- Raise and address potential harms early and often throughout the product development process[.]

---

available at https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2022/04/Meta-Corporate-Governance-Guidelines-(April-3-2022).pdf;

see also Facebook, Corporate Governance Guidelines (Amended as of Dec. 3, 2020) at 1.

[268] Meta, Keep Building Better: The Meta Code of Conduct [effective September 7, 2022] at 5, available at file:///L:/S&CF/471%20-%20Derivative/Facebook%20Human%20Trafficking%20(1000380.000)/Hickey/220%20Cx/Cited%20or%20Quoted/20220907_Meta_Code_of_Conduct.pdf; *see also* Facebook, Keep Building Better: The Facebook Code of Conduct at 5, available at 5 https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/2021/06/FB-Code-of-Conduct.pdf.

[269] *See* sources cited *supra* note 269, at 6.

- Seek out expert voices, diverse perspectives and the resources and tools we have at Meta to inform our decisions[.]
- Engage in necessary reviews, such as Privacy Review and Integrity XFN review[.]
- Work quickly to identify and remove harmful content from Meta platforms, such as hate speech, harassment, child exploitation, threats of violence and terrorism[.]
- Design and build products that prioritize safety, privacy, provide appropriate warnings where necessary and articulate instructions for safe and responsible use[.]

236. The Code of Conduct specifically states that "we have a legal obligation to report to the National Center for Missing and Exploited Children any apparent violation of laws pertaining to child exploitation imagery."[270] The Code of Conduct further states that "[w]e have teams that are specially trained to review, escalate and report this [CEI] content, which must be done in a secure manner exposing the fewest people to this material." *Id.* In contrast, Meta's Code of Conduct fails to recognize any legal obligation to address human trafficking, nor does Meta list any teams that are specially trained to review, escalate, or report content related to human trafficking.

[270] *Id.* at 30.

V. DEFENDANTS' BREACHES OF FIDUCIARY DUTY

A. Meta's Rampant Promotion and Facilitation of Sex/Human Trafficking and Child Exploitation Is a Mission-Critical Risk that Exposes Meta, Its Board, and Its Executives to Criminal/Civil Liability, Regulatory Risk, and Reputational Harm

237. The fact that Meta's platforms promote and facilitate rampant sex/human trafficking and child exploitation is a mission-critical risk that exposes the Company, its executives, and its Board to criminal and civil liability, regulatory risk, as well as monetary and reputational harm.

238. ***First***, as noted above (*see* Sections I.A to I.D *supra*), numerous federal and state statutes make sex/human trafficking a crime. *See, e.g.*, 18 U.S.C. § 1591(a); 11 *Del. C.* § 787(b). In that regard, in response to the same sort of rampant sex trafficking that has occurred and continues to occur on Meta's platforms, Congress passed FOSTA-SESTA, which makes it a crime to "own[], manage[], or operate[] an interactive computer service . . . with the intent to promote or facilitate the prostitution of another person" as well as to "act[] in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of [section] 1591(a)" and subjects violators to statutory fines and/or up to 25 years in prison. 18 U.S.C. § 2421A(a), (b)(2).

239. ***Second***, federal law exposes internet service providers who facilitate trafficking to civil liability. In that regard, FOSTA-SESTA states that "[a]ny person injured by reason of a violation of section 2421A(b) may recover damages and

reasonable attorneys' fees in an action before any appropriate United States district court" and that "in addition to any other civil or criminal penalties authorized by law, the court shall order restitution for any violation of subsection (b)(2)." 18 U.S.C. § 2421A(c)-(d).

240. ***Third***, the extent of Meta's facilitation of, and reckless disregard toward, trafficking on its platforms, as revealed by Ms. Haugen's whistleblower complaints, led to a securities fraud class action titled *Ohio Public Employees Retirement System v. Meta Platforms, Inc.*,[271] as a result of which Meta and its officers and directors face substantial risk of liability and as a result of which the Company is incurring substantial legal costs.

241. ***Fourth***, also as a result of Meta's promotion and facilitation of sex/human trafficking on its platforms—as revealed by Ms. Haugen's whistleblower complaints, federal and state case law, reports by the news media, and Congressional and Parliamentary hearings and other negative publicity—Meta has faced substantial reputational damages, and as a result, declining users, declining revenue, increased regulatory risk, and a declining stock price.

[271] No. 21-cv-08812-JST (N.D. Cal. filed Nov. 12, 2021), consol. sub nom. *In re Meta Platforms, Inc. Sec. Litig.*, No. 21-cv-08812-JST (N.D. Cal. filed Oct. 28, 2022).

242. ***Fifth***, numerous federal and state laws also make the sexual exploitation and abuse of children a crime. *See, e.g.*, 18 U.S.C. §§ 2251-2260A. Internet service providers who commit such crimes are not protected by Section 230 of the CDA. *See* 47 U.S.C. § 230(e)(1). Yet, an accumulating mass of federal and state case law and news reports shows a raging epidemic of child sexual exploitation occurring—openly and unchecked—on Meta's platforms. Meta's internal documents demonstrate the Board and management's utter failure to provide the oversight necessary to address this growing problem. As a result, Meta has faced substantial reputational damages, and as a result, declining users, declining revenue, increased regulatory risk, and a declining stock price.

243. Thus, for all the reasons set forth above, Meta's compliance with federal and state laws prohibiting sex/human trafficking, as well as the sexual exploitation and abuse of children—and particularly by internet service providers—was and is an essential mission-critical risk; the Board thus has had an imperative duty to make a good faith effort to put in place a reasonable board-level system of monitoring and reporting, and having implemented such a system, not to consciously fail to monitor or oversee its operations in the face of waving red flags.

B. Meta's Complete Lack of Any Board or Committee Minutes Discussing Sex/Human Trafficking or Child Exploitation Demonstrates the Board's Utter Failure to Implement Any Board-Level Monitoring, Reporting, or Oversight for These Risks

244. As noted above,[272] in responses to Plaintiffs' books-and-records demands, Meta agreed that "[t]he Company will search for materials provided to the Board and Board minutes since January 1, 2017 relating to the two topics of (i) sex and human trafficking and (ii) teen health, including excerpts of minutes of meetings of the board of directors (or committees of the board) that reflect discussion of those two subjects . . . ."[273] Yet, in responses to Plaintiffs' books-and-records demands—and despite this promise—Defendants produced no minutes whatsoever of any meeting by either the Board, the Audit Committee, or any other committee of the Board.

245. As reflected by the complete lack of minutes discussing sex/human trafficking, child sexual exploitation (or any other subject), it is evident that the Board and the Audit Committee consciously failed to monitor or oversee Meta's operations insofar as they concern sex/human trafficking or child sexual exploitation.

[272] *See* ¶¶ 16, 56-60 *supra*.

[273] Letter from David E. Ross to William S. Norton (Dec. 14, 2021) at 4.

246. This failure is even more notable when one considers how many times the Board met between 2017 and 2021. In 2017, the Board met five times and the Audit Committee met ten times. In 2018, the Board met twelve times and the Audit Committee met eleven times. In 2019, the Board met 13 times and the Audit Committee met ten times. In 2020, the Board met 15 times and the Audit Committee met nine times. In 2021, the Board met 12 times and the Audit Committee met ten times.

247. Throughout these many meetings, the Board and the Audit Committee had ample opportunity to discuss the fact that sex/human trafficking, and child sexual exploitation had been running rampant on Meta's platforms—yet, they utterly failed to do so.

C. Ignoring Glaring Red Flags, the Board Utterly Failed to Implement Any System or Controls to Address the Rampant Sex/Human Trafficking on Meta's Platforms or Consciously Failed to Monitor or Oversee Whatever Controls May Have Existed

248. ***First***, the Board and management saw glaring red flags—in the form of shareholder proposals published in Meta's proxy statements—that put the Board on actual notice that, among other things: "Facebook . . . facilitate[ed] sex trafficking of minors"; "Instagram [was] linked to 'rampant sex trafficking'"; that "94 percent" of "Child Sexual Abuse Material" online "stem[s] from Facebook and its platforms, including Messenger and Instagram"; and that "[i]n 2020, 79 percent of U.S.

underage sex trafficking victims recruited online were recruited through Facebook or Instagram." *See* ¶¶ 111, 169, 115, 139 *supra*.

249. Moreover, two of the Board's proxy advisors, ISS and Glass Lewis, informed the Board—in recommending that the Board support the shareholder proposals mentioned above—that, among other things, that a TTP study identified "366 federal criminal cases over seven years that featured suspects using Facebook for child exploitation," and in May of 2019, although the *BBC* had alerted Meta that "the Company's platform contained posts of sexually explicit or exploitative content and images" and "accounts maintained by convicted sex offenders, specifically pedophiles," and that of "100 images" reported, "only 18 were removed" and "none" of the "pedophiles[']" accounts "were disabled." *See* ¶¶ 162, 171, 173 *supra*.

250. In addition, between 2013 and 2023, at least 70 federal and state courts have issued written decisions in criminal and civil cases involving sex trafficking on Meta's platforms. Likewise, Meta's widespread and ubiquitous facilitation of sex trafficking and human trafficking was reported in more than 175 articles published in U.S. newspapers and other media outlets between 2009 and 2022. *See* Sections II.B & II.A *supra*.

251. ***Second***, that the Board did not monitor, discuss, or address sex/human trafficking is demonstrated by the fact that, as discussed above, Meta has absolutely

no minutes from any meeting of the Board, the Audit Committee, or any other committee discussing sex/human trafficking or child sexual exploitation.

252. ***Third***, the Board had no regular process or protocols requiring management to apprise the Board of issues relating to sex trafficking, human trafficking, or even child safety or exploitation; instead, the Audit Committee only received intermittent, *ad hoc*, management-initiated communications regarding child safety—but no reports whatsoever regarding the extent of sex trafficking or human trafficking on Meta's platforms, and no reports or indications whatsoever of any efforts or initiatives to detect, prevent, or address such trafficking.

253. ***Fourth***, Meta's management saw glaring red flags that Meta's platforms facilitated widespread sex/human trafficking and child sexual exploitation but those additional red flags apparently never reached the Board due to the lack of reporting structure or oversight. In that regard, on October 23, 2019, Meta "received communication from Apple where the company threatened to pull FB & IG apps from its App Store due to them identifying content promoting 'domestic servitude.'" In response, according to Meta's records, Meta's management concluded that that "Facebook's statements about human trafficking were false" because, among other things, Meta internally acknowledged that Meta suffered from an "absence of proactive detection"; Meta had been "under-enforcing on confirmed abusive activity with a nexus to the platform"; and that Meta's own "investigative findings

demonstrate that our platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks."

VI. META HAS SUFFERED SIGNIFICANT DAMAGE AS A RESULT OF DEFENDANTS' BREACHES

254. As a result of Defendants' breaches, Meta has suffered significant reputational harm as the Company has failed to address the widely known and publicized use of its social media platforms for human and child sex trafficking as described above. TechCrunch reported that in February 2022, the Company announced it had lost daily active users for the first time in the Company's history. In addition, *Bloomberg* reported in October 2021 in the wake of Frances Haugen's whistleblower revelations that U.S. teenagers were spending less time on Facebook, and the number of new teens signing up for Facebook accounts was also declining.

255. Because of Defendants' failures to address the ongoing criminal trafficking activity via the use of Meta's social media products, the severity of which was at least partially revealed by Frances Haugen's, *The Wall Street Journal's*, and *CBS News's* disclosures in September and October 2021, the Company is also exposed to significant potential liability in the pending securities class action styled *In re Meta Platforms, Inc. Securities Litigation*.[274]

[274] No. 21-cv-08812-JST (N.D. Cal.).

256. On October 28, 2022, the Lead Plaintiffs in *In re Meta* filed a detailed, 195-page consolidated amended complaint.[275] The *In re Meta* complaint alleges, among other things, that "[t]hroughout the Class Period, Meta made statements that the Company was able to, and in fact did, stop its platforms from being used to facilitate and promote human trafficking" but "in truth, Meta failed to 'fix[] systems that allowed' traffickers to operate despite extensive information concerning their activities and opportunities to remove that content" and that "as *The Wall Street Journal* reported, after a Meta team spent more than one year [in 2018/2019] investigating human trafficking in the Middle East, an internal document [from 2021] warned Meta to be cautious with statements against human trafficking in order to not 'alienate buyers' [i.e., buyers of enslaved domestic workers] who used Meta's platforms."[276]

257. As a result of these and other misrepresentations by Meta about its policies and practices concerning human trafficking and sex trafficking (and other forms of harmful content) and the eventual revelation of the truth regarding Meta's true policies and practices, the *In re Meta* complaint alleges that "[f]rom the date of

[275] Lead Pls.' Consol. Am. Class Action Compl. for Violations of the Federal Securities Laws, *In re Meta*, No. 4:21-cv-08812-JST (N.D. Cal. Oct. 28, 2022) (ECF No. 97).

[276] *Id.* at ¶¶ 413-14.

the first article published by *The Wall Street Journal* on September 13, 2021, to the final disclosures on October 21, 2021, Meta's stock price declined by $54.08 per share, or over 14%, representing ***a total decline of more than $130 billion in Meta's market capitalization***[.]"[277]

258. Of particular relevance to this case, the *In re Meta* complaint alleges that as a result of *The Wall Street Journal's* September 16, 2021 article, which revealed that "human traffickers used Facebook to facilitate their criminal enterprises, and that content violating the Company's domestic servitude policy routinely makes its way on to Meta's platforms without deletion,"[278] Meta's stock price suffered a "***single-day drop [that] erased over $2 billion of Meta's market capitalization***."[279]

259. Similarly, the *In re Meta* complaint also alleges that Meta stock dropped from a closing price of $343.01 on October 1, 2021, to a closing price of $326.23 on October 4, 2021, a steep decline of $16.78 or more than 4%—a stock "drop [that] ***eliminated nearly $40 billion of Meta's market capitalization in a single business day***,"[280] following the revelations (1) on October 3, 2021, that

[277] *Id.* at ¶ 514.

[278] *Id.* at ¶ 318.

[279] *Id.* at ¶ 319.

[280] *Id.* at ¶ 349.

"Facebook whistleblower, Frances Haugen, [gave] two in-depth interviews with *60 Minutes* and *The Wall Street Journal* in advance of her congressional testimony";[281] and (2) that "on October 4, 2021, *CBS News* released the eight whistleblower complaints that Frances Haugen filed with the SEC,"[282] which included Haugen's complaint detailing how Meta "misled investors and the public about its promotion of human trafficking / slavery / servitude."

260. As a result of the Board's utter failure of oversight, leading to the Company's widespread facilitation of human trafficking and sex trafficking, and misrepresentations to its shareholders and the marketplace about its policies and practices concerning human/sex trafficking, Meta now faces massive liability to its shareholders in *In re Meta*, and has already began incurring substantial legal costs of its defense.

261. In addition to *In re Meta*, the Company also faces liability and has been incurring legal costs as a result of *In re Facebook, Inc*., 2021 WL 2603687, a case brought against Meta by three victims of sex trafficking who alleged that Meta "'knows its system facilitates human traffickers in identifying and cultivating victims,' but has nonetheless 'failed to take any reasonable steps to mitigate the use

[281] *Id.* at ¶ 514.

[282] *Id.* at ¶ 351.

of Facebook by human traffickers' because doing so would cost the company users and the advertising revenue those users generate."[283] Meta's costs include at least two state court appeals and one attempted appeal to the U. S. Supreme Court, which have thus far proved unsuccessful in dismissing the victims' case against Meta.

VII. DERIVATIVE ALLEGATIONS

262. Plaintiffs bring this action derivatively to redress injuries suffered by the Company as a direct result of the breaches of fiduciary duty and other breaches by Defendants.

263. Plaintiffs have owned Meta stock continuously during the time of the wrongful course of conduct by the Defendants alleged herein and continue to hold Meta stock.

264. Plaintiffs will adequately and fairly represent the interests of Meta and its stockholders in enforcing and prosecuting the Company's rights.

VIII. DEMAND ON THE BOARD IS EXCUSED BECAUSE IT IS FUTILE

265. Plaintiffs have not made a demand on Meta's Board to bring suit asserting the claims set forth herein because pre-suit demand is excused as a matter of law.

266. Meta's Demand Board consists of nine directors: Defendant Zuckerberg, Defendant Sandberg, Defendant Alford, Defendant Andreessen,

[283] *Facebook Cert.*, 142 S. Ct. at 1088 (2022).

Defendant Houston, Defendant Killefer, Defendant Kimmitt, and Defendant Travis. As set forth below, with respect to the claims for relief asserted by Plaintiffs, at least half the Board is not disinterested and independent.

A. At Least Half of Meta's Demand Board Faces a Substantial Risk of Liability

267. Every one of the Demand Board members is a Defendant and faces a substantial risk of liability as a result of their failure to conduct oversight concerning, and to address, the use of Meta's social media platforms for human trafficking and child exploitation.

268. Each of the Demand Board members knew that significant criminal activity involving sexual exploitation and human trafficking was taking place on Facebook and Instagram. The evidence of such activity was everywhere. As described in Section II.A, the involvement of both platforms in such activity was well publicized by the media, with over 175 articles published in the past decade in the United States detailing how sex/human traffickers have systematically used Facebook to commit their heinous crimes. Hundreds of criminal cases have been filed against criminals who conducted their crimes using the platforms. In presentations to the Board, Facebook's management signaled that the problems were persistent and growing more severe. Facebook's own founder and CEO was repeatedly questioned about Facebook's lack of response by members of Congress. And in October 2021, a whistleblower went public to make clear that Facebook—

despite its representations—did *not* have controls in place sufficient to control human trafficking. The members of the Demand Board were well aware that the Company did not have the controls in place to halt such activity.

269. The misconduct that gives rise to this action was perpetrated both by management and the Board and constitutes knowingly and consciously presiding over rampant criminal activity within Meta's products. For years, the Board has consciously turned a blind eye to systemic evidence of sex/human trafficking and child sexual exploitation. Because every member of the Demand Board faces a substantial likelihood of liability as Defendants in this action, demand on the Board is excused as futile.

Zuckerberg

270. Defendant Zuckerberg is the CEO, chairman, and founder of Facebook and its parent company, Meta. Zuckerberg has served as CEO and as a member of the Board since he created the Company in 2004; he has served as Chairman of the Board since 2012. Zuckerberg is also Meta's controlling shareholder.

271. As CEO and Chairman, Zuckerberg had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities. *See supra* Sections IV.B to IV.C. Zuckerberg was on the Board when it was repeatedly

advised—through the media,[284] by proxy advisors,[285] and by other stockholders—about the pernicious conduct occurring on Meta's platforms.

272. Zuckerberg was also on the Board when it was told by management that:

- Congress would be pushing for Section 230 immunity because of concerns over sex trafficking on internet sites (December 2017);
- Facebook had [redacted] (2019);
- A narrative had developed that [redacted] (September 2019);
- A stockholder proposal was asserting that Facebook was being sued for "facilitating sex trafficking of minors"; that "Instagram [is] being linked to 'rampant sex trafficking [and] child sexual abuse grooming'"; and that "Facebook may face significant regulatory risk if it cannot curb child sexual abuse on existing platforms" (February 2020);
- Facebook needed to [redacted] (2020);
- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and

[284] *See* Exhibit 1 & Section II.A *supra*.

[285] *See* Section V.C *supra*.

- Glass Lewis "d[id not] have any reason to be assured that the Company] w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

273. In addition, multiple reports issued by governmental and non-governmental organizations in 2020, 2021, and 2022 made clear that Facebook was being used for sex and labor exploitation.[286] Zuckerberg was also on the Board in October 2019 when internal Company documents reportedly revealed that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks" and in 2021 when those internal documents were made public by a whistleblower. In 2018, 2019, and 2020, Zuckerberg testified before Congress and legislators repeatedly confronted him about evidence that human trafficking and sexual exploitation flourished on Facebook.[287] Numerous civil and criminal cases were brought in federal and state courts involving sex trafficking linked to the Company while Zuckerberg was on the Board.[288] And Zuckerberg was on the Board and served as CEO in 2018 when Congress addressed the pernicious sex trafficking in the country, including by eliminating the social media platforms' immunity under Section 230 of

[286] *See supra* Sections II.H, II.I, II.K, II.M, II.N, II.V, and II.W.

[287] *See supra* Sections II.., II.E, and II.G.

[288] *See supra* Sections II.B and II.P.

the CDA. Zuckerberg and the other Demand Board members were well aware of the thriving and systemic predation occurring throughout the Company's products and of the increased risk to Meta as a result of these crimes.

274. Nevertheless, the Board, with Zuckerberg at the helm, failed to act concerning trafficking and exploitation, and in fact affirmatively rejected stockholder proposals that would provide transparency regarding any efforts to arrest these safety concerns. Furthermore, although the Board had in place a policy concerning child exploitation, it failed to put in place a policy concerning human trafficking. Zuckerberg was also on the Board when the Company "deactivated a tool that was proactively detecting exploitation . . ."[289] Zuckerberg therefore faces a substantial likelihood of liability for breaching his fiduciary duties under *Caremark*. Furthermore, Zuckerberg is not an independent director under NYSE listing standards.

Sandberg

275. Defendant Sandberg is a director of Meta. Sandberg has served as a director since 2012 and served as COO from 2008 until August 2022.

276. As a director and COO, Sandberg had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and

[289] *See* note 190 *supra*.

Instagram platforms, but consciously disregarded those responsibilities.[290] Sandberg was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Sandberg also was on the Board in October 2019 when internal Company documents reportedly revealed that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks" and in 2021 when those internal documents were made public by a whistleblower.

277. Sandberg was also on the Board when it was told by management that:

- Congress would be pushing for Section 230 immunity because of concerns over sex trafficking on internet sites (December 2017);
- Facebook had [redacted] (2019);
- A stockholder proposal was asserting that Facebook was being sued for "facilitating sex trafficking of minors"; that "Instagram [is] being linked to 'rampant sex trafficking [and] child sexual abuse grooming'"; and that "Facebook may face significant regulatory risk if it cannot curb child sexual abuse on existing platforms" (February 2020);
- A narrative had developed that [redacted] (September 2019);

[290] *See* Sections IV.B to IV.C *supra*.

- Facebook needed to [redacted] (2020);
- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and
- Glass Lewis "d[id not] have any reason to be assured that the Company w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

278. Sandberg therefore faces a substantial likelihood of liability for breaching her fiduciary duties under *Caremark*. Furthermore, Sandberg is not an independent director under NYSE listing standards.

Alford

279. Defendant Alford is a director of Meta and has been a director since 2019.

280. As a director, Alford had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[291] Alford was on the Board when it was repeatedly advised—through the media, by proxy advisors, and

[291] *See* Sections IV.B to IV.C *supra*.

by other stockholders—about the pernicious conduct occurring on its platforms. Alford also was on the Board in October 2019 when internal Company documents reportedly revealed that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks" and in 2021 when those internal documents were made public by a whistleblower.

281. Alford was also on the Board when it was told by management that:

- A narrative had developed that [redacted] (September 2019);
- Facebook needed to [redacted] (2020);
- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and
- Glass Lewis "d[id not] have any reason to be assured that the Company w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

282. Alford has been a member of the Audit Committee since 2019. The Audit Committee also received numerous reports that Facebook was failing to control trafficking and exploitation. For example, in December 2020, the Audit Committee was told that:

- [redacted];
- [redacted];
- The machine learning process [redacted]; and
- The Company lacked [redacted] concerning child exploitative imagery.

283. Additionally, in September 2021, the Audit Committee was told that:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- There were [redacted];
- [redacted];
- [redacted] and
- [redacted]

284. Then, in February 2022, the Audit Committee was told that:

- [redacted]

- A [redacted] and
- Meta had not yet [redacted]

285. However, the members of the Audit Committee, including Alford, failed to take steps to put in place such controls.

286. Alford was also a member of the Compensation Committee in February 2021 when it was told by management that:

- A [redacted] indicated that sex trafficking lawsuits filed by survivors [redacted];
- Child advocates had demonstrated outside Facebook headquarters in October 2020; and
- [redacted]

287. Members of the Compensation Committee—including Alford—failed to act in response to these and other red flags.

288. Alford therefore faces a substantial likelihood of liability for breaching her fiduciary duties under *Caremark*.

Andreessen

289. Defendant Andreessen is a director of Meta and has been a director since 2008.

290. As a director, Andreessen had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[292] Andreessen was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Andreessen was also on the Board in October 2019 when internal Company documents reportedly revealed that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks" and in 2021 when those internal documents were made public by a whistleblower.

291. Andreessen was on the Board when it was told by management that:

- Congress would be pushing for Section 230 immunity because of concerns over sex trafficking on internet sites (December 2017);
- Facebook had [redacted] (2019);
- A stockholder proposal was asserting that Facebook was being sued for "facilitating sex trafficking of minors"; that "Instagram

[292] *See* Sections IV.B to IV.C *supra*.

[is] being linked to 'rampant sex trafficking [and] child sexual abuse grooming'"; and that "Facebook may face significant regulatory risk if it cannot curb child sexual abuse on existing platforms" (February 2020);

- A narrative had developed that [redacted] (September 2019);
- Facebook needed to [redacted] (2020);
- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and
- Glass Lewis "d[id not] have any reason to be assured that the Company w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

292. Andreessen has been a member of the Audit Committee since 2012. The Audit Committee also received numerous reports that Facebook was failing to control trafficking and exploitation. For example, in December 2020, the Audit Committee was told that:

- [redacted]
- [redacted]
- The machine learning process [redacted] and

- The Company lacked [redacted] concerning child exploitative imagery.

293. In addition, in September 2021, the Audit Committee was warned that:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- There were [redacted]
- [redacted]
- [redacted] and
- [redacted]

294. In addition, in February 2022, the Audit Committee was warned that:

- [redacted]
- A [redacted] and
- Meta had not yet [redacted]

295. However, the members of the Audit Committee, including Andreessen, failed to take steps to put in place such controls.

296. Andreessen therefore faces a substantial likelihood of liability for breaching his fiduciary duties under *Caremark*.

Houston

297. Defendant Houston is a director of Meta and has been a director since 2020.

298. As a director, Houston had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[293] Houston was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Houston was also on the Board in 2021 when a whistleblower published internal Facebook documents reportedly revealing that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks "

299. Houston was on the Board when it was warned by management that:

- Facebook needed to [redacted] (2020);

[293] *See* Sections IV.B to IV.C *supra*.

- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and
- Glass Lewis "d[id not] have any reason to be assured that the Company] w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

300. Houston therefore faces a substantial likelihood of liability breaching his fiduciary duties under *Caremark*.

Killefer

301. Defendant Killefer is a director of Meta and has been a director since 2020.

302. As a director, Killefer had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[294] Killefer was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Killefer was also on the Board in 2021 when a whistleblower published internal Facebook documents reportedly revealing that Facebook's "platform enables all

[294] *See* Sections IV.B to IV.C *supra*.

three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks . . . "

303. Killefer was on the Board when it was warned by management that:

- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and
- Glass Lewis "d[id not] have any reason to be assured that the Company w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

304. Killefer has been a member of the Audit Committee since 2020. The Audit Committee also received numerous reports that Facebook was failing to control trafficking and exploitation. For example, in December 2020, the Audit Committee was warned that:

- [redacted]
- [redacted]
- The machine learning process [redacted] and
- The Company lacked [redacted] concerning child exploitative imagery.

305. In addition, in September 2021, the Audit Committee was told that:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- There were [redacted]
- [redacted]
- [redacted] and
- [redacted]

306. Then, in February 2022, the Audit Committee was warned that:

- [redacted]
- A [redacted] and
- Meta had not yet [redacted]

307. However, the members of the Audit Committee, including Killefer, failed to take steps to put in place such controls.

308. Killefer therefore faces a substantial likelihood of liability for breaching her fiduciary duties under *Caremark*.

Kimmitt

309. Defendant Kimmitt is a director of Meta and has been a director since 2020.

310. As a director, Kimmitt had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[295] Kimmitt was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Kimmitt was also on the Board in 2021 when a whistleblower published internal Facebook documents reportedly revealing that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks . . . "

311. Kimmitt was on the Board when it was warned by management that:

- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and

[295] *See* Sections IV.B to IV.C *supra*.

- Glass Lewis "d[id not] have any reason to be assured that the Company w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

312. Kimmitt therefore faces a substantial likelihood of liability for breaching his fiduciary duties under *Caremark*.

Travis

313. Defendant Travis is a director of Meta and has been a director since 2020.

314. As a director, Travis had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[296] Travis was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Travis was also on the Board in 2021 when a whistleblower published internal Facebook documents reportedly revealing that Facebook's "platform enables all three stages of the human exploitation lifecycle (recruitment, facilitation, exploitation) via complex real-world networks . . . "

315. Travis was on the Board when it was warned by management that:

[296] *See* Sections IV.B to IV.C *supra*.

- ISS recommended that the Board "vote FOR" a stockholder proposal concerning child exploitation (May 2020);
- ISS observed that the Company had "alleged[ly] fail[ed] to catch hundreds of cases of child exploitation on its platform from January 2013 through December 2019" (May 2020); and
- Glass Lewis "d[id not] have any reason to be assured that the Company w[ould] act proactively rather than reactively, as demonstrated by numerous controversies related to the distribution of high-risk content on its platform and messaging services" (May 2020).

316. Travis has been a member of the Audit Committee since 2020. The Audit Committee also received numerous reports that Facebook was failing to control trafficking and exploitation. For example, in December 2020, the Audit Committee was told that:

- [redacted]
- [redacted]
- The machine learning process [redacted] and
- The Company lacked [redacted] concerning child exploitative imagery.

317. In addition, in September 2021, the Audit Committee was warned that:

- [redacted]
- [redacted]

- [redacted]
- [redacted]
- There were [redacted]
- [redacted]
- "The CS team does [not] monitor or have alerts to identify anomalies in enforcement volume of recidivist accounts"; and
- [redacted]

318. In addition, in February 2022, the Audit Committee was warned that:

- [redacted]
- A [redacted] and
- Meta had not yet [redacted]

319. Travis therefore faces a substantial likelihood of liability for breaching her fiduciary duties under *Caremark*.

Xu

320. Defendant Xu is a director of Meta and has been a director since January 2022.

321. As a director, Xu had fiduciary duties to monitor for compliance and violations of federal criminal law taking place on the Facebook and Instagram platforms, but consciously disregarded those responsibilities.[297] Xu was on the Board when it was repeatedly advised—through the media, by proxy advisors, and by other stockholders—about the pernicious conduct occurring on its platforms. Xu therefore faces a substantial likelihood of liability for breaching his fiduciary duties under *Caremark*.

B. At Least Half of Meta's Demand Board Lacks Independence

322. In addition to being conflicted because they face a substantial risk of liability, six of the nine Demand Board members—Zuckerberg, Sandberg, Alford, Andreessen, Houston, and Killefer—are also conflicted because they lack independence.

Zuckerberg

323. Zuckerberg is incapable of making an independent and disinterested decision to institute and prosecute this derivative litigation. Zuckerberg is Meta's controlling stockholder, CEO and Chairman of the Board.

324. In addition to being CEO and Chairman, Zuckerberg controls the Board and has exercised such control since the Company was founded. Zuckerberg bragged in two July 2019 question-and-answer meetings with employees that if he

[297] *See* Sections IV.B to IV.C *supra*.

were not his own boss, he would have been fired from Meta. As reported in a *CNBC* article, at the Meta meeting, Zuckerberg discussed his refusal to sell the Company to Yahoo in 2006, stating:

> Yahoo came in with this big offer for a billion dollars, which . . . was going to, like, fulfill everyone's financial dreams for the company. And I was like, "I don't really think we should do this." . . . In 2006, when Yahoo wanted to buy our company, I probably would've been fired, and we would have sold the company. We wouldn't even be here if I didn't have control.[298]

325. The Board demonstrates its subservience to Zuckerberg by regularly supporting his attempts to maintain his voting control, despite shareholder proposals to dilute his hold on the Company. For example, Meta has long resisted separating the positions of Chairman and CEO, preferring that Zuckerberg occupy both roles (though Google, Microsoft, Apple, and Oracle have separate CEO and chairperson roles). A majority of the Company's independent stockholders have voted in favor of shareholder proposals requesting separation of the Chairman and CEO positions at each of the Company's annual meetings from 2019 through 2022. It was only through Zuckerberg's exercise of his ten votes per share Class B stock that the shareholder proposals were defeated. Despite widespread independent stockholder

---

[298] Catherine Clifford, *Mark Zuckerberg: If I Didn't Have Complete Control Of Facebook, I Would Have Been Fired*, CNBC (Oct. 3, 2019), available at https://www.cnbc.com/2019/10/03/zuckerberg-if-i-didnt-have-control-of-facebook-i-wouldve-been-fired.html.

support, the Board has failed to act on stockholder concerns and instead chosen to continue to bend to Zuckerberg's desires.

Sandberg

326. Sandberg lacks independence as she is beholden to Zuckerberg and is therefore incapable of making an independent and disinterested decision to institute and prosecute this derivative litigation against Zuckerberg. Sandberg has been a close confidant and business partner of Zuckerberg at Meta since she joined the Company in 2008 as its COO, a role she only recently relinquished while retaining her seat on the Board. Moreover, Sandberg is one of the few individuals other than Zuckerberg who has held Class B stock entitled to ten votes per share. Sandberg converted all of her Class B shares and sold them as Class A shares through a Company repurchase program, thereby helping Zuckerberg maintain his control through his ownership of his own high-vote Class B stock.

327. Sandberg and Zuckerberg cultivated their friendship over dinners at Sandberg's home once or twice a week for six weeks before Zuckerberg decided to hire Sandberg as Meta's COO. Sandberg's late husband described the dinners as being "like dating."[299]

[299] Ken Auletta, *A Woman's Place*, THE NEW YORKER (July 4, 2011).

328. During her time as Meta's COO, Sandberg was widely considered the Company's second-in-command, behind Zuckerberg, who credited Sandberg with "handl[ing] things I don't want to."[300]

329. Zuckerberg has in turn developed a role as Sandberg's close personal confidant. After Sandberg's husband passed away in 2015, Zuckerberg took the lead in planning his funeral, and Zuckerberg and his wife, Priscilla Chan ("Chan"), "talked to [her] every day ... and [were] just there for [her] and [her] children . . . in every way possible."[301] Sandberg subsequently described Zuckerberg as "the greatest person in the world,"[302] and noted that Zuckerberg is "one of the people who really carried me."[303]

---

[300] *Id*.

[301] Seth Fiegerman, *Inside the partnership of Mark Zuckerberg and Sheryl Sandberg*, CNN (Feb. 7, 2019), available at https://www.cnn.com/2019/02/07/tech/mark-zuckerberg-sheryl-sandberg/index.html.

[302] *Sheryl Sandberg Talks Grief, Appreciating Mark Zuckerberg and Why She Won't Run for Public Office*, YAHOO! FIN. (Apr. 13, 2017), available at https://www.yahoo.com/entertainment/sheryl-sandberg-talks-grief-appreciating-mark-zuckerberg-why-153537336.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIGcaKGoWPENaBMCMypLWx-dfsMMHzi1OMtvgj8zC5C_6zuN6dH6spvy1LIBKEpy8ADP8IV8ALbUTgKOuBRmwUW2I0Wnl7HLJDUjWbx6NyxdrRn8CQZXrspU7bZ8bRMG9bugU2TXsQx9CeSmy1E7DqgOpapnwUvVftckVQT7sCdi.

[303] *Id*.

Alford

330. Alford lacks independence from Zuckerberg and is therefore incapable of making an independent and disinterested decision to institute and prosecute this derivative litigation against Zuckerberg. Alford is an executive at PayPal Holdings, Inc. Zuckerberg installed Alford as CFO and Head of Operations at Zuckerberg's personal philanthropy, the Chan Zuckerberg Initiative ("CZI"), the primary beneficiary of Zuckerberg's plans to sell or donate his Company stock. Following Alford's several year stint as Zuckerberg's trusted representative at CZI, Zuckerberg installed Alford on Meta's Board, a move widely viewed as "evidence that Zuckerberg is keen on building a firewall around him by only appointing loyalists."[304]

331. Alford also worked closely with Chan when both served as initial board members of Summit Learning Program, a nonprofit division of an online learning platform created by Meta and Summit Public Schools, a charter school network.

[304] *See* Mark Emem, *Mark Zuckerberg's Machiavellian Strategy To Crush A Facebook Board Coup*, CCN (aka "Capital & Celeb News") (Sept. 23, 2020), available at https://www.ccn.com/mark-zuckerbergs-machiavellian-strategy-to-crush-a-facebook-boardroom-coup/.

Houston

332. Houston lacks independence from Zuckerberg and is therefore incapable of making an independent and disinterested decision to institute and prosecute this derivative litigation against Zuckerberg.

333. Houston is CEO of Dropbox, a cloud company with hundreds of millions of users and companies using its services for file-syncing and sharing of documents. Houston and Zuckerberg have been close friends for years, "with the former often turning to the latter for advice."[305] Houston told an interviewer from Bloomberg that he often reaches out to Zuckerberg for business advice.[306] Zuckerberg has frequently turned up at Dropbox headquarters to visit Houston.[307] Zuckerberg went to Houston's birthday party where they celebrated and played ping-pong against each other.[308] One article on the announcement that Houston was

---

[305] *See* Avery Hartmans, *Mark Zuckerberg and Dropbox CEO Have Been "Close Friends" For Years*, Entrepreneur.com, available at https://www.entrepreneur.com/business-news/mark-zuckerberg-and-dropbox-ceo-have-been-close-friends/347526.

[306] *See* Eugene Kim, *How Mark Zuckerberg Helps His Friend, The CEO of $10 Billion Dropbox*, BUS. INSIDER (June 25, 2015), available at https://www.businessinsider.com/dropbox-ceo-drew-houston-turns-to-facebook-ceo-mark-zuckerberg-for-advice-2015-6.

[307] *See* J.J. McCorvey, *Dropbox Versus The World*, FAST CO. (March 30, 2015), available at https://www.fastcompany.com/3042436/dropbox-versus-the-world.

[308] *See Travis Kalanick and Mark Zuckerberg Blow Off Steam At Drew Houston's Ping-Pong Birthday Party*, CNBC (Mar. 9, 2017), available at https://www.cnbc.com/2017/03/09/mark-zuckerberg-travis-kalanick-drew-

joining Meta's Board specifically noted: "Houston and Zuckerberg have a long-running and well-documented friendship."[309] Houston's addition to the Board was viewed as adding "another figure to the board who is likely to be strongly supportive of Zuckerberg at a time of mounting regulatory and political scrutiny of the company."[310] Another commentator, in discussing Houston's appointment to the Board, stated: "Given the choice of acting in the interests of independent shareholders or his buddy, it's obvious whose interests will be sacrificed."[311]

Andreessen

334. Andreessen lacks independence from Zuckerberg and is therefore incapable of making an independent and disinterested decision to institute and prosecute this derivative litigation against Zuckerberg.

335. Andreessen's lack of independence from Zuckerberg is well documented. Andreessen has long supported Zuckerberg's belief that a company's founder should maintain company control. In 2009, when Andreessen and Benjamin

---

houston-ping-pong-birthday-pics.html.

[309] *See* Rob Price, *Mark Zuckerberg's Friend Dropbox CEO Drew Houston Is Joining Facebook's Board of Directors*, BUS. INSIDER (Feb. 3, 2020), available at https://www.businessinsider.com/dropbox-ceo-drew-houston-joins-facebook-board-directors-2020-2.

[310] *Id.*

[311] *See* source cited *supra* note 306.

Horowitz cofounded AH Capital Management, LLC d/b/a Andreessen Horowitz, Andreessen's goal was to "design a venture capital firm that would enable founders to run their own companies."[312] In 2006, Yahoo! offered to buy Meta for $1 billion dollars. According to Andreessen, "Every single person involved in Facebook wanted Mark to take the Yahoo! offer. The psychological pressure they put on this twenty-two-year-old was intense. Mark and I really bonded in that period, because I told him, 'Don't sell, don't sell, don't sell!'"[313]

336. Andreessen and his firm have also profited significantly through Andreessen's business ties with Zuckerberg. Meta purchased two Andreessen Horowitz portfolio companies, Instagram and Oculus VR. Andreessen Horowitz made $78 million on the sale of Instagram. Zuckerberg helped facilitate Andreessen Horowitz's investment in Oculus VR, and Andreessen subsequently joined the company's four-member board. Shortly thereafter, Zuckerberg's Meta offered to acquire Oculus VR for $2 billion. Andreessen Horowitz made $270 million on the Oculus VR transaction.[314]

---

[312] Ben Horowitz, "*Why Has Andreessen Horowitz Raised $2.7b in 3 Years*?" BEN'S BLOG, (Jan. 31, 2012), available at https://www.businessinsider.com/why-has-andreessen-horowitz-raised-27b-in-3-years-2012-6.

[313] Tad Friend, *Tomorrow's Advance Man*, THE NEW YORKER (May 18, 2015).

[314] Anita Balakrishnan, *Facebook tried to do Oculus due diligence in a weekend, Zuckerberg reveals in court*, CNBC (Jan. 17, 2017), available at https://www.cnbc.com/2017/01/17/facebook-did-oculus-due-diligence-in-a-weekend-zuckerberg-reveals-in-court.html.

337. Andreessen is also known to have used back-channel communications to Zuckerberg during Board processes to protect Zuckerberg's personal interests. Stockholder litigation challenging the Company's 2016 attempt to issue a new class of shares revealed text messages showing that Andreessen, while serving as a member of the special committee created to represent stockholders considering the share issuance, betrayed stockholders and fed Zuckerberg information regarding the special committee's progress and concerns. These covert communications helped Zuckerberg negotiate against the purportedly independent committee. Andreessen and Zuckerberg communicated privately throughout the committee's negotiation process, with Andreessen providing Zuckerberg live feedback via text explaining how to convince the committee to approve the new class of shares.

Killefer

338. Killefer lacks independence from Sandberg and is therefore incapable of making an independent and disinterested decision to institute and prosecute this derivative litigation against Sandberg. From 1997 to 2000, Killefer and Sandberg both worked at the U.S. Treasury Department. Killefer served as Treasury Assistant Secretary for Management, CFO, and Sandberg served as the Chief of Staff for Treasury Secretary Lawrence Summers. In addition, Killefer was a Senior Partner at McKinsey & Company when Sandberg was hired as a consultant in 1995. Killefer started working at McKinsey in 1979 and, except for her stint at the Treasury Department, worked there until she retired in August 2013. Sandberg remains involved with McKinsey through its partnership with her Lean In Foundation.

FIRST CLAIM FOR RELIEF
(Against All Director Defendants and Former-Director Defendants for Breach of Fiduciary Duty)

339. Plaintiffs repeat and reallege all of the preceding allegations as if fully set forth herein.

340. As Meta's directors, the Director Defendants Zuckerberg, Sandberg, Alford, Andreessen, Houston, Killefer, Kimmitt, Travis, and Xu, and the Former-Director Defendants Bowles, Chenault, Desmond-Hellmann, Hastings, Koum, Thiel, and Zients owed Meta the highest obligation of loyalty, good faith, due care, oversight and candor.

341. The fiduciary duties these directors owed to Meta included, without limitation, implementing and overseeing a system to monitor sex trafficking and other human trafficking on Meta's online interactive platforms, as well as Meta's legal compliance with all applicable laws and regulations. The Director Defendants and Former-Director Defendants had a fundamental duty to make good faith efforts to ensure that the Company's online, interactive platforms were not and are not a danger to public safety.

342. The Director Defendants and Former-Director Defendants consciously breached their fiduciary duties and violated their corporate responsibilities in at least the following ways:

a. despite being made aware of red flags that Meta's platforms—which the Company owns, manages, or operates—promote, facilitate and contribute to widespread sex trafficking and other human trafficking—they consciously and repeatedly failed to assure that the Company's reporting system was adequately designed to elevate all such reports, thus disabling them from being informed of risks or problems requiring their attention;

b. consciously disregarding their duty to investigate red flags and to remedy any misconduct uncovered; and

c. issuing false and misleading statements to Meta's shareholders regarding the Company's programs, systems, and capabilities to detect, prevent, and address the fact that Meta's online, interactive platforms promote, facilitate, and contribute to widespread sex trafficking and other human trafficking, as well as downplaying the extent of sex trafficking and other human trafficking on Meta's platforms.

343. The conduct of the Director Defendants and Former-Director Defendants, individually and collectively, as set forth herein, was due to their intentional, knowing, and/or reckless disregard for the fiduciary duties owed to the Company.

344. The Director Defendants and Former-Director Defendants consciously turned a blind eye to sex/human trafficking, child sexual exploitation, and other predatory conduct occurring on Meta's online platforms, which violated federal and state laws against sex/human trafficking and has exposed Meta to liability through FOSTA-SESTA and other laws. They further disregarded their duties to ensure that Meta was not operating online platforms that facilitated the prostitution of another person and that the Company was not acting in reckless disregard of the fact that conduct on its platform contributed to sex trafficking. The Director Defendants and Former-Director Defendants, consistent with their fiduciary duties, were required to implement and monitor policies and systems to monitor such illegal conduct.

345. The Director Defendants and Former-Director Defendants were required to fulfill their responsibilities as directors under the Audit Committee Charter, the Corporate Governance Guidelines and the Code of Conduct.

346. The Director Defendants and Former-Director Defendants had actual or constructive knowledge that they caused the Company to fail to maintain adequate internal controls and failed to provide adequate oversight to protect the Company from liability related to federal and state sex trafficking laws.

347. These actions were not good-faith exercises of prudent business judgment to protect and promote the Company's corporate interests and those of its shareholders.

348. As a direct and proximate result of the Director Defendants' and Former-Director Defendants' conscious failure to perform their fiduciary duties, Meta has sustained significant damages, both financially and to its corporate image and goodwill. Such damages to Meta include, and will include, substantial risk of liability, legal costs, increased regulatory scrutiny, reputational damages, declining users, declining revenue, declining stock price, increased cost of capital, and other costs, damages and liabilities.

349. For their conscious and bad faith misconduct alleged herein, Director Defendants and Former-Director Defendants are liable to the Company.

SECOND CLAIM FOR RELIEF
(Against the Officer Defendants for Breach of Fiduciary Duty)

350. Plaintiffs repeat and reallege all of the preceding allegations as if fully set forth herein.

351. As executive officers of Meta, the Officer Defendants Bosworth, Schroepfer, Clegg, Cox, Newstead, Sandberg, Wehner, and Zuckerberg owed Meta the highest obligation of loyalty, good faith, due care, oversight and candor.

352. The fiduciary duties owed by the Officer Defendants included the obligation to operate the Company in compliance with state and federal laws and without undue risk to public safety, the duty to implement and oversee programs to ensure compliance with criminal and civil laws and regulations governing sex trafficking and other human trafficking, and the duty to report significant risks to the Board, governmental and civil authorities, and Meta and its stockholders.

353. The Officer Defendants, individually and collectively, breached their fiduciary duties and/or acted with gross negligence in at least the following ways:

a. Acting in conscious disregard of the red flags that Meta's online platforms promote, facilitate, and contribute to widespread sex trafficking and other human trafficking and that Meta was benefiting financially from such illegal misconduct;

b. Consciously and repeatedly failing to implement, maintain, audit, and/or monitor a compliance and safety program to detect, prevent, and

address the predation on Meta's online platforms, contributing to widespread sex trafficking and other human trafficking;

c. Consciously disregarding their duties to investigate red flags and other evidence of wrongdoing and to remedy any misconduct uncovered; and

d. Consciously failing to report to the Board and/or covering up red flags that Meta's online platforms promote, facilitate and contribute to widespread sex trafficking and other human trafficking.

354. As officers of the Company, the Officer Defendants are not entitled to exculpation under 8 *Del. C.* § 102(b)(7).

355. The Officer Defendants had actual or constructive knowledge that they caused the Company to fail to maintain adequate internal controls and failed to provide adequate oversight to protect the Company from liability related to federal and state sex trafficking laws.

356. These actions were not good-faith exercises of prudent business judgment to protect and promote the Company's corporate interests and those of its shareholders.

357. As a result of the Officer Defendants' breaches of fiduciary duty—including their conscious and/or grossly negligent failure to perform their fiduciary duties—Meta has sustained significant damages both financially and to its corporate image and goodwill. Such damages to Meta caused by the Officer Defendants'

misconduct include, and will include, substantial risk of liability, legal costs, increased regulatory scrutiny, reputational damages, declining users, declining revenue, a declining stock price, increased cost of capital, and other costs, damages, and liabilities described herein.

358. As a result of the misconduct alleged herein, the Officer Defendants are liable to the Company.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request the following relief:

A. An order declaring that Plaintiffs may maintain this action on behalf of Meta and that Plaintiffs are adequate representatives of the Company;

B. An order declaring that Defendants have breached their fiduciary duties to Meta;

C. An order determining and awarding to Meta the damages sustained as a result of the violations set forth above by all Defendants, jointly and severally, together with pre-judgment and post-judgment interest thereon;

D. An order directing Meta to take all necessary actions to reform and improve its corporate governance, internal controls, and policies by implementing a Board-level reporting and information system—and to monitor that system—to ensure that the Company addresses the

rampant sex trafficking, human trafficking, and child sexual exploitation occurring on Meta's interactive computer platforms, and to ensure the Company's compliance with FOSTA-SESTA and other civil and criminal laws relating to sex trafficking, human trafficking, and child sexual exploitation (including the statutes set forth in Section I, *supra*);

E. An order against all Defendants and in favor of the Company for extraordinary equitable and injunctive relief as permitted by law and/or equity as this Court deems just and appropriate;

F. Awarding Plaintiffs' costs and disbursements for this action, including reasonable attorneys' fees and expenses; and

G. Granting such other relief as this Court deems just and appropriate.

Dated: March 10, 2023

GRANT & EISENHOFER P.A.

/s/ Christine M. Mackintosh

Michael J. Barry
Christine M. Mackintosh
Rebecca A. Musarra
Edward M. Lilly
123 Justison Street
Wilmington, DE 19801
Tel:

Barbara J. Hart
GRANT & EISENHOFER P.A.
485 Lexington Avenue
New York, NY 10017
Tel:

William S. Norton
Meredith B. Weatherby
MOTLEY RICE LLC
28 Bridgeside Blvd.
Mt. Pleasant, SC 29464
Tel:

Serena Hallowell
MOTLEY RICE LLC
777 Third Avenue, 27th Floor
New York, NY 10017
Tel:

David P. Abel
U.S. MARKET ADVISORS LAW GROUP PLLC
5335 Wisconsin Ave., Ste. 440
Washington, D.C. 20015
Tel: [redacted]

Attorneys for Plaintiff

From: Robert Healey [redacted]
Sent: Monday, March 27, 2023 2:27 AM
To: Regulations
Subject: re CPRA Cybersecurity Audit requirements

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Hi California,

Formiti Data International UK represents a number of clients with high and complex personal data processing activities.
We note the new requirement for an independent Cybersecurity audit. Can you please confirm

- Is there a Cybersecurity standard such as NIST, ISO27001 or SOC11 that you require the audit to be aligned to.
- What is the date the first audit is required to be submitted?

Kind Regards

Robert

Robert Healey
CEO Formiti Data International UK
Grosvenor House
11 St Pauls Square
Birmingham B3 1RB
United Kingdom
Phone: +44 (0) 121 582 0192
Mobile: [redacted]
Email: [redacted]
Web: www.formiti.com

From: Ridhi Shetty [redacted]
Sent: Monday, March 27, 2023 6:00 AM
To: Regulations
Cc: Matthew Scherer
Subject: CDT Comments on PR 02-2023
Attachments: CDT Comments to CPPA PR 02-2023.pdf

Dear Kevin Sabo,

The Center for Democracy & Technology respectfully submits the attached comments in response to the California Privacy Protection Agency's Invitation for Preliminary Comments on Proposed Rulemaking 02-2023, regarding cybersecurity audits, risk assessments, and automated decision-making.

Thank you,

Ridhi Shetty | Policy Counsel, Privacy & Data Project
Center for Democracy & Technology | cdt.org
E: [redacted] | **P:** [redacted] | [she/her/hers]

CENTER FOR DEMOCRACY & TECHNOLOGY

March 27, 2023

To: Kevin Sabo
California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Re: Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decision-making, PR 02-2023

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the California Privacy Protection Agency's (Agency) invitation for preliminary comments on its proposed rulemaking regarding cybersecurity audits, risk assessments, and automated decision-making.[1] CDT is a nonprofit 501(c)(3) organization dedicated to advancing privacy, consumer, and civil rights for all in the digital age. CDT's work includes a focus on automated decision-making and effective safeguards for its use.[2]

The bulk of our comments address automated decision-making. We also include a section that addresses risk assessments, incorporating previously answered questions along the way.

Automated decision-making

Question 1: Laws requiring access and/or opt-out rights for automated decision-making

At least two other laws require access or opt-out rights in the context of automated decision-making: the federal Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA). However, both require only *access*, and only in a limited and indirect way. The FCRA

[1] California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking: Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, Feb. 10, 2023, https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf.

[2] CDT has continuously engaged in the Agency's proposed rulemaking pursuant to the California Privacy RIghts Act. *See* Center for Democracy & Technology, *CDT Provides Testimony for California Privacy Protection Agency on Automated Decisionmaking, Limited Sensitive Uses of Data + More* (May 12, 2022), https://cdt.org/insights/cdt-provides-testimony-for-california-privacy-protection-agency-on-automated-decisionmaking-limited-sensitive-uses-of-data-more/; Center for Democracy & Technology, *Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, Nov. 8, 2021, https://cdt.org/wp-content/uploads/2021/11/CDT-Comments-to-Cal-Privacy-Protection-Agency-on-CPRA-Rulemaking.pdf.

allows consumers to receive a free copy of their credit report once per year from each of the three major consumer credit reporting agencies.[3] This requirement allows the consumer to review credit-related information that informs credit decisions. The ECOA gives consumers who are denied credit the right to be told the specific reasons for the adverse credit decision.[4] Because most credit decisions today involve at least some automated decision-making, the effect of these laws is that the consumers can access *some* information about the automated decision-making process or an automated decision. However, these are limited access rights, and California should go beyond them, as recommended in response to Questions 3f and 9.

Question 2: Other requirements, frameworks, and/or best practices currently in use.

At this time, there are not widely accepted industry standards or frameworks for automated decision-making. We also cannot speak to the degree to which companies actually use, implement, or adhere to their own published standards or best practices in the context of automated decision-making, because companies are not required to disclose their decision-making practices to regulators or the public. Consequently, we would urge the Agency to exercise caution to the extent industry actors hold up their own published (or unpublished) standards and practices as potential regulatory models. The Agency should also consider how companies may refer to the National Institute of Standards and Technology's AI Risk Management Framework to inform their decision-making practices.[5]

Question 3f: Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations?

We would not recommend that the Agency consider these other requirements discussed in the previous sections.

We would instead urge the Agency to look to the European Union's General Data Protection Regulation (GDPR) as a model for access and opt-out rights. Under the GDPR, individuals have the right:

- To information on "the existence of automated decision-making . . . and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[,]"[6] and

[3] 15 U.S.C. §1681j(a)(1)(A).
[4] 15 U.S.C. §1691(d).
[5] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[6] General Data Protection Regulation, Art. 15.1(h).

- "[N]ot to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[7]

The Agency should also recognize that "automated decision-making" encompasses both (1) a system's design, training data, and logic and (2) the greater contexts in which the system is embedded and uses of its outputs.[8] Therefore, when developing regulations governing access and opt-out, we urge the Agency to allow consumers to opt out of companies' use of the consumers' data to train automated decision-making systems. This would ensure that consumers have true agency with respect to how companies use their data.

Questions 4: How companies are using automated decision-making
Question 5: Consumers' experiences and concerns regarding automated decision-making technology

Today, automated decision-making systems influence decisions in multiple critical areas, including housing, credit, employment, and education. People have little to no choice in being subjected to these systems to access the opportunities about which the systems make decisions, and people may not be able to anticipate these systems' harms. Unregulated and inappropriate data use can result in biased training data for AI systems, compound historical discrimination, and yield incorrect assumptions. Unfortunately, all too often, these risks are disproportionately borne by historically marginalized groups, including people of color, immigrants, Indigenous populations, women, people with disabilities, and the LGBTQ+ community.[9]

The resulting harms can take a number of different forms, and can occur for a number of reasons:

- Companies train these systems on data sets that do not accurately represent all people on which the systems are used – or conversely, the training data may incorporate substantial data that over-represents a particular protected class.

---

[7] General Data Protection Regulation, Art. 22.1.
[8] *See Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, *supra* note 2 (citing Hannah Quay-De La Vallee and Natasha Duarte, Center for Democracy & Technology, *Algorithmic Systems In Education: Incorporating Equity and Fairness When Using Student Data* 6-8 (2019), https://cdt.org/wpcontent/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf).
[9] *See generally* Andrew Crawford, Center for Democracy & Technology, *Placing Equity at the Center of Health Care & Technology* 13 (2022), https://cdt.org/wp-content/uploads/2022/03/2022-03-22-CDT-Placing-Equity-at-the-Center-of-Health- Care-Technology-final.pdf.

- Companies may design these systems to evaluate consumer data from which protected characteristics could be inferred, which could enable or result in discrimination.
- Companies may not design these systems to ensure that all people subject to the systems can successfully navigate and use them.
- Companies may fail to establish processes for auditing the systems for inaccuracies or biases sufficiently to address and correct all harms.

Note that these factors are not always intentional. System design often executes the priorities and policies of the companies developing and using these systems, as well as societal biases regarding which people are entitled to have their fundamental needs met. In particular, people with a range of different disabilities, including chronic illnesses and mental health disabilities, face significant discrimination by algorithm-driven decision-making systems in a wide swath of areas, both because of exclusionary design and because of discriminatory targeting or profiling. Companies are neglecting disability-specific considerations when their decision-making systems rely on training data and operations parameters that under-represent disabled people, and companies can enable targeting of disabled people when training data and parameters overrepresent disabled people. Yet, the lack of transparency in how these decision-making systems work makes it difficult for people to demonstrate that a data practice has violated current federal civil rights laws.

Below, we discuss how companies are misusing data-driven systems in ways that make it difficult for people to challenge the data practice responsible for discriminatory housing, credit, employment, education, and public benefits decisions.

i. Housing and credit

To inform mortgage and other lending decisions and to screen rental applicants, "fintech" companies deploy systems that evaluate credit history, employment and income data, banking and purchase activity, rental payment history, eviction records, arrest and court records, education history, and other data.[10] These data points are supposed to predict whether applicants will fulfill the obligations that come with the housing or loan opportunities for which

[10] Jung Choi, Karan Kaul, & Laurie Goodman, *FinTech Innovation in the Home Purchase and Financing Market*, Urban Inst. 9 (2019), https://www.urban.org/sites/default/files/publication/100533/fintech_innovation_in_the_home_purchase_and_financing_market_2.pdf; Karen Hao, *The Coming War on The Hidden Algorithms That Trap People in Poverty*, MIT Tech. Rev. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back/.

they are applying. However, many fintech companies' systems have been shown to charge higher interest rates to low-income and Black borrowers, and the systems are not designed to account for the context in which this data is generated.[11]

For instance, data about past arrest records, eviction proceedings, and financial, employment, and education history may not reflect people's *current* ability to make regular rental payments or loan repayments.[12] Meanwhile, data that would more reliably indicate current ability to make regular payments, such as recent history of on-time utility payments, is not considered.[13] As a result, people can remain trapped in a cycle of poor access to credit because they are punished for past records despite changes in their circumstances or qualifications. In addition, tenant screening companies like CoreLogic use algorithms that consider data such as arrest and eviction records, which are unreliable predictors for how applicants will treat other tenants or property.[14] Higher volumes of arrest data are generated in overpoliced neighborhoods, disproportionately affecting Black, Indigenous, and Latinx communities, disabled people, and transgender people. Landlords often evict tenants after calls to police related to domestic violence – as CDT has written, this occurs even more frequently for disabled people and people of color, and contributes to unreliable eviction data.[15]

Biometric data can also contribute to housing decisions. Besides tenant screening and other functions, property technology companies also provide video surveillance and facial recognition to monitor properties for any unpermitted activity or unauthorized presence, and biometric entry systems to prevent such situations.[16] In these cases, biometric data can also trigger

---

[11] Choi et al., *supra* note 6, at 10-11.
[12] Christopher K. Odinet, *The New Data of Student Debt*, 92 Southern Cal. L. Rev 1617, 1667 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349478; Center for Democracy & Technology, Comments to Financial Regulators on Financial Institutions' Use of Artificial Intelligence, Jul. 1, 2021, https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf.
[13] *Id.* at 1663; Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage Approval Algorithms*, The Markup (Aug. 25, 2021, 6:50 AM), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.
[14] Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Center for Democracy & Technology (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/ [hereinafter Brown, *Tenant Screening Algorithms*].
[15] Am. Civ. Liberties Union, *Calling 911 Shouldn't Lead to an Eviction* (Mar. 15, 2022, 1:45 PM), https://www.aclu-wi.org/en/news/calling-911-shouldnt-lead-eviction.
[16] Avi-Asher Schapiro, *Good Business or Digital Bias? The Divisive Rise of 'Proptech',* Thomson Reuters (July 15, 2020, 5:14 PM), https://news.trust.org/item/20200715162819-bngcy; Anti-Eviction Mapping Project, Landlord Tech Watch, https://antievictionmappingproject.github.io/landlordtech/.

evictions or arrests, further criminalizing people who are already disproportionately surveilled, and for whom facial analysis has been shown to produce unreliable matches.[17] Disabled people are currently at extraordinary risk of compounded discriminatory effects of rapidly expanding surveillance technologies. For instance, studies estimate up to 85% of incarcerated youth have learning or behavioral disabilities.[18] Use of tenant screening software, employment background checks, and predictive policing tools that inappropriately and sometimes illegally use arrest or conviction records thus has an outsized impact on disabled people, creating further inequities down the line in access to housing, employment, and social services.

Housing discrimination also occurs through targeted advertising, which has been shown to direct advertisements for critical opportunities and services to, or away from, certain categories of people who would be interested in acting on the advertisements. In such cases, targeted advertising can either deny these people access to information that could help them access opportunities and services, or relegate them to receiving advertisements for more unfavorable opportunities or products.[19] For example, a Department of Justice (DOJ) lawsuit alleged that Meta's advertising system enabled advertisers to use categories created based on race, color, religion, sex, disability, familial status, and national origin, and proxies for these characteristics, to designate eligible audiences for delivery of housing advertisements.[20]

While the companies responsible for data-driven discrimination in lending and housing should be subject to liability under federal civil rights laws, the lack of transparency from companies erects barriers for people to vindicate their civil rights even against entities that are subject to civil rights laws. The Fair Housing Act (FHA) prohibits discrimination in advertisements, offers, and sale or rental of housing on the basis of race, color, religion, sex, disability, familial status, or

---

[17] *See generally* Sophia Maalsen, Peta Wolifson, Dallas Rogers, Jacqueline Nelson, and Caitlin Buckle, AHURI, *Understanding Discrimination Effects in Private Rental Housing* (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916655. *See also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings Of Machine Learning Research 2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[18] Daja E. Henry & Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students with Disabilities*, Slate (Oct. 21, 2020, 9:00 AM), https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html.

[19] *See e.g.*, Julia Angwin & Terry Parris, Jr., *Facebook Says It Will Stop Allowing Some Advertisers to Exclude Users by Race*, ProPublica (Nov. 11, 2016, 10:00 AM), https://www.propublica.org/article/facebook-to-stop-allowing-some-advertisers-to-exclude-users-by-race.

[20] Department of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

national origin.[21] The Department of Housing and Urban Development (HUD) has warned that the use of criminal arrest records can violate the FHA because it can have a disparate impact based on race and national origin.[22] HUD has also advised that evictions following domestic violence-related calls to police can indicate disability or gender discrimination,[23] which can make housing decisions relying on eviction records more likely discriminatory as well. This has not deterred the use of tenant screening algorithms that include these records, though.[24]

HUD and other agencies have initiated efforts to address the ongoing harms of tenant screening algorithms. The CFPB published reports last fall examining the prevalence of tenant screening platforms and their impacts on housing access for marginalized renters, observing that while these tools can violate fair housing and consumer protection laws, renters are unable to dispute adverse outcomes arising from these tools.[25] HUD recently announced that it will issue guidance regarding how tenant screening algorithms can violate the FHA, and will work with the FTC, CFPB, and other agencies to release best practices for using tenant screening reports.[26] And the FTC and CFPB have since issued a request for information on tenant screening issues affecting the public, including the role of algorithm-based systems on these issues.[27]

The ECOA prohibits discrimination against applicants in any aspect of a credit transaction on the basis of race, color, religion, national origin, sex, marital status, age, or income derived from a public assistance program.[28] The CFPB issued guidance in 2022 stating that the ECOA requires creditors to provide people with a specific and accurate statement of principal reasons for

---

[21] 42 U.S.C. §3604 *et seq*.
[22] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions* (2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.
[23] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Enforcement of Local Nuisance and Crime-Free Housing Ordinances Against Victims of Domestic Violence, Other Crime Victims, and Others Who Require Police or Emergency Services* (2016) https://www.hud.gov/sites/documents/FINALNUISANCEORDGDNCE.PDF.
[24] Brown, *Tenant Screening Algorithms*, *supra* note 10.
[25] *CFPB Reports Highlight Problems with Tenant Background Checks*, Nov. 15, 2022, https://www.consumerfinance.gov/about-us/newsroom/cfpb-reports-highlight-problems-with-tenant-background-checks/.
[26] The White House Blueprint for a Renters Bill of Rights (2023), https://www.whitehouse.gov/wp-content/uploads/2023/01/White-House-Blueprint-for-a-Renters-Bill-of-Rights.pdf.
[27] Federal Trade Commission, *FTC and CFPB Seek Public Comment on How Background Screening May Shut Renters Out of Housing* (Feb. 28, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-cfpb-seek-public-comment-how-background-screening-may-shut-renters-out-housing.
[28] 15 U.S.C. §1691(a).

adverse actions resulting from an algorithmic system.[29] Data practices that make or inform decisions regarding the extension of credit can violate the ECOA by using data that functions as proxies for these protected characteristics, but this does not extend to disability discrimination.

The ECOA requires creditors to inform credit applicants in writing about the reasons for an adverse credit decision or about the applicants' right to receive such a notice upon request, including for adverse actions resulting from algorithmic systems.[30] CDT has raised concerns about this form of notice to financial regulators, observing that it does not give applicants an opportunity to verify the accuracy of the data being evaluated during the approval process, or to provide additional information to supplement that data.[31] The ECOA also requires correction of inaccuracies in credit records upon request, which places responsibility on people to detect such errors, without clarity about which data contributed to the ultimate decision. Further, the ECOA offers limited recourse for targeted advertising – it protects people who actually apply for credit, extending to prospective applicants only insofar as it prohibits creditors from stating discriminatory preferences in advertising.[32]

ii. Employment

Algorithmic tools play a driving role in decisions including hiring, promotion, and termination. Vendors develop hiring technologies that aim to distinguish candidates in an applicant pool based on attributes they appear to have in common with other successful candidates and employees – in other words, attributes of people who have historically been hired more often.[33] Vendors market many of these tools as bias audited or less biased, without showing how (or even whether) the tools have been examined for disability bias.[34] Meanwhile, the tools collect and analyze data about candidates that is not relevant to candidates' ability to perform job

---

[29] Consumer Financial Protection Bureau, *Circular 2022-03: Adverse Action Notification Requirements in Connection With Credit Decisions Based on Complex Algorithms*, https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

[30] *Id.*; 15 U.S.C. §1691(d)(2).

[31] Samir Jain & Ridhi Shetty, *Taking a Hard Line on AI Bias in Consumer Finance*, Center for Democracy & Technology, https://cdt.org/insights/taking-a-hard-line-on-ai-bias-in-consumer-finance/.

[32] 12 C.F.R. Supplement I to Part 1002, Paragraph 4(b).

[33] Miranda Bogen & Aaron Rieke, Upturn, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[34] *See* Manish Raghavan, Solon Barocas, Jon Kleinberg, & Karen Levy, *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 469 (2020), https://arxiv.org/pdf/1906.09208.pdf.

functions, causing workers to be rejected over irrelevant data related to marginalized identities.[35]

One such algorithm-driven hiring tool is resume screening. Ideal's resume screening software analyzes language and details in resumes, from candidates' names to affiliations to employment gaps, to identify whether the resumes reflect qualities the tools are designed to look for.[36] Taleo assigns bonus points for keywords in resumes that reflect attributes that are desired but not required.[37] As Amazon's now-discontinued resume screening tool demonstrated, resume screening tools can observe patterns in resumes that are moved forward in the hiring process and learn to filter out resumes with terms associated with women, such as women-oriented affiliation groups.[38] Such tools could similarly learn to exclude candidates based on data related to racial or ethnic identity.[39] Additionally, marginalized people who have previously experienced discrimination in their education, employment, or access to healthcare (especially if they face multiple forms of discrimination) might not get past screening tools that downgrade or screen out resumes before human reviewers can consider them. For instance, a disabled person may previously have had difficulty getting full-time employment, thus leading to gaps in their resume that will be flagged by such systems.[40]

Research by CDT and fellow advocates has raised concerns about other tools that purport to measure "soft skills" through gamified personality and aptitude assessments, or through

---

[35] *See* Hilke Schellmann, *Finding it Hard to Get a New Job? Robot Recruiters Might Be to Blame*, The Guardian (May 11, 2022, 4:30 PM), https://www.theguardian.com/us-news/2022/may/11/artitifical-intelligence-job-applications-screen-robot-recruiters (discussing how automated hiring technologies exhibit gender biases and use criteria such as names and data about non-professional activities).

[36] Ideal, *Screening*, https://ideal.com/product/screening/. *See also* Avi-Asher Schapiro, *AI is Taking Over Job Hiring, But Can it Be Racist?*, Thomson Reuters (Jun. 7, 2021, 7:04 AM), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC.

[37] James Hu, *Taleo: 4 Ways the Most Popular ATS Ranks Your Job Application*, Jobscan (Mar. 8, 2018), https://www.jobscan.co/blog/taleo-popular-ats-ranks-job-applications/.

[38] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women,* Thomson Reuters (Oct. 10, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[39] Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated Against Women*, American Civil Liberties Union (Oct. 12, 2018), https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.

[40] Jim Fruchterman & Joan Mellea, Benetech, *Expanding Employment Success for People With Disabilities* (2018), https://benetech.org/about/resources/expanding-employment-success-for-people-with-disabilities-2/.

analysis of video interviews.[41] The use of such tools presumes that everyone demonstrates the traits employers look for – such as empathy, optimism, or adaptability – the same way. Paradox Traitify provides candidates with a series of images, requiring them to indicate whether they identify with what is depicted in each image to determine their alignment with a pseudoscientific personality model.[42] Pymetrics analyzes data collected while candidates complete a set of games to predict "cognitive and emotional attributes," which it claims to be "fairness-optimized" but has not been examined for disability bias.[43] Pymetrics was recently acquired by Harver, which implements "behavioral-based AI methodology" in soft skills assessments and automates matching of "high-potential" candidates.[44] Cappfinity's Koru uses a survey that requires candidates to select the responses with which they feel they align most, to assess soft skills.[45] Blind people and people with mobility impairments might not be able to adequately interface with a gamified assessment, while people with mental health disabilities or cognitive disabilities might have difficulty processing the information quickly enough to score well. Similarly, autistic and other neurodivergent people may be unable to answer correctly on personality tests that score candidates on characteristics unrelated to core competencies or essential functions of the job at hand.

HireVue has used video interview assessments that process data about how candidates physically appear, move, emote, and sound as they respond to interview questions. This treats candidates' eye contact, facial expressions, fidgeting, tics, vocabulary, and speech patterns as data points to infer personality traits such as confidence and trustworthiness.[46] HireVue has stated that it does not use video analysis or audio characteristics, but it analyzes personality

---

[41] Center for Democracy & Technology, *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?* 11-12 (2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf; Aaron Rieke, Urmila Janardan, Mingwei Hsu, and Natasha Duarte, Upturn, *Essential Work* (2021), https://www.upturn.org/work/essential-work/.
[42] Paradox, *Assessments*, https://www.paradox.ai/products/assessments; Olivia Goldhill, *We Took the World's Most Scientific Personality Test – and Discovered Unexpectedly Sexist Results* (Feb. 11, 2018), https://qz.com/1201773/we-took-the-worlds-most-scientific-personality-test-and-discovered-unexpectedly-sexist-results/.
[43] Pymetrics, *Assessments*, https://www.pymetrics.ai/assessments; Christo Wilson, Avijit Ghosh, Shan Jiang, Alan Mislove, Lewis Baker, Janelle Szary, Kelly Trindel, and Frida Polli, *Building and Auditing Fair Algorithms: a Case Study in Candidate Screening* (2021), https://evijit.github.io/docs/pymetrics_audit_FAccT.pdf.
[44] Harver, *Harver Acquires Pymetrics, Further Enhancing Talent Decision Capabilities Across the Employee Lifecycle* (Aug. 11, 2022), https://harver.com/press/harver-acquires-pymetrics/; Harver, *Assessments*, https://harver.com/software/assessments/; Harver, *Hiring Process Optimization*, https://harver.com/software/hiring-process-optimization/.
[45] Cappfinity, *Skills Identification*, https://www.cappfinity.com/cappfinity-product-page/assessment-cognitive-3/.
[46] Drew Harwell, *A Face-Scanning Algorithm Increasing Decides Whether You Deserve the Job*, Wash. Post (Nov. 6, 2019, 12:21 PM), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

traits and aptitudes by applying natural language processing to a transcription developed through an AI-driven speech-to-text service.[47] Disabled candidates who possess the traits that are necessary for successful job performance can nonetheless be scored unfairly by this type of tool, because their disabilities can cause them to demonstrate examined traits in ways that cannot be accurately captured through the analyzed data points.[48] This type of tool could also produce unfair scores for candidates of color or candidates who have been socialized to follow certain gender norms, as cultural norms can also affect speech patterns and eye contact.[49] HireVue also claims its product has been audited for fairness, but does not make its audit report available unless one provides their name, email address, and professional affiliation and agrees not to use any part of the audit report without HireVue's written authorization.[50] HireVue is now facing a class action lawsuit over its collection and use of biometric data.[51]

Companies are also increasingly developing and deploying sophisticated electronic surveillance to automate the monitoring and management of workers, whether they are in a warehouse, out making deliveries, at an office, or working remotely from home. CDT's report, *Warning: Bossware May Be Hazardous to Your Health*, examines companies' use of such automated systems, commonly referred to as "bossware," to perform a wide variety of monitoring tasks, such as tracking workers' location and movements, productivity and downtime, computer use, facial expressions, biometric markers, and frequency and length of bathroom and other breaks.[52] One system, Crossover's WorkSmart productivity tool, takes periodic screenshots and images of workstations to monitor what workers are doing.[53] Another company, Time Doctor,

---

[47] HireVue, *Explainability Statement* (2022), https://webapi.hirevue.com/wp-content/uploads/2022/03/HV_AI_Short-Form_Explainability_3152022.pdf.
[48] Matthew Scherer, *HireVue "AI Explainability Statement" Mostly Fails to Explain what it Does*, Center for Democracy & Technology (Sept. 8, 2022), https://cdt.org/insights/hirevue-ai-explainability-statement-mostly-fails-to-explain-what-it-does/.
[49] Goodman, *supra* note 35.
[50] HireVue, *Download IO Psychology Audit Description by Landers Workforce Science LLC*, https://www.hirevue.com/resources/template/hirevue-io-psychology-audit-report.
[51] Samantha Hawkins, *HireVue Attempts to Escape Biometrics Suit Over AI Interviews*, Bloomberg (June 22, 2022, 1:16 PM), https://news.bloomberglaw.com/privacy-and-data-security/hirevue-attempts-to-escape-biometrics-suit-over-ai-interviews.
[52] Jodi Kantor, Arya Sundaram, Aliza Aufrichtig, & Rumsey Taylor, *Workplace Productivity: Are You Being Tracked?*, N.Y. Times (Aug. 16, 2022, 10:03 AM), https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html; Spencer Soper, *Fired by Bot at Amazon: 'It's You Against the Machine'*, Bloomberg (June 28, 2021, 6:00 AM), https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out.
[53] Sean Captain, *In 20 Years, Your Boss May Track Your Every Glance, Keystroke, and HeartBeat*, Fast Company (Jan. 27, 2020), https://www.fastcompany.com/90450122/in-20-years-your-boss-may-track-your-every-glance-keystroke-and-heartbeat.

prevents workers from deleting screenshots to protect their privacy by deducting time worked during the period when screenshots were taken.[54] Some programs use workers' phones or computers to listen, watch, or monitor other sensors in their device, and can penalize workers for moving away from their workstation or slowing productivity.

Companies often use these technologies to optimize tasks for their own profit, but they put workers' health and safety at risk and threaten their privacy, autonomy, and dignity.[55] For example, Amazon has used productivity monitoring to monitor "time off task," which triggers warnings to workers for resting even when needed, putting them at risk of termination if they do not work at a pace that is dangerously fast.[56] Productivity monitoring also fails to capture work that is being performed offline or that cannot be accurately quantified through surveillance measures, and can punish and deter worker organizing.[57]

Many low-wage and hourly workers endure constant surveillance, often combined with algorithmic management systems that can discipline or even terminate them.[58] This exacerbates the already-wide gaps in information and bargaining power that low-wage workers face. Algorithmic tools further diminish gig workers' bargaining power, as they determine compensation and availability and termination of jobs.[59]

Low-wage workers marginalized on the basis of disability, race, ethnicity, and gender identity are at an even greater disadvantage. As many as 100,000 disabled workers are paid subminimum wages due to a provision in the Fair Labor Standards Act that allows employers to pay disabled workers commensurate with wages paid to non-disabled workers for "the same type, quality, and quantity of work" – effectively limiting disabled workers' wages based on their

---

[54] Matt Scherer, Center for Democracy & Technology, *Warning: Bossware May Be Hazardous to Your Health* 9 (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/ [hereinafter *Bossware*].
[55] *Id.* at 36.
[56] Deborah Berkowitz, *Packaging Pain: Workplace Injuries in Amazon's Empire*, Nat'l Emp. Law Project, https://www.nelp.org/publication/packaging-pain-workplace-injuries-amazons-empire/; Colin Lecher, *How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'*, The Verge (Apr. 25, 2019, 12:06 PM), https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.
[57] Kantor et al., *supra* note 48.
[58] Aiha Nguyen, *The Constant Boss: Labor Under Digital Surveillance*, Data & Society (2021), https://datasociety.net/library/the-constant-boss/.
[59] Federal Trade Commission, Policy Statement on Enforcement Related to Gig Work (Sept. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Matter%20No.%20P227600%20Gig%20Policy%20Statement.pdf.

challenges in meeting productivity expectations.[60] In other words, this provision allows an employer to pay a disabled worker only for the hours a non-disabled worker would take to complete the same work rather than the hours of labor the disabled worker has actually put in. Productivity monitoring systems can discriminate against disabled workers, pregnant or breastfeeding workers, older workers, and workers requiring religious prayer breaks by flagging breaks or slower pace of work, increasing the risk of injury to physical or mental health.[61] These effects are especially worse for people with physical, mental health, developmental, or cognitive disabilities.

Relatedly, more employers are relying on workplace wellness programs to increase worker productivity while reducing the cost of benefits claims for employers, even turning to gamified approaches to influence employees' behavior and personal health decisions.[62] Studies have shown that these programs do not deliver the intended positive effects on healthcare expenses or productivity.[63] Meanwhile, the programs impose expectations for physical exercise and diet that disabled workers may not be able to meet, and reinforce the higher societal value assigned to being "healthy."[64] To make matters worse, these programs pressure employees to provide health data that might make its way to third parties.[65]

While the discriminatory outcomes of hiring and algorithmic management technologies run afoul of federal employment discrimination laws, enforcement has not kept up with these technologies. For instance, Title I of the ADA prohibits adverse employment decisions based on

[60] Rebecca Vallas, Kim Knackstedt, Hayley Brown, Julie Cai, Shawn Fremstad, & Andrew Stettner, The Century Fdn. and Disability Econ. Just. Collaborative, *Economic Justice is Disability Justice* (2022), https://tcf.org/content/report/economic-justice-disability-justice/. Section 14(c) of the Fair Labor Standards Act allows employers to apply for special certificates to employ disabled workers at subminimum wages. 29 U.S.C. §214(c).

[61] *The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before House Comm. on Ed. & Labor, Civil & Human Serv. Subcomm.* (2020) (testimony of Jenny Yang, Senior Fellow, Urban Institute), https://edlabor.house.gov/imo/media/doc/YangTestimony02052020.pdf.

[62] *See* Joseph Sanford & Kevin Sexton, *Opinion: Improve Employee Health Using Behavioral Economics*, CFO (Feb. 3, 2022), https://www.cfo.com/human-capital/health-benefits/2022/02/employee-health-wellness-medical-claims-behavorial-economics/.

[63] Sally Wadyka, *Are Workplace Wellness Programs a Privacy Problem?*, Consumer Reports (Jan. 16, 2020), https://www.consumerreports.org/health-privacy/are-workplace-wellness-programs-a-privacy-problem-a2586134220/.

[64] *See* Lydia X. Z. Brown, Ridhi Shetty, Matthew U. Scherer, & Andrew Crawford, Center for Democracy & Technology, *Ableism And Disability Discrimination in New Surveillance Technologies* 54-55 (2022), https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/; Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 129-30, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211.

[65] *Id.*

workers' disability, and it requires employers to provide reasonable accommodations when doing so would not pose an undue hardship on employers.[66] Hiring and algorithmic management technologies provided by private companies can make or influence adverse decisions using disability-related data, without informing workers about how the technologies are collecting and analyzing their data, how this will influence employment decisions, and how workers might access accommodations that enable fairer evaluation.[67] Thus, workers may not have enough detail to pursue disability discrimination claims arising from these technologies' use. Similar issues plague enforcement of Title VII of the Civil Rights Act. The Equal Employment Opportunity Commission's draft Strategic Enforcement Plan for Fiscal Years 2023-2027 recognizes these issues, and the agency plans to dedicate resources to addressing employment discrimination related to the use of algorithm-driven hiring technologies.[68]

Beyond civil rights protections, there are few other laws or rules governing employers' use of surveillance technologies or safeguarding workers from their harmful effects. Workers have no concrete privacy rights under either federal law or the laws of most states. The Occupational Safety and Health Act prohibits practices that pose a risk of death or serious injury to workers, but the Occupational Safety and Health Administration's regulations do not cover many of the harms to workers' health that these technologies can impose, such as repetitive motion injuries and threats to workers' mental health. Gig workers are also not adequately protected under existing civil rights laws and the Occupational Health and Safety Act, which do not classify all workers as covered "employees."[69]

In addition, a new fact sheet from the Department of Labor regarding reporting requirements under the Labor-Management Reporting and Disclosure Act states that employers must report expenditures made for surveillance of employees and unfair labor practices, but only when the surveillance is used to obtain information connected to a labor dispute or the labor practices are intended to undermine the right to organize.[70]

---

[66] 42 U.S.C. §12112.
[67] *Algorithm-Driven Hiring Tools*, *supra* note 37.
[68] Center for Democracy & Technology, *CDT Comments Supporting EEOC's Recognition of Discriminatory Tech as an Enforcement Priority*, Feb. 9, 2023, https://cdt.org/insights/cdt-comments-supporting-eeocs-recognition-of-discriminatory-tech-as-an-enforcement-priority/.
[69] Scherer, *Bossware*, *supra* note 50, at 16.
[70] Jeffrey Freund, *How We're Ramping Up Enforcement of Surveillance Reporting*, Department of Labor Blog (Sept. 15, 2022), https://blog.dol.gov/2022/09/15/how-were-ramping-up-our-enforcement-of-surveillance-reporting; Office of Labor-Management Standards, U.S. Department of Labor, *OLMS Fact Sheet on Form LM-10 Employer Reporting: Transparency Concerning Persuader, Surveillance, and Unfair Labor Practices Expenditures*, https://www.dol.gov/sites/dolgov/files/OLMS/regs/compliance/LM10_FactSheet.pdf.

iii. Education

Public sector services, from education to governmental benefits, regularly involve the collection of personal data. Students and families may be subjected to data practices that worsen inequity throughout the education context, from the use of cameras equipped with computer vision on campus, to algorithms that make critical decisions about students' lives, to software that monitors everything students do online — often through technology sold by private contractors. Those uses of data and technology surveil students often without meaningful consent or opportunity to opt out because they are a condition for students' ability to access a fundamental service — their education.

CDT has researched student activity monitoring software, a type of school surveillance technology that allows schools to view students' screens, record their browsing and search histories, and scan their messages and documents stored online or on school devices.[71] The results showed that surveillance is pervasive: 89 percent of teachers report that their school uses student activity monitoring software,[72] and monitoring often occurs even outside of school hours. Although vendors claim that student activity monitoring and other forms of commercial surveillance benefit students, those claims are largely unsubstantiated.[73]
Instead, monitoring violates rights traditionally protected by civil rights laws.[74] Further, students experiencing poverty and students of color rely more heavily on school-issued devices, which are more likely to be subject to monitoring than personal devices.[75] As a result, these groups of

[71] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: The Misleading Promise of Monitoring Students Online* (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of- monitoring-students-online [hereinafter *Hidden Harms*].
[72] *Id.* at 8.
[73] Center for Democracy & Technology & Brennan Center for Justice, Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns (2019), https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns; *see also* Rebecca Heilweil, *The Problem with Schools Turning to Surveillance After Mass Shootings*, Vox (June 2, 2022, 7:30 AM), https://www.vox.com/recode/23150863/school-surveillance-mass-shooting- texas-uvalde; Lucas Ropek, *Surveillance Tech Didn't Stop the Uvalde Massacre*, Gizmodo (May 27, 2022), https://gizmodo.com/surveillance-tech-uvalde-robb-elementary-school-shootin-1848977283; Jolie McCollough & Kate McGee, *Texas Already "Hardened" Schools. It Didn't Save Uvalde.*, Texas Tribune (May 26, 2022), https://www.texastribune.org/2022/05/26/texas-uvalde-shooting-harden-schools;
[74] *Hidden Harms*, *supra* note 67, at 19-24.
[75] DeVan L. Hankerson Madrigal, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, & Dhanaraj Thakur, Center for Democracy & Technology, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software* 10 (Sept. 21, 2021), https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/; Hugh Grant-Chapman & Elizabeth Laird, Center for Democracy & Technology, *Research Slides: Key Views Toward Ed Tech, School Data, and Student Privacy* 48 (Nov. 15, 2021), https://cdt.org/insights/report-navigating-the-new-normal-ensuring-equitable-and-trustworthy-edtech-for-the-future.

students are similarly subject to increased risks of discrimination. These incursions on students' fundamental rights are a betrayal of schools' role as "the nurseries of democracy."[76]

National reporting has also underscored the harms caused by commercial surveillance in education. Students with disabilities are at higher risk of generating false positives and false negatives when surveilled by student monitoring tools that are designed to identify atypical sounds, text, speech, or movements as potential indicators that students may be engaging in violent or prohibited conduct, making threats, or cheating on tests. For instance, a ProPublica investigation found that aggression-detection microphones were so unreliable that they flagged loud laughter and locker doors slamming as indicators of violence.[77] Those false positives raise concerns for students whose disabilities affect their speech and movement, such as students with cerebral palsy who might not be able to modulate voice volume or students with Tourette's who have loud vocal tics.

Meanwhile, student advocacy organizations such as the National Disabled Law Students Association have documented the discriminatory barriers that students with a wide range of disabilities, including ADD, blindness, and Crohn's disease, experience when required to use automated proctoring software.[78] Students reported not being permitted to take enough bathroom breaks, worrying about false positives from needing to move or pace, or not moving their eyes or hands the right way. For disabled students of color or LGBTQ+ students with disabilities, who also face additional discrimination and prejudice, the risks of student monitoring and commercial surveillance programs are further compounded.

Although existing laws address many of the impacts of the uses of data and technology on civil rights, they do not cover all harms to historically marginalized groups of people who are not recognized as a legally protected class, such as unhoused students, low-income students, foster care students, and rural students. Title VI[79] and Title IX[80] of the Civil Rights Act prohibit discrimination on the basis of race, sex, and related classes by entities receiving certain federal funds, including in the education sector. However, when discrimination is caused by technology

[76] Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2046 (2021).
[77] Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.
[78] National Disabled Law Students Association, *Report on Concerns Regarding Online Administration of Bar Exams* (2020), https://ndlsa.org/wp-content/uploads/2020/08/NDLSA_Online-Exam-Concerns-Report1.pdf.
[79] 42 U.S. Code § 2000d.
[80] 20 U.S.C. §§ 1681–1688.

distributed by private contractors for schools, students and families may not be aware of the discriminatory impact, due to a lack of transparency around the implementation and utilization of technological systems. Schools have very little ability to gain insight into contractors' data practices, no matter how reasonable their precautions, and this prevents them from providing parents with adequate notice. Schools, families, and students are consequently dependent on contractors' representations regarding data use, and need transparency regarding contractors' collection and use of student data.

Students and families do not have a meaningful choice in whether to consent to the surveillance. Students are often required or encouraged to use school-issued devices that are subject to monitoring,[81] or they may rely on school-issued devices because of their families' socioeconomic status.[82] Further, students and families are often not provided accurate, complete disclosures around commercial surveillance in education. For example, in recent CDT research, 47 percent of parents reported they were not informed about how their schools' contractors collect data about students' activity online; only 39% reported they were asked for input on those practices.[83] Even if students and families are provided adequate disclosures, they are typically not given a choice (whether opt-in or opt-out) with respect to whether and how schools or their contractors monitor student online activity. Moreover, it may be impractical or even impossible for students and families to switch schools to avoid their commercial surveillance practices.

For example, an algorithmic system used to assign students to schools may rely on a variety of factors, not all of which may be known to students and families.[84] This information asymmetry may make it difficult or impossible to challenge discriminatory practices caused by data or technology use. In interviews, school IT leaders stated they took strides through contractual measures to hold contractors accountable for their uses of student data, and expressed frustration with "what they describe as a lack of distinguishable options for privacy-forward

[81] Hankerson Madrigal et al., *supra* note 71, at 10.
[82] *Id.*
[83] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: Research Slide Deck* 30–32 (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online.
[84] Hannah Quay-de la Vallee & Natasha Duarte, Center for Democracy & Technology, *Algorithmic Systems in Education* 8-9 (2019), https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/.

devices."[85] Similarly, 94 percent of parents and 88 percent of students stated it was "important" for schools to engage them on the uses of student data.[86]

Title VI[87] and Title IX[88] prohibit entities receiving certain federal funds from acquiring discriminatory technology, but would not preclude private vendors from selling it in the first place. Further, certain uses of data and technology may not intentionally discriminate against people based on race, sex, disability status, or other protected classes, but nonetheless cause disparate impact. Courts, however, have curtailed people's ability to challenge disparate impact under critical civil rights laws in court,[89] limiting their ability to seek redress. CDT has called on the Office for Civil Rights in the U.S. Department of Education to address harms from some uses of data and technology on students of color, students with disabilities, and LGBTQ+ students.[90]

Lax data security practices by private contractors in the education sector also cause harm by undermining students' and families' trust in schools and contractors, and putting their financial and physical wellbeing at risk. Lax data security practices can result in breaches and other data security incidents, which have substantially increased in both number and scope since 2016 and strained schools' resources.[91] For example, one recent incident involved a contractor serving schools in six states, affecting over three million current and former students.[92] Similarly, a

---

[85] Hankerson Madrigal et al., *supra* note 71, at 17.
[86] *Hidden Harms*, *supra* note 67, at 18.
[87] 42 U.S. Code § 2000d.
[88] 20 U.S.C. §§ 1681–1688.
[89] *E.g.*, Jackson v. Birmingham Bd. of Educ., 544 U.S. 167, 178, 178 n.2 (2005) (Title IX); Alexander v. Sandoval, 532 U.S. 275 (2001) (Title VI); Doe v. BlueCross BlueShield of Tenn., Inc., 926 F.3d 235, 240-42 (6th Cir. 2019).
[90] Center for Democracy & Technology, *Comment on Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance*, Docket No. ED-2021-OCR-0166 (filed Sept. 12, 2022), https://cdt.org/insights/cdt-urges-us-department-of-education-to-protect-lgbtqi-students-from-discrimination-in-proposed-title-ix-rules; Letter to Catherine Lhamon, Assistant Secretary for Civil Rights, U.S. Department of Education, from Coalition of Civil, Digital, and Education Rights Organizations (filed Aug. 2, 2022), https://cdt.org/insights/letter-to-ed-office-for-civil-rights-on-discriminatory-effects-of-online-monitoring-of-students/; Center for Democracy & Technology, *Comments on Request for Information Regarding the Nondiscriminatory Administration of School Discipline*, Docket No. ED-2021-OCR-0068 (filed July 23, 2022), https://cdt.org/insights/cdt-comments-to-us-dept-of-ed-urging-the-protection-of-students-of-color-and-students-with-disabilities-and-their-data; Center for Democracy & Technology, *Comments on Announcement of Public Hearing; Title IX of the Education Amendments of 1972*, 86 Fed. Reg. 27429 (filed June 11, 2021), https://cdt.org/insights/cdt-comments-on-protecting-privacy-rights-and-ensuring-equitable-algorithmic-systems-for-transgender-and-gender-non-conforming-students/.
[91] K12 SIX, State of K-12 Cybersecurity 3 (2022), https://www.k12six.org/the-report.
[92] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire/.

recent ransomware attack on Los Angeles Unified School District resulted in the release of students' personal information, and parents and students have questioned the district's preparation and transparency.[93] A ransomware attack on a Texas school district cost more than a half million dollars to mitigate, and attacks in Baltimore and Buffalo cost in excess of $9 million each.[94]

As the Government Accountability Office has described, student data "can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood."[95] One breach included the personal information of students who completed surveys on bullying, and another included students' phone numbers, which "were used to send text messages that threatened physical violence."[96] In light of these harms, "COPPA-covered companies, including ed tech providers, must have procedures to maintain the confidentiality, security, and integrity of children's personal information. For example, even absent a breach, COPPA-covered ed tech providers violate COPPA if they lack reasonable security."[97]

Policymakers should note that public sector services are provided in part or entirely by private contractors or vendors, so new regulations should protect the privacy-forward provision of governmental services by such contractors.[98] Governments regularly contract out services to private companies, and many of those services involve data collection and use. Schools and school districts may contract with private contractors to provide systems for online lessons, communications services, or managing students' personal information. Other governmental

---

[93] Howard Blume & Alejandra Reyes-Velarde, *Student Information Remains at Risk After Massive Cyberattack on Los Angeles Unified*, Los Angeles Times (Sept. 7, 2022), https://www.latimes.com/california/story/2022-09-07/los-angeles-unified- schools-cyberattack; Joshua Bay, *LA Parents Sound Off After Cyberattack Leaves Students Vulnerable*, The 74 (Oct. 7, 2022), *https://www.the74million.org/article/la-parents-sound-off-after-cyberattack-leaves-students-vulnerable*.

[94] K12 SIX, *supra* note 176, at 8; *see also* McKenna Oxenden, *Baltimore County Schools Suffered a Ransomware Attack. Here's What You Need to Know*, Baltimore Sun (Nov. 30, 2020, 8:33 PM), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-co-what-to-know-schools-ransomware-attack-20201130-2j3ws6yffzcrrkfzzf3m43zxma-story.html.

[95] Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 13 (2021), https://www.gao.gov/products/gao-20-644.

[96] *Id.*

[97] Federal Trade Commission, Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act 3 (2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online.

[98] *See Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, *supra* note 2, at 12-14 (explaining the importance of scoping rules to protect student privacy without creating unintended consequences for service provision).

entities may contract with private entities for a variety of services such as identity verification. A broadly applicable data-related rule may not apply as easily to entities providing government services and may even interfere with those services.[99]

iv. ID verification for government services

Both recipients of government services and victims of identity theft face risks from the use of private vendors by state and federal agencies providing benefits and services.[100] However, regulation of private vendors assisting with government service delivery presents a further challenge: just as with private providers of educational services, improperly considered rules may hamper the ability of government agencies to effectively deliver essential services. On the other hand, rules are clearly needed: the use and collection of citizen data by private companies poses risks to privacy that could result in material harm, such as identity theft; and government outsourcing of key benefits determinations to private companies can result in preventing some individuals from getting essential benefits.

The starting point for delivery of governmental services is identity verification, where the government agency checks that an applicant is who they say they are. As public agencies seek to modernize identity verification through data and technology use, they are increasingly considering incorporating assistance from private companies. Examples of vendor assistance include: attribute validation, where the vendor confirms that the information provided by an applicant matches that in other identity databases (such as driver's license data, health records, or financial records); and biometric verification, where the vendor confirms through the use of physical or biological information that the applicant matches any submitted identity documents (1:1 matching) or other biometric information in the vendor's database (1:many matching).[101] Most recently, the use of facial recognition as a kind of biometric verification has garnered widespread scrutiny.[102]

---

[99] For an analysis of how rules affecting private companies should be scoped to avoid unintended consequences for government service providers, *see* Center for Democracy & Technology, *Comments on FTC's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*, at 48-51, https://cdt.org/wp-content/uploads/2022/11/CDT-Comments-to-FTC-on-ANPR-R111004.pdf.

[100] Here, we focus on practices that involve passing data to private technology vendors and exclude services that are provided solely by governmental entities or primarily involve in-person verification.

[101] *See* Michael Yang, Center for Democracy & Technology, *Digital Identity Verification: Best Practices for Public Agencies* (2022), https://cdt.org/insights/digital-identity-verification-best-practices-for-public-agencies/.

[102] Brian Naylor, *IRS Has Second Thoughts About Selfie Requirement*, NPR (Feb. 7, 2022, 3:29 PM), https://www.npr.org/2022/02/07/1078024597/want-information-from-the-irs-for-some-the-agency-wants-a-selfie.

The two main risks in the provision and use of such identification verification services are data breaches and biased algorithms.[103] First, when sensitive information is processed by a third party for purposes of identity verification, this data sharing increases the potential for data breaches. For example, ID.me, a facial recognition identity verification company, allowed employees to bring home devices that carried U.S. citizens' identity data and retained biometric data longer than necessary.[104] Such practices increase the chances of data being leaked onto the internet and later used for identity theft. Similar risks came to fruition when Equifax, a credit agency that also provides attribute validation for identity verification, exposed personal information of 147 million people in a 2017 data leak, allowing both domestic and foreign criminals to defraud state governments of pandemic unemployment assistance by using false or stolen identities.[105] Victims of identity theft face significant obstacles in re-asserting their identity and regaining access to government services.

Second, biometric analysis for identity verification may be less accurate for individuals from some racial backgrounds.[106] That bias harms members of those groups because they face increased barriers in accessing government services that require biometrics as part of identity verification. For this reason, the General Services Administration (GSA) committed in January 2022 not to use facial recognition, from private companies or otherwise, for identity verification in government service delivery until facial recognition is sufficiently free of biases.[107] However, the GSA's new rule is limited to the products that it deploys (namely, Login.gov, the single sign-on authentication solution it provides to other federal, state, and local agencies), and does

---

[103] Hannah Quay-de la Vallee, *Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives*, Center for Democracy & Technology (Jun. 7, 2022), https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/.

[104] Caroline Haskins, *Inside ID.me's Torrid Pandemic Growth Spurt, Which Led to Frantic Hiring, Ill-Equipped Staff, and Data-Security Lapses as Tte Company Closed Lucrative Deals With Unemployment Agencies and the IRS*, Bus. Insider (Jun. 7, 2022, 5:00 AM), https://www.businessinsider.com/id-me-customer-service-workers-hiring-secuirty-privacy-stress-data-2022-6. Jessy Edwards, *ID.me Lawsuit Claims Company Violates Data Storage Requirements*, Top Class Actions (Aug. 22, 2022), https://topclassactions.com/lawsuit-settlements/privacy/bipa/id-me-lawsuit-claims-company-violates-data-storage-requirements/.

[105] Cezary Podkul, *How Unemployment Insurance Fraud Exploded During the Pandemic*, ProPublica (July 26, 2021, 5:00 AM), https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

[106] Nicol Turner Lee, *Mitigating Bias and Equity in Use of Facial Recognition Technology by the U.S. Customs and Border Protection*, Brookings Institution (July 27, 2022), https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/.

[107] *Executive Order 13985 – Equity Action Plan*, General Services Administration (Jan. 20, 2022), https://www.gsa.gov/cdnstatic/GSAEquityPlan_EO13985_2022.pdf.

not address bias in other forms of biometrics, like voice recognition.[108] Other government agencies at every level may still use biometrics from private vendors, regardless of levels of bias, for identity verification. Thus, other agencies should consider the appropriate level of accuracy and fairness for biometrics to be used safely, and establish that as the standard all private vendors must meet when providing biometric verification to government services on the ground.

v. Eligibility determination and allocation of benefits

Government agencies also use private vendors' algorithm-driven systems to determine eligibility for, allocate, and verify legitimate provision of benefits. Private contractors develop many of these systems, some of which are off-the-shelf products while others are developed for specific populations in the jurisdictions where they are used. People with disabilities who are not able to work, or who can work only limited hours, may be reliant on public benefits – including Medicaid coverage for basic health care and long-term supports and services, housing assistance, food stamps, and cash assistance – that are subject to algorithm-driven decisions generated by private companies.

For instance, algorithmic systems are used in determinations about home- and community-based services to assess hours of care a beneficiary will need or the budget for providing necessary care.[109] Advocates have documented that in many cases, states' implementation of these systems has caused sudden, drastic, and arbitrary reductions or terminations of benefits that were previously granted. This has had devastating and terrifying effects on the lives of disabled and low-income people because it deprives recipients of care that supports independent living at home. Recipients cannot reasonably avoid such outcomes because reductions or terminations to their benefits often take effect before they are properly informed. For instance, one health services technology company, Optum, developed a needs assessment tool for Arkansas that cut approved care hours for some people with developmental disabilities in Arkansas nearly in half without explanation, putting them at imminent risk of serious injury and potential institutionalization, and preventing them from completing basic

[108] Claudia Lopez Lloreda, *Speech Recognition Tech Is Yet Another Example of Bias*, Scientific American (July 5, 2020), https://www.scientificamerican.com/article/speech-recognition-tech-is-yet-another-example-of-bias/.
[109] Lydia X.Z. Brown et al, Ctr. for Democracy & Tech., *Challenging the Use of Algorithm-Driven Decision-Making in Benefits Determinations Affecting People With Disabilities* (2020), https://cdt.org/insights/report-challenging-the-use-of-algorithm-driven-decision-making-in-benefits-determinations-affecting-people-with-disabilities/ [hereinafter *Benefits Determinations*].

daily functions like eating and using a bathroom.[110] Similarly, in Indiana, IBM's algorithm-driven system for processing welfare applications caused sudden termination of benefits for huge numbers of low-income people, who received confusing and delayed notices about noncompliance or fraud.[111]

While state agencies violate civil rights and constitutional protections when adopting systems that impose these harms, people currently have little to no recourse against the private companies that develop and sell these tools to arbitrarily and drastically cut people's benefits. Under Title II of the ADA, a person may not be excluded from participation in or denied benefits of the services of any "public entity" on the basis of disability.[112] Public benefits determinations that deprive recipients of benefits that allow them to live independently can force recipients to be institutionalized. This violates the ADA's community integration mandate that the Supreme Court affirmed in 1999, which requires government entities to administer government services and programs in a manner that enables disabled people to interact with non-disabled people in the most integrated setting possible.[113] Although government agencies should avoid procuring systems from private vendors that would interfere with disabled people's ability to continue living in their own homes, vendors are not precluded from selling tools that have this outcome.

Even when a benefits recipient is granted these services in the correct amount, the use of electronic visit verification (EVV) systems can interfere with the provision of personal care services. Similar to algorithmic systems used for benefits determination, EVV mobile apps and software are often provided by private home health tech companies.[114] With these systems, companies like Sandata and Direct Care Innovations require care workers to confirm that they are providing services as approved by interacting with facial recognition, voice verification, and

---

[110] *Id.* at 21. *See also* Upturn, Benefits Tech Advocacy Hub, *Arkansas Medicaid Home and Community Based Services Hours Cuts*, https://www.btah.org/case-study/arkansas-medicaid-home-and-community-based-services-hours-cuts.html; Ryan Calo & Danielle Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 Emory L.J. 797, 799 (2021), https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj.

[111] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, at 39-54 (2018); Rick Callahan & Tom Davies, *Judge: IBM Owes Indiana $78M for Failed Welfare Automation*, APNews (Aug. 7, 2017), https://apnews.com/article/8eb53eb9bdf94adb92e5b8b09559d8d0.

[112] 42. U.S.C. 12132.

[113] Brown, *Benefits Determinations*, *supra* note 105, at 17.

[114] Alexandra Mateescu, Data & Society, Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care 14 (2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf. For a non-exhaustive list of private EVV vendors, *see* Applied Self-Direction, *Directory of EVV Vendors Interested in Serving Self-Direction Programs* (last updated Oct. 5, 2022), https://www.appliedselfdirection.com/resources/directory-evv-vendors-interested-serving-self-direction-programs.

GPS location tracking features during home visits.[115] Companies require workers to verify their service provision through their designated EVV systems frequently, with precision, and within narrow windows of time during their home visits to prove that benefits are not being abused.[116]

When a system incorrectly flags that workers did not provide services at the approved time and location, this delays payments until this flag is resolved, costing workers their wages.[117] This can also obligate recipients to pay for workers' lost wages out of pocket and to stay within the confines of their homes due to geofencing limits that cause their care workers to be flagged for fraud, and it reduces the home care workforce.[118] One company, CareBridge, plans to combine EVV technology with a predictive model to assess care needs, creating new risks for unreliable data practices to undercut provision of care.[119] This interferes with the care disabled people are supposed to receive as well as the wages that care workers (who are disproportionately women of color, and often disabled and from immigrant communities) can lose over minor errors or delays.[120]

Question 6: Prevalence of algorithmic discrimination and sectors of concern

Unfortunately, there is no good data on the prevalence of algorithmic discrimination--either across the economy or in particular sectors--because companies generally are not required to publicly disclose the existence (much less the impact) of automated decision-making in their

[115] Sandata, *Ensure EVV Compliance with Multiple Verification Methods*, https://www.sandata.com/multiple-verification-methods-help-ensure-evv-compliance/; Direct Care Innovations, *High Tech and Low Tech Options for EVV* (Mar. 24, 2019), https://www.dcisoftware.com/blog/dci-evv-options/.
[116] Mateescu, *supra* note 110, at 30. *See also* Public Partnerships, *Time4Care Electronic Visit Verification (EVV) Mobile App*, https://www.publicpartnerships.com/tools/time4care-evv/.
[117] Virginia Eubanks & Alexandra Mateescu, *'We Don't Deserve This': New App Places US Caregivers Under Digital Surveillance*, The Guardian (July 28, 2021, 6:00 AM), https://www.theguardian.com/us-news/2021/jul/28/digital-surveillance-caregivers-artificial-intelligence; Jacqueline Miller et al., University of California San Francisco Health Workforce Research Center on Long-Term Care, *Impact of Electronic Visit Verification (EVV) on Personal Care Services Workers and Consumers in the United States* 12, 15-16 (2021), https://healthworkforce.ucsf.edu/sites/healthworkforce.ucsf.edu/files/EVV_Report_210722.pdf.
[118] Eubanks, *supra* note 113; Naomi Gallopyn & Liza I. Iezzoni, *Views of Electronic Visit Verification (EVV) Among Home-Based Personal Assistance Services Consumers and Workers*, Disability and Health Journal (2020), https://www.ancor.org/wp-content/uploads/2022/08/disability_and_health_journal_article_on_views_of_evv.pdf.
[119] *CareBridge Launches to Improve Care for Individuals Receiving Long-Term Support Services*, Business Wire (Jan. 12, 2020, 4:58 PM), https://www.businesswire.com/news/home/20200113005935/en/CareBridge-Launches-Improve-Care-Individuals-Receiving-Long-Term.
[120] Id at 45-46. See also Lydia X.Z. Brown, *EVV Threatens Disabled People's Privacy and Dignity – Whether We Need Care, or Work as Professional Caregivers*, Ctr. for Democracy & Tech (Mar. 24, 2022), https://cdt.org/insights/evv-threatens-disabled-peoples-privacy-and-dignity-whether-we-need-care-or-work-as-professional-caregivers/.

operations. There are some limited exceptions to this general rule. For example, federal contractors are usually required to maintain records on all personnel actions[121] and may be subjected to compliance reviews by the federal Department of Labor's Office of Federal Contractor Compliance Programs (OFCCP) that require them to reveal information about particular practices.[122] But such information is not collected from a sufficient number of employers to reliably estimate the prevalence of automated decision-making in any particular sector.

Question 7: How access and opt-out rights can address algorithmic discrimination

Lack of transparency regarding automated decision-making is a recurring theme in our responses to the preceding questions, and that opacity is one of the key areas that the Agency can help address through regulations ensuring access and accountability, in particular. Additionally, opt-out rights could help reduce the risk of discrimination, such as by giving disabled consumers and workers the right to opt out of decision-making processes for which they cannot obtain adequate accommodation, or where they otherwise believe the automated system will not make a fair and accurate decision due to their disability.

Question 8: Whether access/opt-out rights should vary depending on certain factors

Access and opt-out rights for automated decision-making should depend, as under the GDPR, on whether the decision affects the consumer's legal rights or would have significant effects on the consumer's life (such as housing, employment, education, and credit). When such decisions are left to automated systems, the consumer should have the right to access the information upon which the decision was based, to obtain an explanation as to the reasons for the decision itself, and to opt-out of purely automated decision-making and request human review. This approach will allow the consumer an opportunity to raise concerns, request accommodation, and make an informed decision about whether, when, and how to proceed with the automated decision-making process. Those rights should not be reduced or otherwise changed in particular settings and sectors.

[121] 41 C.F.R. 60-1.12.

[122] *See generally* Federal Contract Compliance Manual, Chapter 1A00 (Types of Compliance Evaluations), https://www.dol.gov/agencies/ofccp/manual/fccm/1a-introduction/1a00-types-compliance-evaluations.

Question 9: Information that should be included in response to access requests

We recommend that the Agency examine Standard 4 of the *Civil Rights Standards for 21st Century Employment Selection Procedures*,[123] which CDT and a coalition of other national civil rights organizations published in December 2022. Standard 4 would require all companies that sell or use automated employment decision technologies (or other employment selection procedures) to publish a short-form disclosure on their website and provide the disclosure to each candidate about whom the tool will make an employment decision. The required disclosure must include the following:

- What types of employment decisions will be made or informed by the tool,
- The positions for which the selection procedure will be used; the knowledge, skills, abilities, and other characteristics that the tool will assess; how those characteristics relate to the position's essential functions; and how the tool measures those characteristics,
- How to interpret the results or other outputs of the tool,
- Any reasonably foreseeable accommodations that candidates may require,
- How candidates can access accommodations, communicate concerns, or file a complaint relating to the tool, and
- How a candidate can opt out of the automated decision-making process.

We believe that this approach should be applied to automated decisions made in other contexts as well. One way to adapt those requirements for the CPPA, which would cover automated decision-making systems in a broad range of additional settings beyond employment would be to require brief, accessible disclosures that inform consumers subjected to automated decision-making of the following information:

- The types of automated decisions to which the consumer may be subjected,
- How the automated system makes those decisions, including the information it is relying upon and how that information is relevant to the decision being made,
- How the consumer can interpret the system's output,
- What accommodations the consumer may require,
- How the consumer can request accommodation, raise concerns, or file a complaint, and
- How the consumer can opt out of the automated decision process altogether.

[123] *Civil Rights Standards for 21st Century Employment Selection Procedures* (2022), https://cdt.org/insights/civil-rights-standards-for-21st-century-employment-selection-procedures/.

Risk Assessments

Question 1: Existing risk assessment requirements for processing personal information

To our knowledge, there are no laws requiring California[124] businesses to conduct risk assessments for "processing . . . personal information" as a general matter. There are, however, laws requiring companies to conduct analyses regarding certain *decisions* that may be based on the processing of personal data, perhaps most notably in the context of employment discrimination laws. Title VII of the federal Civil Rights Act of 1964, for example, generally prohibits companies from employment practices that have an adverse impact on a protected group. Where such adverse impacts exist, Title VII requires companies to establish that the employment practice causing the adverse impact is "job related for the position in question and consistent with business necessity."[125] However, federal law does not affirmatively require companies to conduct adverse impact analyses or job-relatedness (or validation) studies; companies simply have an incentive to do so to avoid liability for discrimination should adverse impacts arise as a result of using a selection procedure.

The absence of effective risk assessment requirements for the processing of personal information is a major weakness in the current legal regime governing the processing of personal information, particularly when decisions significantly impacting the consumer are made through such processing. Companies should be required to conduct detailed impact assessments to identify potential harms that might result from the processing of personal information *before* deploying systems relying on such processing.

Question 2: Harms that can result from processing personal information

For this question, we incorporate by reference our response to questions 4 and 5 from the Automated Decision-making section.

Question 3: GDPR and other potential models for risk assessment requirements

We would consider the GDPR's data protection impact assessment provisions to be a solid, if imperfect, model for risk assessment requirements. Substantively, the GDPR requires the impact assessment to describe the data processing operations, state the purposes of the processing,

[124] In our response to Question 3, below, we discuss laws applicable elsewhere--specifically the EU's GDPR and the Colorado Privacy Act.
[125] 42 U.S.C. 2000e-2(k)(1)(A)(i).

and assess the necessity and proportionality of the processing in relation to those purposes, the risks to the "rights and freedoms" of data subjects, and the measures envisaged to address those risks.[126] These are sound principles, although merely assessing potential threats to data subjects' "rights and freedoms" does not address the full scope of potential risk that consumers face when subjected to data processing that affects major aspects of the data subject's life or livelihood, such as decisions relating to housing, employment, or education.

To provide a more thorough and meaningful disclosure, we recommend an approach akin to that suggested by the Berkeley Labor Center in its Framework for Worker Technology Rights (hereafter, "BLC Framework").[127] Specifically, Section 8 of the BLC Framework covers impact assessments, and it states companies "should evaluate the full range of potential harms to workers," including "discrimination, harms to mental and physical health and safety, loss of privacy, and negative economic impacts."[128]

The GDPR's approach is also limited in other respects. It requires impact assessments only when a "new" technology "is likely to result in a high risk to the rights and freedoms of natural persons."[129] The impact assessment requirement should not be limited to new technologies; on the contrary, companies should be required to reexamine their data processing operations regularly to ensure that new risks are identified and mitigated when they arise in the course of a processing system's operations. Moreover, the GDPR's "likely to result in a high risk" limitation on which systems must be assessed is too ambiguous, potentially leaving companies with the ability to avoid the requirements by claiming that they did not subjectively perceive the risk of harm to be "high." The Colorado Privacy Act's (CoPA) data protection assessment requirements suffer from a similar deficiency, requiring assessments to be conducted only if the data processing creates a "reasonably foreseeable risk of" certain harms.[130]

The scope of the Agency's risk assessment requirements should instead be based on concrete factors such as the nature of the processing (e.g., those relating to employment, education,

[126] General Data Protection Regulation, art. 35.7.
[127] Annette Bernhardt, et al., Berkeley Labor Center, *Data and Algorithms at Work: The Case for Worker Technology Rights*, Part II: A Framework for Worker Technology Rights, Nov. 3, 2021, https://laborcenter.berkeley.edu/data-algorithms-at-work/.
[128] *Id.*
[129] General Data Protection Regulation, art. 35.1.
[130] Colo. Rev. Stat. § 6-1-1309(2)(a).

housing, credit, etc, or that process sensitive personal information) and the number of consumers potentially affected.[131]

Question 4: Minimum content of impact assessments
Question 5: Benefits and drawbacks of adopting GDPR or CoPA approaches
Question 6: Format of risk assessments submitted to the Agency

For the reasons stated in response to Question 3, we believe that the impact assessment requirements of the GDPR are a good starting point for the Agency, with the caveats stated in that response regarding the scope of what types of data processing should be subject to risk assessment requirements.

We do not believe that the requirements of the CoPA serve as a suitable model for the content of risk assessment requirements because they are not specific as to what details should be included in such assessments. The CoPA requires companies to "identify and weigh" the data processing's potential "benefits" and "risks to the rights of the consumer," factoring in circumstances such as "the use of de-identified data and the reasonable expectations of consumers."[132] These requirements are too vague and, on their face, could allow companies to satisfy the statute with very cursory impact assessments that would provide neither the company, consumers, nor the Agency with the information needed to determine the degree of risk a data processing practice might pose.

We believe that the Agency should require risk assessments that, at a minimum:

- Identify the purposes of the data processing
- Describe the nature of the data processing
- Assess the necessity and proportionality of the data processing in relation to the purposes
- Evaluate the full range of potential harms to consumers and workers that the data processing may pose, including potential harms relating to consumers' and workers':
    - Rights and freedoms, including the right to be free from discrimination
    - Health and safety
    - Finances and economic situation

[131] The National Institute of Standards and Technology's AI Risk Management Framework proposes additional factors to consider when measuring risk. *See Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, *supra* note 5.
[132] Colo. Rev. Stat. § 6-1-1309(3).

- State what safeguards, mitigation measures, or other efforts to address these potential harms the data processor has taken, and what additional steps could or should be taken to reduce the risk of harm
- Are conducted prior to the deployment of the data processing system or practice, and repeated at least annually for as long as the system or practice remains in place
- Are conducted by a third party with no conflict of interest with respect to the data processor or the data at issue
- Are:
    - Submitted to the Agency; and
    - Published in an accessible format on the website of the data processor and any company from whom the data was obtained or with whom the data is sold or shared

Conclusion

We thank the Agency for its thoughtful questions on these important topics and for providing us with the opportunity to comment in advance of the formal rulemaking process. We look forward to engaging with the Agency and supporting its efforts to protect the rights and dignity of California's consumers and workers.

From:	Monticollo, Allaire [redacted]
Sent:	Monday, March 27, 2023 8:16 AM
To:	Regulations
Cc:	Christopher Oswald; [redacted]
Subject:	Association of National Advertisers (ANA) - Comments - PR 02-2023
Attachments:	ANA Comments in Response to CPPA's Request for Preliminary Input on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Dear California Privacy Protection Agency:

Please find attached comments of the **Association of National Advertisers (ANA)** in response to the California Privacy Protection Agency's invitation for preliminary comments on its proposed rulemaking related to cybersecurity audits, risk assessments, and automated decisionmaking. We appreciate your consideration of these comments.

If you have any questions about this letter, please feel free to reach out to Chris Oswald, Executive Vice President for Law, Ethics, & Government Relations for the Association of National Advertisers at [redacted].

Best Regards,
Allaire Monticollo

Allaire Monticollo, Esq. (she/her) | Venable LLP
t [redacted] | **f** [redacted]
600 Massachusetts Avenue, NW, Washington, DC 20001
[redacted] | www.Venable.com

Before the
CALIFORNIA PRIVACY PROTECTION AGENCY
Sacramento, CA 95834

COMMENTS

of the

ANA – ASSOCIATION OF NATIONAL ADVERTISERS

on the

INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING
PR 02-2023

Christopher Oswald
EVP for Law, Ethics, & Govt. Relations
Association of National Advertisers
2020 K Street, NW
Suite 660
Washington, DC 20006
[redacted]

Counsel:
Stu Ingis
Tara Sugiyama Potashnik
Allaire Monticollo
Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
[redacted]

March 27, 2023

On behalf of the Association of National Advertisers ("ANA"), we provide input ("Comments") below in response to the California Privacy Protection Agency's ("CPPA" or "Agency") request for preliminary comments on its proposed rulemaking related to cybersecurity audits, risk assessments, and automated decisionmaking ("RFC").[1] As America's oldest and largest advertising trade association, the ANA has long supported brands, advertisers, marketing service providers, and countless other entities that engage in advertising in their mission to connect consumers with relevant messaging, products, and services. We assist our member companies in their efforts to address applicable legal obligations, including by helping members identify appropriate data governance activities and by encouraging members to maintain relevant documentation related to the topics set forth in the RFC. We thank the Agency for the opportunity to respond to its request for preliminary comments on these important topics.

The mission of the ANA is to drive growth for marketing professionals, brands and businesses, the industry, and humanity. The ANA serves the marketing needs of 20,000 brands by leveraging the 12-point ANA Growth Agenda, which has been endorsed by the Global CMO Growth Council. The ANA's membership consists of U.S. and international companies, including client-side marketers, nonprofits, fundraisers, and marketing solutions providers (data science and technology companies, ad agencies, publishers, media companies, suppliers, and vendors). The ANA creates Marketing Growth Champions by serving, educating, and advocating for more than 50,000 industry members that collectively invest more than $400 billion in marketing and advertising annually. Our members include small, mid-size, and large firms, and virtually all of them engage in or benefit from data-driven advertising practices that give consumers access to relevant information, messaging, and advertisements at the right time and in the right place.

Our Comments proceed by first discussing the Agency's regulatory mandate under the text of the California Consumer Privacy Act ("CCPA") itself. We urge the CPPA to critically consider and clearly define which processing activities present a "significant risk" to consumer privacy or security. We then address the topics of cybersecurity audits and risk assessments and encourage the Agency to promote flexible regulatory standards that can be tailored to the nature of the personal information processed and the size, sophistication, and resources available to regulated entities. Finally, we recommend that the Agency's proposed rules related to automated decisionmaking align with existing requirements in other jurisdictions to promote consumer opt-out rights for the benefit of all Californians and harmonize with the approach to privacy choices taken by the CCPA. Overall, we emphasize that the CPPA must remain within the bounds of its regulatory authority when promulgating rules related to cybersecurity audits, risk assessments, and automated decisionmaking. We ask the Agency to promote flexibility, interoperability, and clarity in regulatory requirements tied to such topics.

[1] California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking – Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking* (Feb. 10, 2023), located here (hereinafter, "RFC").

I. The Agency's rules related to cybersecurity audits and risk assessments should be clearly defined and must address processing activities that present a "significant risk" to consumer privacy or security.

The CCPA specifically authorizes the Agency to "issu[e] regulations requiring businesses whose processing of consumers' personal information presents *significant risk* to consumers' privacy or security" to perform cybersecurity audits and risk assessments.[2] Regulations related to cybersecurity audits and risk assessments should clearly define which activities present a significant risk to consumers and should refrain from extending the concept of "significant risk" to routine, reasonable, and expected data processing activities. "Significant risk" is a higher standard than "risk" alone, and the Agency should acknowledge as much in its regulations.

Additionally, the Agency should place auditing and assessment requirements on only those *processing activities* that present a significant risk to consumers' privacy or security, rather than businesses' data processing practices as a whole. Such a regulation would help ensure the processing activity that actually presents the significant risk to consumers is appropriately scrutinized and analyzed in an assessment or audit. Auditing and assessment requirements should be imposed only for business processing activities that present a significant risk to consumer privacy or security.

Finally, the CPPA should prioritize clarity in its rules related to cybersecurity audits and risk assessments. To promote such clarity, the Agency should consider plainly defining "significant risk" to mean "personal information processing that (A) results in demonstrable and quantifiable harm to a consumer, and (B) is completed to determine that a consumer is ineligible for any of the following benefits: employment, credit, insurance, health care, education admissions, financial aid, or housing, except as permitted under other applicable laws."[3]

Processing decisions impacting the aforementioned critical areas may reasonably be subject to additional data governance processes, such as cybersecurity audits or risk assessments, given that the consequences of those processing decisions may impose a heightened risk to consumers. Other processing activities, such as routine data processing to facilitate advertising, do not present a similarly *significant risk* to consumer privacy or security. Moreover, such processing activities should be subject to auditing and assessment requirements only if they may result in actual, tangible harm to consumers. Including such a harm requirement in the definition of "significant risk" would reduce the need for businesses to complete assessments or audits for processing activities do not present any sort of risk of harm to consumers. The Agency should prioritize drafting a clear definition of what constitutes "significant risk," and including a harm standard in its definition, as such clarity will help businesses accurately evaluate when cybersecurity audits and risk assessments are required under California law.

---

[2] Cal. Civ. Code § 1798.185(a)(15) (emphasis added).

[3] *See generally* Civil Rights Act of 1964, 42 U.S.C. § 2000d et seq.; Fair Housing Act, 42 U.S.C. § 3601 et seq.; Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; Equal Credit Opportunity Act, 15 U.S.C. § 1691 et seq.; Americans with Disabilities Act, 42 U.S.C. § 12101 et seq.

II. Regulatory requirements related to cybersecurity audits and risk assessments should be appropriately tailored to businesses' size and sophistication and should be interoperable with similar requirements under other laws.

The CPPA's regulations related to audits and assessments should not impose one-size-fits-all mandates on businesses. Regulations should instead focus on promoting flexibility so that businesses of all sizes can meet applicable requirements, even in the face of potentially unavoidable constraints they may face in terms of staff and time available to dedicate to audits and assessments. When determining the scope of audit and assessment requirements, the Agency should keep in mind the fact that smaller businesses may not have as many resources to contribute to data governance requirements as their larger business counterparts. The Agency's requirements should thus be clear and tailored to the size and complexity of the business and the nature and scope of data processing activities.

Existing laws place requirements on businesses to conduct cybersecurity audits and risk assessments related to data processing. The Agency's RFC specifically asks about the benefits and drawbacks related to accepting audits and assessments businesses have completed to comply with such other laws.[4] One significant benefit of accepting such audits and assessments would be simplifying compliance for companies who are already required to complete audits and assessments under different legal regimes. The Agency should accept audits and assessments conducted to satisfy other laws, such as the European Union's General Data Privacy Regulation (GDPR), the Connecticut Data Privacy Act, the Colorado Privacy Act, and the Virginia Consumer Data Protection Act.[5] A regulation stating that the Agency will accept cybersecurity audits and risk assessments issued under other relevant state or federal laws or standards-setting bodies would provide clarity and consistency for businesses operating in California.

The Agency should also clarify that any documentation it collects from businesses as part of the audit and assessment requirements remains protected under applicable work product and/or attorney-client privilege doctrines. This approach has been adopted by virtually every other state that has required risk assessments related to data processing activities.[6] Attorney-client privilege and work product protections create a sphere of safety surrounding businesses' confidential conversations with their legal representatives. These protections help ensure that companies seeking advice or aid from attorneys can be completely open and frank with their counsel, which facilitates better outcomes for consumers, businesses, and society overall. Ensuring businesses' work product and attorney-client privilege protections remain in-tact in the context of auditing and assessment requirements will ensure the foundational purposes for such protections continue to be prioritized.

III. Regulations related to automated decisionmaking should promote meaningful transparency and an opt-out regime to align with the text of the CCPA.

We encourage the Agency to ensure its requirements related to automated decisionmaking reflect the regulatory directive set forth in the CCPA and align with similar

[4] RFC at Section I(3), Section II(5).
[5] E.U. General Data Protection Regulation at Art. 35; Conn. Gen. Stat. § 42-522; Colo. Rev. Stat § 6-1-1309; Va. Code Ann. § 59.1-580.
[6] *Id.*

requirements in other states. Specifically, the law tasks the Agency with issuing regulations "governing access and opt-out rights with respect to businesses' use of automated decision making technology."[7] As a result, the CPPA should ensure its regulations promote transparency that will be useful and meaningful to consumers regarding automated decisionmaking processes, as well as provide opt-out choices for such processing.

Access requirements related to automated decisionmaking should provide consumers with useful and understandable information about applicable practices while ensuring businesses' proprietary information and trade secrets remain protected. In particular, the CCPA states the Agency may promulgate rules requiring businesses to include "a description of the likely outcome of the [automated decisionmaking] process with respect to the consumer." Any such requirements should be limited to providing a description of potential outcomes and results for consumers writ-large rather than requiring businesses to individualize responses to specific consumers by guessing at the outcome of the process prior to it being initiated or finalized.

The CCPA also states the Agency may promulgate rules requiring businesses to include "meaningful information" about the logic involved in automated decisionmaking processes in response to a consumer access request.[8] Access rights should be appropriately tailored to promote transparency while refraining from requiring businesses to divulge trade secrets or other protected business information. The Agency should balance the need to promote meaningful transparency for consumers with the need of businesses to keep their proprietary algorithms and systems protected. The CPPA should refrain from forcing businesses to make overly specific disclosures regarding automated decisionmaking processes to avoid mandating that they reveal information that could place them at a competitive disadvantage.

Finally, the Agency's automated decisionmaking rules should be harmonized with other legal requirements related to automated processing to the extent such alignment is possible. Such harmonization would ensure Californians may exercise meaningful choices regarding automated decisionmaking processes as well as foster reliable consumer expectations about such processing. The Agency should prioritize adopting requirements related to automated decisionmaking that promote interoperability among state privacy laws, ensure Californians have a consistent and clear set of expectations about businesses' automated decisionmaking activities, and simplify compliance efforts for businesses.

* * *

Thank you for the opportunity to submit these Comments in response to the Agency's RFC. Please do not hesitate to contact us with any questions regarding this submission.

[7] Cal. Civ. Code § 1798.185(a)(16).
[8] *Id.*

From: Joanne Furtsch [redacted]
Sent: Monday, March 27, 2023 8:35 AM
To: Regulations
Subject: CPPA Public Comment: PR 02-2023
Attachments: CCPA Regulation Comments_FINAL.pdf

Attn: Kevin Sabo

Please find TrustArc's comments regarding the proposed rulemaking for cybersecurity audits, risk assessments, and automated decision making attached. Contact me if you have any questions.

Best -
Joanne Furtsch

Joanne B. Furtsch
Director, Privacy Intelligence Development / CIPP/US/C, CIPT, FIP
M: [redacted] | [redacted]

August 23, 2022

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834
Attn: Brain Soublet

By Email Submission to: regulations@cppa.ca.gov

RE: TrustArc's CCPA Public Comment

TrustArc Inc ("TrustArc") appreciates the opportunity to provide comments on the text of the proposed California Consumer Privacy Act Regulations. TrustArc knows well the challenges consumers face in protecting their personal information and businesses encounter when implementing new laws and regulations. TrustArc agrees that clear guidelines for businesses to implement the law's requirements are necessary to ensure consumers are able to easily and effectively manage their rights under the California Consumer Privacy Act.

Our concerns center around the cost and effort to implement that may overshadow consumer rights. There is an opportunity to clarify the requirements in a way that enables businesses, and their service providers and contractors to comply.

We want to emphasize the following:

- Rules need to be clarified around how a business needs to obtain new consent when there is a conflict between the consumer's established preference and browser signal setting.

- The mechanisms businesses must implement to communicate whether a consumer's preference signal is being honored need clear requirements.

- The new requirements to manage third party service providers and contractors open the door for contractual abuse if not specifically addressed, especially for small businesses that do not have leverage to change or update service agreements.

Our detailed comments are provided below. For any questions regarding this submission, please contact Joanne Furtsch, Director, Privacy Intelligence Development, at [redacted].

I. OPT-OUT SIGNALS

A. § 7025. Opt-out Preference Signals May Increase Consumer Consent Fatigue.

Issue
Consumers are constantly inundated now with making choices about the use of trackers to the point that they accept (or decline) everything without understanding the effect on their rights. The following implementation may create an endless loop.

Requirement: c(3)
(3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display in a conspicuous manner the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

Example: c(7)(B)
(B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.

Problem
TrustArc believes there may be an endless loop with how the requirement in c(3) may be implemented based on the example described in c(7)(B).

Each time the consumer ("Noelle") visits the website with her opt-out preference signal on and is not yet logged in, the opt-out signal must be honored. If she logs in, and her preferences conflict with the opt-out signal, she has to confirm consent to the sale/sharing of her personal information. This will happen each time she visits the site because the site does not recognize her until she logs in.

If she logs out of the site and then comes back (opt-out preference signal is on), the signal is honored, she logs back in, new confirmation of consent is required because there is a conflict between her preference and the signal. She is considered opted-out until she consents again.

This will happen each time she logs out and revisits the site, creating an endless cycle of the site having to obtain new consent and a poor user experience each time she visits the site.

Recommendation
A clarification needs to be added explaining that once a consumer has consented to the sale/sharing of their personal information and the business has logged receiving the consumer's consent while their preference signal was on, the signal can be subsequently ignored when the consumer logs back in again and the site recognizes that the consumer as having consented to the sale/sharing of their personal information. Consent then does not need to be collected each time the consumer logs back in.

If the consumer does not log in, and is not recognized by the site, then the preference signal must be honored for that device until the consumer logs in and is recognized by the site.

B. § 7025. Opt-Out Preference Signals Need Clear Implementation Requirements.

Issue
Opt-out preference signal being honored indicator as described in c(6) is unclear about what exactly is required.

Requirement: c(6)
(6) The business should display whether or not it has processed the consumer's opt-out preference signal. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

Problem
It is unclear what the "honored" indicator needs to look like and how businesses should go about implementing this requirement. For example, if a business implements a toggle or radio button as described in c(6), what effect clicking the toggle or radio button is supposed to have is unknown.

Recommendation
The proposed regulation should outline clear requirements for implementing the opt-out preference signal honored indicator. Requirements should address where on the website does the indicator need to appear and how prominent does it need to be in relation to other items on the website. If the toggle or radio button is implemented, explain what the toggle is expected to do and the types of actions a consumer could take.

Consider allowing the use of an icon, something similar to the DAA Ad Choices icon, that is easily recognizable, does not take up much real estate on the site, and is easily actionable by consumers.

II. CONTRACTUAL ISSUES FOR SERVICE PROVIDERS AND CONTRACTORS

A. Article 4 § 7051 Contract Requirements for Service Providers and Contractors.

Issue
Potential for contractual requirements that lead to ineffective and non-compliant business operations.

Requirement: (a)(6)
(a) The contract required by the CCPA for service providers and contractors shall

(6) Require the service provider or contractor to comply with all *applicable sections of the CCPA and these regulations, including providing the* ***same*** *level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.*

Problem
The problem is not in the intent, but in how the wording will be implemented. The word "same" where bolded in (a)(6) of Article 4 § 7051 can create a level of contractual complexity that can make it nearly impossible for any business to meet the requirements, especially a small business or a contractor who is typically an individual.

In particular, a service provider's customers will each tend to add specific privacy and security controls rather than requiring "reasonable" procedures and practices - emphasizing the "same" rather than the "same level." The varied specificity will create an impossible compliance regime for service providers. Whereas a service provider can negotiate their own controls, they may be required to push down the "same" controls to their subcontractors; thus, compounding the conflicting requirements.

Thus, the problem is in the interpretation and implementation. It is not possible for a service provider to have the **same** privacy protection as required by all of its customers, although the **same level** is possible.

Recommendation:
1. Replace the word "same" with "appropriate" to read "...including providing appropriate levels of privacy protections as required by all its customers…"
2. Add a requirement for the service providers to meet the CCPA level of protection imposed and make it clear that meeting the CCPA standards is sufficient.

This will align California's requirements with other U.S. state laws and federal laws such as HIPAA (the Health Insurance Portability and Accountability Act of 1996, along with its subsequent amendments, "HIPAA") as noted in the two examples below.

Example 1:
Under the Colorado Privacy Act CRS 6-1-1305(4)[1], processors are required to implement *"...appropriate technical and organizational measures to ensure a level of security appropriate to the risk…"* .

(4) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures.

Example 2:
The HIPAA Security Rule 45 CFR § 164.308[2] - Administrative safeguards. (b)(1) and (b)(2) use the phrase "…obtains satisfactory assurance that they will appropriately safeguard the information…"

(b)
(1) Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

B. Article 4 § 7051 Contract Requirements for Service Providers and Contractors

Issue
Clarification desired for self reviews or third-party review to meet the requirement.

Requirement: (a)(7)
(a) The contract required by the CCPA for service providers and contractors shall

(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.

[1] Colorado Privacy Act CRS 6-1-1305(4)
[2] HIPAA Security Rule 45 CFR § 164.30 (b)(1) and (b)(2)

Problem
It is not clear whether the draft regulation allows service providers to use third party audits or certifications as a means to fulfill the audit requirement in Article 4 § 7051(a)(7) and enable businesses to recognize those as such.

Both the Colorado Privacy Act[3] and Virginia Consumer Data Protection Act[4] allow for processors to use a qualified and independent third party to conduct an audit to ensure that the processor is meeting its obligations.

Recommendation:
Include independent third party reviews, and specify certifications and validations as a means to satisfy the audit requirement by adding the words "internal or third party" and "certifications and validations" to the last sentence to have it read as follows:

> *Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third party assessments, audits, certifications and validations, or other technical and operational testing at least once every 12 months.*

This will align the regulation with other U.S. state consumer privacy laws that recognize independent third party reviews as a means to demonstrate compliance.

C. Article 4 § 7051 Contract Requirements for Service Providers and Contractors

Issue
Disproportionate impact on small businesses if audits or tests are required as a defense.

Requirement: (e)
(e) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Problem
If a business does not exercise the right to audit its service providers, it puts them at a disadvantage. For example, small businesses use a variety of cloud services to manage their business and the personal information that is collected. Large service providers such as Google, Oracle, and Salesforce have services that cater to small businesses. Small businesses are not able to impose a right to audit on these organizations. If a large service provider is using personal information in violation of CCPA, a small business

[3] Colorado Privacy Act CRS 6-1-1305 - Responsibility according to role - Audits
[4] Virginia Consumer Data Protection Act § 59.1-575. B. Responsibility according to role; controller and processor. - Contracts

will be unable to effectively defend itself if it is unable to “audit” or “test the . . . systems” of the service provider.

If the small business is a service provider, it is costly for them to submit to such audits making it harder for them to compete against larger competitors.

Recommendation
Allow business to rely on public third party audit results (e.g., SOC 2 reports) or third party certifications or validations conducted by an independent and qualified third party. As noted above, both the Colorado Privacy Act and Virginia Data Protection Act allow for the recognition of third party audits, certifications, and validations as a means to ensure processors are meeting their obligations under these laws.

Some large service providers like Salesforce already have areas of their website[5] dedicated to building trust and demonstrating compliance listing out the third party audits and certifications they undergo. Validation of these certifications can be easily checked by businesses and consumers.

D. § 7053. Contract Requirements for Third Parties.

Issue
Infeasible requirement for current state of technology.

Requirement: (b)
(b) A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party’s own purposes, shall contractually require the third party to check for and comply with a consumer’s opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information.

Issue
This requirement is difficult for any business with third party contracts to manage. It places administrative burdens on businesses requiring processes and mechanisms by which to communicate the consumer’s consent. Implementation will be difficult to enforce due to a lack of consistency across customers (e.g., a third party complying with various customer requirements) and current state of technology and interoperability.

Recommendation
Table this requirement until uniform opt-out global privacy control is adopted.

Conclusion
Thank you for your time and consideration. We look forward to enhancements and further clarification as noted above. For any questions regarding this submission, please contact Joanne Furtsch, Director, Privacy Intelligence Development, at [redacted].

[5] https://compliance.salesforce.com/en?_ga=2.131851719.912381987.1659482552-1570373810.1659482552

From: Kate Goodloe [redacted]
Sent: Monday, March 27, 2023 9:42 AM
To: Regulations
Cc: Olga Medina; Matthew Lenz; Abigail Wilson
Subject: PR 02-2023 - Comments of BSA | The Software Alliance
Attachments: 2023.3.27 - BSA Comments to CPPA - Final.pdf

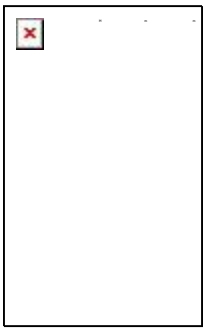
WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Good morning,

BSA | The Software Alliance appreciates the opportunity to submit comments in response to the CPPA's invitation for preliminary comments on cybersecurity audits, risk assessments, and automated decision-making. Please find our comments attached. We would welcome an opportunity to further engage with the CPPA on these important issues.

Best,

Kate Goodloe



Kate Goodloe
Managing Director, Policy
BSA | The Software Alliance
W bsa.org

BSA | The Software Alliance

Submission to California Privacy Protection Agency
Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decision-Making

BSA | The Software Alliance appreciates the opportunity to submit comments in response to the invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (CPRA) and the California Consumer Privacy Act (CCPA) regarding cybersecurity audits, risk assessments and automated decision-making. We appreciate the California Privacy Protection Agency's (CPPA's) work to address consumer privacy and its goal of issuing regulations that better protect consumer privacy.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive data — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and BSA members' business models do not depend on monetizing users' personal information.

Our comments focus on the three topics on which the CPPA seeks input:

1. ***Cybersecurity Audits.*** New regulations are to require annual cybersecurity audits for businesses whose processing presents a "significant risk" to security. We urge the CPPA to allow companies to satisfy this requirement by demonstrating compliance with existing laws or internationally-recognized cybersecurity standards — without creating new audits or assessments. We also encourage the CPPA to define "significant risk" in line with, or by reference to, leading cybersecurity laws, policies and standards.

2. ***Risk Assessments.*** New regulations are to require businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy to submit risk assessments to the CPPA. We urge the CPPA to ensure these risk assessments are interoperable with risk assessments conducted under leading global and state privacy laws. We also encourage the agency to define "significant risk" to privacy in line with leading global and state data protection laws and to focus

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

on requiring companies to provide assessments upon request, rather than requiring all companies provide assessments to the agency on a standard timeframe.

3. ***Automated Decision-Making.*** New regulations are to address the use of automated decision making in certain circumstances. We support reading this authority in line with the narrow statutory text, to focus the use of automated decision-making technology in the context of the access and opt-out rights already included in the CCPA. If the agency creates a right to opt out of profiling under California law, we encourage the CPPA to ensure that right aligns with similar rights in global privacy laws and in other states, so that California consumers may exercise their rights using established and centralized processes.

I. Cybersecurity Audits

Under the CCPA, regulations are to require businesses whose processing of personal information presents "significant risk" to consumers' security to perform annual cybersecurity audits. The statute identifies several factors to be used in assessing whether processing involves significant risk and states that regulations are to define the scope of the audit and establish a process to ensure that audits are "thorough and independent."[2]

BSA recognizes that data security is integral to protecting personal information and privacy. Given the dramatic increase in the cybersecurity laws worldwide, we strongly encourage the CPPA to focus on recognizing compliance by companies with existing cybersecurity laws and standards — without creating any new certification or audit standards.

Question 1*: What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits? For the laws identified:*

a. *To what degree are these laws' cybersecurity audit requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?*
b. *What processes have businesses or organizations implemented to comply with these laws that could also assist with their compliance with CCPA's cybersecurity audit requirements?*
c. *What gaps or weaknesses exist in these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?*
d. *What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?*
e. *Would you recommend that the Agency consider the cybersecurity audit models created by these laws when drafting its regulations? Why, or why not?*

Companies already comply with a significant range of obligations designed to support strong cybersecurity practices. These include not only obligations that are legally required, but an increasing number of compliance assessments and audits that are regularly used across industry sectors even though they are not directly required by legislation. For example, the United States Government requires companies supplying products or services to federal agencies comply with FedRAMP, the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC), the Federal Information Processing Standards, and forthcoming NIST conformity assessments, among other requirements. Internationally, companies often certify compliance to standards based on the Common Criteria, which underpin the Common Criteria Recognition Agreement. In Japan, the Information System Security Management and

[2] Cal. Civil Code 1798.185(15)(A).

Assessment Program (ISMAP) applies cybersecurity protections to government cloud services; the United Kingdom, Korea, Singapore, and Australia have similar schemes.

These requirements are part of a rising number of cybersecurity laws globally. In the European Union alone, the Network and Information Security 2 (NIS2) Directive took effect in January, creating new cross-sector cybersecurity requirements.[3] The EU has also adopted new cybersecurity requirements financial services entities (through the Digital Operational Resilience Act) and is proposing additional cybersecurity regulations for products with digital elements (through the Cyber Resilience Act).

In the United States, businesses conduct audits or assessments of their cybersecurity practices to comply with a range of laws including:

- *Sarbanes-Oxley Act (SOX)***,** which requires publicly traded companies to maintain adequate controls, including cybersecurity controls, over their financial reporting;
- *Health Insurance Portability and Accountability Act of 1996 (HIPAA),* which requires organizations that possess patient health information to protect that information;
- *Gramm-Leach-Bliley Act (GLBA),* which requires financial institutions to secure customer information;
- *Federal Acquisition Regulation (FAR),* which require organizations that sell solutions to the US Government to meet baseline cybersecurity practices; and
- *Defense Federal Acquisition Regulations Supplement (DFARS),* which requires organizations in the defense industrial base to meet baseline cybersecurity practices.

In addition to any legal requirements to conduct cybersecurity audits, customers often require their vendors to demonstrate strong cybersecurity practices — creating another layer of certifications and audit requirements. For example, customers frequently require vendors to certify they are compliant with the ISO 27000 series of standards (which govern information security management)[4] and Service Organization Control (SOC) 2 Type 2 requirements (which assess controls related to security, availability, processing integrity, confidentiality, or privacy of information).[5] Companies that offer multiple products may be required to obtain a certification for each product, compounding these requirements.

Organizations have invested heavily in complying with these cybersecurity obligations, but the increasing number and variety of cybersecurity obligations can make it more costly for companies to serve government and private sector organizations, create additional barriers to entry for smaller businesses, and divert resources that would otherwise focus on substantively improving security. As the President's National Security Telecommunications Advisory Committee (NSTAC) draft Strategy for Increasing Trust Report notes:

> Against this backdrop, the number of security requirements and security assurance programs have increased dramatically. This cacophony has a cost. While government Departments and Agencies (hereinafter, "Agencies") and private businesses have long noted a shortage of qualified security personnel, they have nonetheless created an environment in which valuable and limited resources must be spent to comply with overlapping and sometimes redundant or inconsistent regulatory regimes. To create a more meaningful and robust system, the U.S. government must

[3] EU Directive 2022/2555, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.
[4] *See* ISO/IEC 27001 and related standards, *available at* https://www.iso.org/isoiec-27001-information-security.html.
[5] *See* Association of International Certified Professional Accountants, SOC for Service Organizations, *available at* https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.

streamline the way that security requirements are created, strengthen mechanisms for vendors to demonstrate compliance, and provide easier ways for vendors to convey their efforts to concerned parties.[6]

The Biden-Harris Administration expressly supported harmonizing audit requirements in its recently-published National Cybersecurity Strategy. That Strategy encourages regulators to work together to minimize the harms created by duplicative or overly burdensome regulations, after finding that effective regulations minimize cost burden and thereby enable organizations to invest in "building resilience and defending their systems and assets." The Strategy identifies ensuring cybersecurity regulatory frameworks are "harmonized to reduce duplication" and "cognizant of the cost of implementation" as a strategic objective of the Administration.[7] In addition, the Strategy recognizes that "regulators should work to harmonize not only regulations and rules, but also assessments and audits of regulated entities." This latter point — of harmonizing audits — is critical to avoid duplicative requirements for companies subject to cybersecurity regulations.

In other contexts, states including California have recognized the importance of treating companies as compliant with state requirements when they already fulfill similar federal requirements. For example, California participates in the StateRAMP program, which recognizes that companies that have invested in compliance with FedRAMP are compliant with similar obligations at the state level. The same approach is needed here.

Recommendation: The CPPA should allow companies to satisfy any new California requirements by complying with existing cybersecurity laws or standards, through self-attestation or obtaining a recognized certification, which demonstrates the business is managing cybersecurity risks in line with California requirements

Question 2*: In addition to any legally required cybersecurity audits identified in response to question 1, what other cybersecurity audits, assessments, or evaluations that are currently performed, or best practices, should the Agency consider in its regulations for CCPA's cybersecurity audits pursuant to Civil Code 1798.185(a)(15)(A)? For the cybersecurity audits, assessments, evaluations, or best practices identified:*

- *a. To what degree are these cybersecurity audits, assessments, evaluations, or best practices aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?*
- *b. What processes have businesses or organizations implemented to complete or comply with these cybersecurity audits, assessments, evaluations, or best practices that could also assist with compliance with CCPA's cybersecurity audit requirements?*
- *c. What gaps or weaknesses exist in these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?*
- *d. What gaps or weaknesses exist in businesses or organizations' completion of or compliance processes with these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?*

---

[6] *See* Draft NSTAC Strategy Trust Report (Jan. 31, 2023), *available at* https://www.cisa.gov/sites/default/files/202303/Draft%20NSTAC%20Strategy%20for%20Increasing%20Trust%20Report%20% 281-31-23%29_508.pdf.

[7] National Cybersecurity Strategy, Strategic Objective 1.1 (March 2023), *available at* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

e. *Would you recommend that the Agency consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations? Why, or why not? If so, how?*

California should not create its own cybersecurity certification or audit standards. Rather, the CPPA should recognize compliance with existing standards and best practices for cybersecurity risk management as meeting any new California requirements.

In addition to the obligations discussed above, the CPPA should recognize that compliance with existing standards and best practices for cybersecurity risk management, including the NIST Cybersecurity Framework and the ISO 27000 family of standards, meet any new California requirements. NIST's Cybersecurity Framework and ISO 27001 are the leading tools for organizations and governments to use in managing cybersecurity-related risks.[8] NIST is also in the process of updating its Cybersecurity Framework, to keep pace with improvements in cybersecurity risk management. Although the Cybersecurity Framework was initially developed with a focus on critical infrastructure, such as transportation and the electric power grid, it has been adopted far more broadly by cross-sector organizations of all sizes and has been embraced by governments and industries worldwide. Likewise, as the leading global standard for information security, ISO 27001 is leveraged widely by organizations of all sizes. The CPPA should recognize compliance with these longstanding and trusted resources.

By recognizing that compliance with existing cybersecurity obligations meets California's requirements, the CPPA can drive investment in strong practices that lead to better outcomes. In contrast, new regulations that create another layer of audit requirements would fragment compliance and divert resources that could otherwise be focused on substantively improving cybersecurity protections. That approach would also make it much more challenging for California companies to expand and compete in the global marketplace because in addition to meeting the CCPA's requirements, they would then have to invest heavily in meeting the cybersecurity requirements used by other states, the US Government, and other countries around the world.

Recommendation: California should not create its own cybersecurity certification or audit standards. Rather, the CPPA should recognize compliance with existing standards and best practices for cybersecurity risk management as meeting any new California requirements.

Question 3*: What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency that such cybersecurity audits, assessments, or evaluations comply with CCPA's cybersecurity audit requirements?*

There are significant benefits for both businesses and consumers if the CPPA accepts cybersecurity audits that businesses conduct to comply with leading cybersecurity laws. As explained above, California should not create its own cybersecurity certification or audit standards. Rather, the CPPA should recognize compliance with existing standards and best practices for cybersecurity risk management as meeting any new California requirements.

[8] *See* ISO 27001, ISO - ISO/IEC 27001 — Information security management,NIST Cybersecurity Framework, *available at* https://www.nist.gov/cyberframework/framework.

We recommend the CPPA allow companies to demonstrate compliance with existing cybersecurity laws and standards in two ways:

- ***First, we recommend the CPPA's regulations set forth the characteristics of cybersecurity frameworks that meet CCPA's requirements and identify specific cybersecurity certification and audit frameworks that meet the requirements imposed by California's regulations***, including ISO 27001, SOC 2 Type 2, and FedRAMP. The regulations should then provide that businesses compliant with ISO 27001, SOC 2 Type 2, or FedRAMP have satisfied the California cybersecurity audit requirement. Companies could demonstrate their compliance with these standards by producing a certification, attestation, or other artifact demonstrating compliance, including certifications or attestations by third parties. This approach enables California to leverage these existing thorough and independent certification programs and allows the CPPA to focus its own resources on organizations that have not obtained such certifications. Referring to existing standards also helps reduce fragmentation of privacy operations and enhances national and global harmonization on strong cybersecurity practices.

- **Second, the CPPA should allow companies to demonstrate that they have satisfied California's cybersecurity audit requirement through artifacts, such as certifications, attestations, and audit assessment reports, that demonstrate use of practices consistent with existing leading security standards and frameworks.** Given the limited pool of existing auditors with sufficient security expertise, as well as the process involved in conducting a thorough audit, establishing new audit regimes is time-consuming and costly, especially for small businesses and technology consumers that may ultimately absorb such costs. We therefore encourage the CPPA to leverage existing leading security standards and frameworks whenever possible, which will ensure companies are compliant with high standards of data security while reducing both the time delays and costs of demonstrating such compliance.

For example, many organizations may already implement strong data protection safeguards using leading security standards and best practices, including the NIST Cybersecurity Framework, ISO 27001, and Service Organization Controls (SOC) 2 Type 2 certifications. The CPPA's regulations should leverage certifications, attestations, and reports that demonstrate compliance with those existing standards and frameworks. For instance, organizations may engage independent third-party assessment programs to obtain an ISO 27001 certification, which demonstrates conformance with ISO 27001 practices, or may obtain a SOC 2 Type 2 certification after an audit of certain controls like those focused on security or confidentiality, or may obtain FedRAMP authorization, which demonstrates conformance with practices consistent with the NIST Cybersecurity Framework (since both the NIST Cybersecurity Framework and FedRAMP baseline map to NIST 800-53, the U.S. Federal baseline for information security). Compliance with these standards and frameworks should satisfy California's cybersecurity audit requirement. The CPPA should therefore recognize that businesses satisfy California's audit obligations by producing artifacts, such as certifications, attestations, and audit assessment reports, that demonstrate the use of practices consistent with leading standards and frameworks.

One of the standards that California should recognize as satisfying any new cybersecurity requirements is an organization's authorization by the FedRAMP program and the StateRAMP program. FedRAMP is the US Government's approach to the adoption and use of cloud services. FedRAMP aims to grow the use of cloud services (which itself creates opportunities to improve cybersecurity) while reducing duplicative efforts to assess an

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

organization's cybersecurity practices. An organization that earns a FedRAMP authorization or meets similar requirements typically completes a readiness assessment and pre-authorization prior to undergoing a full security assessment and authorization process, and finally engages in continuous monitoring. At the state level, California participates in StateRAMP, which is a multi-state organization that provides state and local governments a common method for verifying an organization's cloud security. Achieving FedRAMP or StateRAMP authorization should be more than sufficient to demonstrate that organizations have adopted cybersecurity practices designed to manage cybersecurity risks, in line with any new CPPA requirements.

Finally, thought should be given to the ability of smaller businesses that have yet to receive a certification to use records of a recent audit to demonstrate compliance with an adequate level of security.

Recommendation: The CPPA should recognize that compliance with existing best practices for cybersecurity risk management, including existing audits, attestations, and certifications, meet any new California requirements.

Question 4: *With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent? What else should the agency consider to ensure that cybersecurity audits will be thorough and independent?*

To improve a business's cybersecurity protections, audits and assessments must be robust, and we encourage the CPPA to focus on prioritizing the thoroughness of an audit, which is often distinct from the question of whether an audit is independent. For example, under existing laws a range of different actors may undertake audits or assessments, including both external auditors and audits conducted by internal compliance teams whose role is to assess the company's processes and implement changes across the organization.

The appropriate entity to conduct an audit will vary in different scenarios. For example, businesses may engage third-party auditors to conduct an assessment in a situation where the third party has clear standards to audit against and the business may select an auditor that is certified with a specific accrediting body. SOC audits, for example, are conducted by CPAs and governed by the American Institute of Certified Public Accountants. In contrast, internal audits create an opportunity for continuous monitoring, which can help businesses to identify issues before they become legal, policy, or other business-oriented challenges. Internal audits are also more cost-effective and consequently do not create such high barriers to entry that would have particularly challenging impacts for small businesses.

Recommendation: The CPPA should prioritize robust audits and assessments and recognize that the question of whether an audit is robust is separate from the question of whether it is independent.

Question 5: *What else should the Agency consider to define the scope of cybersecurity audits?*

New regulations are to require businesses whose processing presents a "significant risk" to consumers' security to perform annual cybersecurity audits.

Defining the "significant risk" that triggers this obligation is a key aspect of scoping this obligation. We encourage the CPPA to define processing that presents a "significant risk" to consumers' security in line with, or by reference to, leading cybersecurity laws, policies, and standards. These sources may help the CPPA to flesh out the CCPA's requirement that the definition of "significant risk" consider the "size and complexity of the business and the nature and scope of processing activities."[9] These may include:

- **National Institute of Standards and Technology, Glossary – Definition of High Impact.** NIST has published a glossary of terms that defines "high impact" as a "loss of confidentiality, integrity, or availability [that] could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." Such a loss "might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." This definition builds on guidance in NIST-FIPS 199, which is used in categorizing federal information and information systems.[10]

- **Securities and Exchange Commission, Guidance on Risk Factors for Identifying Cybersecurity Risks.** The SEC has published guidance intended to help companies identify which cybersecurity risks should be disclosed. It contains a non-exhaustive list that can help companies to identify the risks that are significant enough to make investments speculative or risky. The eight criteria identified by the SEC include the probability of the occurrence and potential magnitude of cybersecurity incidents, the adequacy of preventative actions taken by the company to reduce cybersecurity risks, and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks.[11]

Recommendation: The CPPA should define processing that presents a "significant risk" to consumers' security in line with, or by reference to, leading cybersecurity laws, policies, and standards.

II. Privacy Risk Assessments

Under the CCPA, new regulations are to require businesses whose processing of consumers' personal information presents a "significant risk" to consumers' privacy submit to the CPPA "on a regular basis" a risk assessment. The statute identifies information to be included in that assessment and specifies that it does not require businesses to divulge trade secrets.[12]

Privacy risk assessments are an important component of data protection programs. BSA supports requiring businesses to conduct risk assessments for activities that are likely to result in significant privacy risks to consumers. We have therefore supported a range of

[9] Cal. Civil Code 1798.185(15)(A).
[10] NIST – FIPS Pub. 199, Standards for Security Categorization of Federal Information and Information Systems, *available at* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.
[11] Securities and Exchange Commission, 17 CFR Parts 229 and 249 (Feb. 26, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[12] Cal. Civil Code 1798.185(15)(B).

state privacy laws that require businesses to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks that may arise from those activities and to adopt appropriate mitigation measures. As explained below, a range of countries and states *already* require businesses to conduct data privacy assessments under existing laws. We strongly encourage the CPPA to align California's requirements for privacy assessments with the requirements established by leading global and state laws. This approach will help businesses to invest in a strong set of compliance practices that satisfy multiple legal obligations while identifying and mitigating issues across the business's products and services.

***Question 1**: What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?*

For the laws or other requirements identified:

a. *To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?*
b. *What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA's risk-assessments requirements (e.g., product reviews)?*
c. *What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?*
d. *What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?*
e. *Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?*

Privacy and data protection laws worldwide require companies that engage in certain activities to conduct privacy risk assessments. These include:

- **European Union General Data Protection Regulation (GDPR).** The GDPR requires controllers to carry out a data protection impact assessment when processing is "likely to result in a high risk to the rights and freedoms of natural persons."[13]

- **UK General Data Protection Regulation (UK GDPR).** Like the GDPR, the UK GDPR requires controllers to carry out data protection impact assessments for processing that is likely to result in a high risk to individuals. The UK's Information Commissioner's Office has published extensive guidance for companies conducting a data protection impact assessment, including a sample template.[14]

- **Colorado Privacy Act**. Colorado's state privacy law will require controllers to conduct a data protection assessment for processing that presents a "heightened risk of harm to a consumer." It defines that term to include: (1) targeted advertising, (2)

[13] GDPR Article 35.
[14] *See* Information Commissioner's Office, Data Protection Impact Assessments, *available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments.

profiling that presents certain reasonably foreseeable risks; (3) selling personal data, and (4) processing sensitive data.[15]

- **Connecticut Data Privacy Act**. Connecticut will require controllers to conduct data protection assessments for activities that present a "heightened risk of harm to a consumer." It defines that term to include: (1) targeted advertising, (2) sale of personal data, (3) profiling that presents certain reasonably foreseeable risks, and (4) processing of sensitive data.[16]

- **Virginia Consumer Data Protection Act.** Virginia's law requires controllers to conduct data protection assessments for five types of processing: (1) targeted advertising; (2) sale of personal data, (3) profiling that presents certain "reasonably foreseeable risks"; (4) processing of sensitive data, and (5) any processing activities involving personal data that present a heightened risk of harm to consumers.[17]

In many other countries, regulators are either authorized to require companies to conduct privacy risk assessments in certain contexts or have issued guidance encouraging companies to use privacy risk assessments to satisfy other legal obligations. For example:

- **Brazil General Data Protection Law (LGPD).** Controllers may be required to prepare data protection impact assessments, subject to requirements set out in future regulations by the country's National Agency of Data Protection (ANPD).

- **Singapore Personal Data Protection Act (PDPA)**. Singapore's PDPA does not expressly provide for organizations to conduct data protection impact assessments, but the Personal Data Protection Commission has issued detailed guidance explaining how organizations can use data protection impact assessments to ensure their handling of personal data aligns with the law.[18]

- **Australia Privacy Act**. The Office of the Australian Information Commissioner (OAIC) has published a Privacy Impact Assessment Guide intended to help entities subject to the Australia Privacy Act conduct privacy impact assessments.[19] While the statute does not currently require private-sector companies to conduct such assessments, OAIC has recommended entities use privacy impact assessments to satisfy other legal obligations imposed by the Act, including the requirement to take reasonable steps to implement practices, procedures, and systems that will ensure compliance with the Australia Privacy Principles.[20]

---

[15] Colorado Privacy Act Sec. 6-1-1309(1)-(2).
[16] Connecticut Data Privacy Act Sec. 8(a).
[17] Virginia Consumer Data Protection Act, Sec. 59.1-580.A.
[18] *See* Personal Data Protection Commission of Singapore, Guide to Data Protection Impact Assessments, *available at* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.pdf; Personal Data Protection Commission of Singapore, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Revised May 2022), *available at* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.pdf.
[19] Office of the Australian Information Commissioner, Guide to Undertaking Privacy Impact Assessments (Sept. 2, 2021), *available at* https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments.
[20] Under the Australia Privacy Act, only government agencies are required to conduct privacy impact assessments. However, the Australian government is undertaking a comprehensive review of the Privacy Act and the Attorney General has recommended that private-sector organizations be required to

The goals and processes of the data protection assessments requirements listed above largely align with the processes and goals articulated in Cal. Civil Code 1798.185(a)(15)(B). Indeed, under many global and state laws, the content of a data protection impact assessment is very similar to the GDPR's requirements. Under Article 35 of the GDPR, a data protection impact assessment must address four topics:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Companies have designed strong global compliance programs that satisfy obligations to conduct data protection impact assessments across multiple jurisdictions. By focusing their investment and resources in compliance practices that satisfy the obligations in more than one country, a business can develop an interoperable global data protection assessment that is better positioned to identify and address issues across the company's products and services. For example, if a company that serves customers in six countries were required to conduct an entirely separate data privacy assessment for each jurisdiction, it may be forced to repeat the same assessment six separate times (or more) — without a clear benefit to consumer privacy. Rather than forcing companies to expend resources to perform the same assessment multiple times, data protection laws can encourage companies to invest in a strong data privacy assessment practice that can be leveraged across jurisdictions. Conducting an interoperable global assessment ensures that a company has time to address and mitigate issues identified in the assessment, rather than simply re-starting the assessment process.

Recommendation: We strongly recommend that the CPPA allow companies to satisfy their obligation to conduct a risk assessment under California law by using risk assessments conducted for the purpose of complying with another jurisdiction's law or regulations. Specifically, we recommend any regulations clearly state that an assessment shall satisfy California's requirements if it is reasonably similar in scope and effect to the data protection assessment that would otherwise be done pursuant to CCPA.

***Question 3**: To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code 1798.185(a)(15):*

a. What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessments?

b. What other models or factors should the Agency consider? Why? How?

conduct privacy impact assessments prior to undertaking a high privacy risk activity. *See* Attorney-General's Department, Privacy Act Review, Report 2022, Recommendation 13.1, *available at* https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

c. *Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?*
d. *What processing, if any, does not present significant risk to consumers' privacy or security? Why?*

We encourage CPPA to define processing that presents a "significant risk" to consumers' privacy in line with other global and state data protection laws. Although California need not adopt a definition identical to those in other laws, the CPPA can benefit both consumers and businesses by adopting a definition of "significant risk" that aligns with other leading privacy laws. Supporting a consistent approach in identifying the types of data for which risk assessments are appropriate increases shared expectations about how consumers' data will be protected.

We highlight two potential approaches the CPPA could take in identifying processing that presents a "significant risk":

- **First, the CPPA could adopt a definition of "significant risk" modeled on the EU GDPR, by identifying criteria that companies are to use in determining if processing presents a significant risk.**

  The GDPR requires companies to conduct data protection impact assessments when processing is "likely to result in a high risk to the rights and freedoms of natural persons" —an assessment that takes into account the "nature, scope, context, and purposes of the processing." GDPR Article 35.3 also identifies three non-exhaustive circumstances in which assessments are required:

  (1) a systemic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, that produces legal or similarly significant effects on a person;
  (2) large scale processing of special categories of data or data on criminal offenses; or
  (3) large scale systemic monitoring of a publicly accessible area.

  For other activities, companies are to determine if processing is high risk based on guidance endorsed by the European Data Protection Board (EDPB).[21] That guidance identifies nine criteria to consider in determining if processing is likely to result in high risks to the rights and freedoms of a natural person and suggests an assessment is required if two criteria are met. The criteria are:

  (1) the use of evaluation or scoring;
  (2) automated decision-making with legal or similar significant effects;
  (3) systemic monitoring;
  (4) sensitive data or data of a highly personal nature;
  (5) data processing on a large scale;
  (6) matching or combining datasets;
  (7) data concerning vulnerable data subjects;
  (8) innovative use or applying new technological or organizational solutions; or
  (9) when the processing itself prevents data subjects from exercising a right or using a service or contract.

[21] *See* Article 29 Working Party, Guidelines on Data Protection Impact Assessments, endorsed by EDPB on May 25, 2018, *available at* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

To build on these criteria, data protection authorities (DPAs) in EU member states have created whitelists and blacklists of more specific processing activities intended to complement the guidelines.[22]

Benefits of the GDPR approach: This approach prioritizes identifying "high risk" or "significant risk" activities based on the context and substance of the processing. By using flexible criteria rather than a static list, it helps ensure the definition may be applied to new types of technology as they develop.

- **Second, the CPPA could define "significant risk" in line with the Colorado, Connecticut, and Virginia privacy laws, by identifying specific processing activities that present significant risks.**

  The Colorado Privacy Act and Connecticut Data Privacy Act require companies to conduct risk assessments of processing that presents a "heightened risk of harm to a consumer."[23] Those laws define such risks to include:

  1. Targeted advertising;
  2. Sale of personal data;
  3. Profiling that presents certain "reasonably foreseeable" risks; and
  4. Processing sensitive data.

  The Virginia Consumer Data Protection Act similarly requires companies to conduct data protection assessments in four specific scenarios. It also includes a broader catch-all provision.[24] Under the Virginia law, assessments are required for the following activities:

  1. Targeted advertising;
  2. Sale of personal data;
  3. Profiling that presents certain reasonably foreseeable risks;
  4. Processing sensitive data; and
  5. Processing activities involving personal data that present a "heightened risk of harm" to consumers.

Benefits of the Colorado, Connecticut, and Virginia approach: This approach has the benefit of identifying specific scenarios that clearly require risk assessments, which sets clear expectations for consumers and clear implementation guidance for companies.

Recommendation: We strongly encourage CPPA to adopt a definition of "significant risk" that aligns with the approaches embodied in other leading privacy and data protection laws. This will help ensure that companies conducting risk assessments focus their resources on the substance of the assessment and will support a common understanding of the types of processing activities that may present heightened risks to consumers.

---

[22] *See, e.g.*, IAPP, EU Member State DPIA Whitelists, Blacklists and Guidance (last revised December 2019), *available at* https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/ (collecting guidance from DPAs); *see also* Muge Eazlioglu, IAPP Privacy Advisor, What's Subject to a DPIA Under The EDPB?, *available at* https://iapp.org/news/a/whats-subject-to-a-dpia-under-the-gdpr-edpb-on-draft-lists-of-22-supervisory-authorities/ (analyzing the EDPB's opinions on the lists of "high risk" activities by 22 DPAs).

[23] Colorado Privacy Act Sec. 6-1-1309(1)-(2); Connecticut Data Privacy Act Sec. 8(a).

[24] Virginia Consumer Data Protection Act Sec. 59.1-580.A

Question 4: *What minimum content should be required in businesses' risk assessments? In addition:*

a. *What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?*
b. *What, if any, additional content should be included in risk assessments for processing that involves automated decisionmaking, including profiling? Why?*

California's requirements for privacy risk assessments should mirror CCPA's statutory language, which states that a risk assessment is to address the processing of personal information "including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."[25]

As noted above, this statutory language aligns in large part with the requirements of GDPR and of state privacy laws in Virginia, Colorado, and Connecticut.[26]

GDPR Article 35 states:

> The assessment shall contain at least:
> - a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
> - an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
> - an assessment of the risks to the rights and freedoms of data; and
> - the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[27]

Colorado's Privacy Act states:

> Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.[28]

[25] Cal. Civ. Code 1798.185(a)(15)(B).
[26] Virginia Consumer Data Protection Act Sec. 59.1-580.B.
[27] GDPR Article 35.
[28] Colorado Privacy Act Sec. 6-1-1309(3).

Connecticut's Data Privacy Act states:

> Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.[29]

Virginia's CDPA states:

> Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.[30]

Recommendation: The requirements for privacy risk assessments in California should mirror the CCPA's statutory text. That text aligns in large part with leading global data protection laws and state privacy laws.

Question 5: *What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?*

There are significant benefits to both businesses and consumers if the CPPA accepts the submission of risk assessments that were completed in compliance with the GDPR or the Colorado Privacy Act, or other laws with requirements reasonably similar in scope or effect.

In many cases, companies that do business across state and national boundaries have already established processes for conducting and documenting privacy-related risk assessments, including under global privacy laws like the EU's GDPR, Brazil's LGPD, and the obligations imposed by state laws in Colorado, Connecticut, and Virginia. Companies are better positioned to detect and respond to privacy concerns identified through a privacy risk assessment if they invest in a strong and centralized privacy assessment process that can be leveraged for compliance with the range of privacy and data protection laws to which the company's processing activities are subject.

In contrast, if the CPPA adopts regulations that require separate (and overlapping) assessments, it will fragment compliance efforts—a diversion of resources that should

[29] Connecticut Data Privacy Act Sec. 8(b).
[30] Virginia Consumer Data Protection Act Sec. 59.1-580.B.

reflect an intentional choice rather than an unintentional consequence of creating regulations that do not account for existing laws, frameworks, and compliance mechanisms.

Recommendation: We strongly recommend that the CPPA allow businesses to satisfy their obligation to conduct a privacy risk assessment under California law by using risk assessments conducted for the purpose of complying with another jurisdiction's law or regulations. Specifically, we recommend any regulations clearly state that an assessment shall satisfy California's requirements if it is reasonably similar in scope and effect to the data protection assessment that would otherwise be done pursuant to CCPA.

Question 6: *In what format should businesses submit risk assessments to the Agency? In particular:*

a. *If businesses were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business):*
    i. *What should these summaries include?*
    ii. *In what format should they be submitted?*
    iii. *How often should they be submitted?*
b. *How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements (e.g., summaries signed under penalty of perjury)?*

Under the CCPA, new regulations are to require risk assessments be submitted to the CPPA "on a regular basis."

We encourage the CPPA to adopt regulations stating this "regular basis" should be interpreted as meaning the risk assessments be provided to the CPPA upon request. This approach would allow the agency flexibility in requesting assessments from specific organizations and from broader categories of organizations for which the agency seeks to better understand the potential risks of processing. Adopting an alternative approach of specifying that all organizations are to submit risk assessments to the CPPA at a set interval, such as every two years or every five years, would create a potentially enormous quantity of assessments flowing into the CPPA that may not reflect the agency's priorities in identifying and addressing consumer harms. Reviewing those materials may also require such significant resources that it could divert staff away from other important efforts by the agency.

In addition, the regulations should provide that the CPPA will treat risk assessments provided to the agency as confidential and not subject to public disclosure and make clear that the disclosure of those assessments to the agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.[31] This will not only help avoid inadvertent disclosure of proprietary data and business practices that may be reflected in a risk assessment, but will also help ensure strong incentives for companies to undertake rigorous risk assessments.

Recommendation: We encourage the CPPA to define "regular basis" as meaning risk assessments should be provided to the agency upon request.

[31] Other states provide such protection. *See, e.g.*, Colorado Privacy Act Sec. 6-1-1309(4); Connecticut Data Privacy Act Sec. 8(c); Virginia Consumer Data Protection Act Sec. 59.1-576.C.

III. Automated Decision-Making

Under the CCPA, new regulations are to govern "access and opt-out rights with respect to business' use of automated decision-making technology, including profiling." Regulations are also to require that business' response to access requests include "meaningful information about the logic involved" in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.[32]

***Question 1**: What laws requiring access and/or opt-out rights in the context of automated decision-making currently apply to businesses or organizations (individually or as members of specific sectors)?*

Access Rights. In the United States, all five states to enact comprehensive privacy laws create rights for consumers to access personal information. These access rights are not limited to personal information processed in connection with automated decision-making, but apply to a much broader range of processing activities. Like other state privacy laws, the CCPA creates a right for consumers to request certain information from a business that collects personal information about the consumer.

Because the CCPA already gives consumers a broad right of access, the CPPA should not create a separate — and potentially duplicative — access right focused only on access in connection with automated decision-making. Instead, the CPPA should focus any new regulations on addressing how the statute's existing access right applies in the context of automated decision-making.

Opt-Out Rights. In the United States, comprehensive state privacy laws in three states create clear statutory rights for individuals to opt out of certain automated decision-making activities that amount to "profiling." Those states are Colorado, Connecticut, and Virginia.

Colorado's Privacy Act states:

> A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of . . . profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.[33]
>
> Profiling is defined as "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[34]

[32] *See* Cal. Civil Code Sec. 1798.185(16).
[33] *See* Colorado Privacy Act Sec. 6-1-1306(1)(a)(I)(C). "Decisions that product legal or similarly significant effects concerning a consumer" are defined as "a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services." *Id.* at Sec. 6-1-1303(10).
[34] *Id.* at Sec. 6-1-1303(20).

Connecticut's Data Privacy Act states:

> A consumer shall have the right to: . . . opt out of the processing of the personal data for purposes of . . . profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer[35].
>
> Profiling is defined as "any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[36]

Virginia's Consumer Data Protection Act states:

> A controller shall comply with an authenticated consumer request to exercise the right . . . [t]o opt out of the processing of the personal data for purposes of . . . .(i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[37]
>
> Profiling is defined as "any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[38]

Unlike the statutory language in Colorado, Connecticut, and Virginia, the CCPA's text does not clearly call for a stand-alone right to opt out of certain types of automated decision-making. Rather, the statutory text narrowly focuses on the use of automated decision-making in the context of the access and opt-out rights already included in CCPA. The plain language of the statue accordingly calls for regulations that identify how the existing access and opt-out rights operate in the context of businesses using automated decision-making technology, including profiling. This reading of the statute is confirmed by the next part of the CCPA's text, which focuses on how the access right works in this context, by requiring businesses to provide "meaningful information about the logic involved" in such automated decision-making processes and a description of the likely outcome of such processes.

Conversely, adopting a broader reading of the CCPA's language would seem to exceed the statutory text, which does not envision regulations that contain the type of automated decision-making rights found in GDPR or the rights to opt out of certain types of profiling found in the Colorado, Connecticut, and Virginia state privacy laws.[39] While we appreciate the

---

[35] Connecticut Data Privacy Act Sec. 4(a)(5)(C).
[36] *Id.* Sec. 1(22). "Decisions that produce legal or similarly significant effects concerning the consumer" are defined as "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services." *Id.* at Sec. 1(12).
[37] Virginia Consumer Data Protection Act Sec. 59.1-577.A.5(iii).
[38] *Id.* at Sec. 59.1-575. "Decisions that produce legal or similarly significant effects concerning a consumer" are further defined as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."
[39] *See, e.g.*, GDPR Article 22 (stating that data subjects have a right "not to be subject to a decision based solely on automated processing . . . which produces legal effects concerning him or her or

role that a strong data privacy law can play in ensuring that automated decision-making technology is used in responsible ways, and we believe focusing on these issues is needed as the underlying technology continues to be developed, the upcoming regulations do not appear to be the forum best suited to addressing these issues, given their narrow scope.

Recommendation: New regulations should focus on how existing access and opt-out rights created by the CCPA apply in the context of automated decision-making technology, in line with the statute's narrow text.

Question 3: *With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:*

a. *How is "automated decision-making technology" defined? Should the Agency adopt any of these definitions? Why, or why not? 7 Civ. Code § 1798.185(a)(16).*
b. *To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?*
c. *What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decision-making technology requirements?*
d. *What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decision-making? What is the impact of these gaps or weaknesses on consumers?*
e. *What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decision-making? What is the impact of these gaps or weaknesses on consumers?*
f. *Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, how?*

If the CPPA creates a new right to opt out of profiling, we strongly recommend that right be defined in line with the rights already established in Colorado, Connecticut, and Virginia's privacy laws. These laws share important similarities, including:

- *Creating a right to opt-out of profiling for decisions with "legal or similarly significant effects."* Focusing a right to opt out of profiling on a core set of decisions about individuals is critical to ensure any right is not so broad or vague that it would be impractical to implement in practice. As noted earlier, the three existing state laws that create rights to opt out of profiling activities apply to decisions with "legal or similarly significant effects" and define that term in similar ways. For example, Connecticut's law defines such effects to mean "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services."[40] Virginia and Colorado define the term similarly.[41]

similarly significantly affects him or her"); Virginia Consumer Data Protection Act Sec. 59.1-573 (creating a right to opt out of profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"); Colorado Privacy Act Sec. 6-1-1306(a)(I)(C) (granting same right to opt out of profiling as Virginia law).

[40] Connecticut Data Privacy Act Sec. 1(12).

[41] Virginia Consumer Data Protection Act Sec. 59.1-575; Colorado Privacy Act Sec. 6-1-1303(10).

- *Creating a right that applies to final decisions*. As Colorado, Connecticut, and Virginia's state privacy laws recognize, a right to opt out of certain profiling activities should apply to final decisions made by a company. For example, Connecticut's right to opt out of profiling applies to certain "*decisions made by the controller* that *result in the provision or denial* by the controller," of certain services or opportunities.[42] Virginia and Colorado's laws similarly focus on final decisions.

Because the Colorado, Connecticut, and Virginia privacy laws all create a clear statutory right to opt out of profiling, companies have already designed and implemented processes for responding to requests to opt out of profiling covered by those laws.

As noted above, the CCPA's plain text does not appear to contemplate the creation of a stand-alone right to opt out of profiling. However, if the CPPA does create a right to opt out of profiling under California law, aligning that right with the existing rights created by other state laws would allow California consumers to use the processes that businesses have already established to comply with this new right. To the extent California creates a right to opt out of profiling that does not align with those created in other states, companies may be required to create a separate process for complying with California requests. In practice, the more separate processes a company must establish to comply with similar types of consumer requests, the more difficult it becomes to maintain and improve those processes. Different but overlapping processes that vary among states are also likely to increase confusion for consumers. Companies that can establish a single process to comply with rights to opt out of profiling are better positioned to update that process across products and services based on practical experience and consumer feedback, leading to better outcomes for consumers.

Recommendation: If the CPPA creates a new right to opt out of profiling under California law, it is important to align that right with existing rights created by other state laws so that California consumers can use established and centralized processes to exercise their right. Any right should: (1) apply to decisions that produce "legal or similarly significant effects," and (2) apply only to final decisions, in line with other state privacy laws.

Question 9: *What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decision-making processes and the description of the likely outcome of the process with respect to the consumer? In addition:*

a. What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?

b. How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?

The CPPA contemplates that new regulations will require businesses responding to access requests to provide "meaningful information about the logic involved" in automated decision-making processes, as well as "a description of the likely outcome of the process with respect to the consumer."[43] This language mirrors the GDPR, which creates a right for individuals to access certain information when their personal data is processed for profiling, including "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[44]

[42] Connecticut Data Privacy Act Sec. 1(12) (emphasis added).
[43] *Id.*
[44] *See* GDPR Article 15(1)(h).

European regulators applying this standard have emphasized the need for "simple" explanations that do not confuse consumers. We encourage the CPPA to apply the CCPA's requirement in a similar manner, by focusing on providing simple and understandable information to consumers. In addition, we encourage the CPPA to ensure any new regulations on access requests do not jeopardize trade secret protections.

European Data Protection Board (EDPB). Guidance endorsed by the EDPB addresses how controllers can provide meaningful information about automated decision-making processes, emphasizing the need for individuals to understand the information provided.[45] That guidance states:

> The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision.

UK Information Commissioner. Similarly, the UK ICO has focused on applying this standard to require controllers to provide information that does not confuse a consumer.[46] The ICO's guidance states:

> Providing 'meaningful information about the logic' and 'the significance and envisaged consequences' of a process doesn't mean you have to confuse people with over-complex explanations of algorithms. You should focus on describing:
> - the type of information you collect or use in creating the profile or making the automated decision;
> - why this information is relevant; and
> - what the likely impact is going to be/how it's likely to affect them.

Recommendation: The CCPA's requirement to provide "meaningful information" about automated decision-making systems should be applied in a practical manner, to focus on providing simple and understandable information to consumers. In addition, any new regulations on access requests should not jeopardize trade secret protections.

Question 10: *To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?*

As with other rights created in the CCPA, it is important that any new regulations continue to recognize that consumers are to exercise access and opt-out rights by going directly to a business, rather than to its service providers.

---

[45] *See* Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Oct. 3, 2017, revised Feb. 6, 2018), endorsed by European Data Protection Board (EPDB) on May 25, 2018, *available at* https://ec.europa.eu/newsroom/article29/items/612053/en.

[46] UK Information Commissioner Office, What Else Do We Need to Consider if Article 22 Applies, *available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/.

Although the CCPA primarily focuses on businesses, which "determine[] the purposes and means of the processing of consumers' personal information,"[47] the statute also recognizes that businesses may engage service providers to "process[] personal information on behalf of a business."[48] Service providers must enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business. In this way, the CCPA ensures that personal information is subject to statutory protections both when a business collects and processes a consumer's personal information itself, and when that business hires service providers to process a consumer's personal information on its behalf. The statute also recognizes the distinct roles of businesses and service providers by assigning them different obligations based on their different roles in handling consumers' personal information.

Under the CCPA, businesses are assigned the responsibility of responding to consumers' requests to access, correct, and delete their personal information. This is consistent with all other state consumer privacy laws and leading data protection laws worldwide, which place this obligation on companies that decide how and why to collect consumers' data — rather than the service providers acting on behalf of such companies. If the CPPA creates a new right to opt out of profiling via regulations, that right should similarly be exercised by the consumer going directly to the business.

Recommendation: As the CCPA contemplates new regulations addressing access and opt-out rights, it should ensure those rights continue to reflect the statute's recognition of the distinct roles of businesses and service providers.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the CPPA on these important issues.

—

For further information, please contact:
Kate Goodloe, Managing Director, Policy
[redacted]

[47] Cal. Civ. Code 1798.140(d)(1).
[48] Cal. Civ. Code 1798.140(ag)(1).

From: Blake Edwards [redacted]
Sent: Monday, March 27, 2023 10:44 AM
To: Regulations
Cc: Howard Fienberg; Stuart Pardau
Subject: PR 02-2023
Attachments: Insights -- Comments for CPPA. 3.27.23.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Mr. Sabo

On behalf of the Insights Association, please see attached.

--

Blake M. Edwards
Law Offices of Stuart L. Pardau & Associates
11620 Wilshire Blvd Suite #850
Los Angeles, CA 90025
p: [redacted]
e: [redacted]

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd
Sacramento, CA 95834
regulations@cppa.ca.gov

March 27, 2023

Re: PR 02-2023

Mr. Sabo:

The Insights Association ("Insights") submits the following comments on proposed rulemaking related to cybersecurity audits, risk assessments, and automated decision making, per the invitation of the California Privacy Protection Agency (the "Agency").

Representing more than 900 individuals and companies in California and more than 7,200 across the United States, Insights is the leading nonprofit trade association for the market research[1] and data analytics industry. We are the world's leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

The California Privacy Rights Act ("CPRA") is going to have a profound impact on the business community, including the market research and data analytics industry. Small and medium-sized research firms in particular will face tremendous costs in updating and expanding on their already-extensive compliance efforts in connection with the California Consumer Privacy Act of 2018 ("CCPA"). Accordingly, and on behalf of our members, we commend your decision to seek input and are grateful for the opportunity to comment.

1. In determining what processing presents a "significant risk" to consumers' privacy or security, use a clearer, more concise approach than the European Data Protection Board's Guidelines on Data Protection Impact Assessment (the "Guidelines").

On page 5 of the Agency's invitation for comments, the Agency asks about the benefits and drawbacks of following the Guidelines.

[1] Market research, as defined in model federal privacy legislation from Privacy for America, is "the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (ii) used to advertise or market to any particular individual or device." See Part I, Section 1, R: https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/

The Guidelines include nine different criteria for determining what processing operations are "likely to result in a high risk"; namely, (1) evaluation or scoring, (2) automated decision-making, (3) systematic monitoring, (4) sensitive data, (5) data processed on a large scale, (6) matching or combining datasets, (7) data concerning vulnerable data subjects, (8) innovative use or new technological or organizational solutions, and (9) when the processing itself prevents data subjects from exercising a right or using a service or contract.

We respectfully suggest that the Agency's adoption of a similar approach entailing the application of so many different factors will result in an overly nebulous and at any rate unhelpful analysis that will create more problems than it solves.

The Guidelines stipulate that "[i]n most cases, a data controller can consider that a processing meeting two criteria would require a data protection impact assessment (DPIA) to be carried out," and that "[i]n some cases," a single criteria will be sufficient. It is not clear, however, how much weight should be given to each criteria, or whether there are any meaningful thresholds for individual criteria. Is the processing of a hundred records of sensitive data enough to qualify under criteria #4? A thousand? Ten thousand? How many data sets have to be matched or combined to trigger criteria #6? How much data concerning vulnerable data subjects is sufficient under criteria #7? These are the types of questions the Guidelines do not answer.

While the Guidelines do include some "examples of processing" purporting to illustrate the application of possible relevant criteria, these examples do not make the analysis any clearer. Accordingly, we strongly urge the Agency to implement clearer, more concise standards for what constitutes "significant risk" so that businesses have more meaningful guidance about whether they are subject to the cybersecurity audit and risk assessment requirements.

2. Limit the cybersecurity audit and risk assessment requirements to firms that meet one of the first two prongs of the CCPA's "business" definition.

On pages 4 and 8 of the Agency's invitation for comments, the Agency asks "What else should the Agency consider to define the scope of cybersecurity audits?" and "What else should the Agency consider in drafting its regulations for risk assessments?"

As the Agency is aware, there are three different ways for an organization to be defined as a "business" under CCPA: (1) annual gross revenues in excess of $25 million; (2) buying, selling, or sharing the personal information of at least 100,000 consumers or households; or (3) deriving 50 percent or more of its annual revenues from selling or sharing personal information.

Because the third prong is not tied in any way to business size or processing volume, it includes a substantial number of small and medium-sized firms in the market research and data analytics industry. Firms like this who are subject to CCPA solely on the basis of this third prong should be exempt from costly cybersecurity audits and risk assessments.

To comply with these requirements, small businesses will likely have to hire outside expertise and expend considerable expense relative to the size of their enterprise. Because the cybersecurity audits and risk assessments are already premised on processing that presents a "significant risk" to consumers' privacy or security, we believe limiting these requirements as we propose would allow the Agency to balance the interests of small businesses without hampering the opt-out right of California consumers.

Alternatively, the Agency could limit the cybersecurity audit and risk assessment requirements based on smaller limits than those in the CCPA's "business" definition (e.g., firms that do $15 million in revenue

or deal with at least 50,000 records), to protect the smallest businesses from overly onerous regulatory requirements.

3. Limit processing which presents a "significant risk" to processing which occurs on a regular basis or a minimum number of times per year

In addition to limiting "significant risk" scenarios as described above, the Agency could also clarify that such processing must occur on a regular basis, or at least with some minimal frequency, to trigger the auditing and risk assessment requirements. It does not meaningfully further the spirit of the CCPA, and imposes particularly unnecessary burdens on small businesses, to require an audit and security assessment solely on the basis of one, two, or a handful of isolated instances of processing deemed to present a "significant risk" in a given year.

4. Limit processing which presents a "significant risk" to processing of at least 100,000 records

Alternatively, we suggest the Agency could incorporate some numerical trigger into what constitutes "significant risk" processing. For example, this number could track the figure in the CCPA's "business" definition of 100,000 records, or the Agency could select some lower number. In any case, the underlying statutory language of the CCPA counsels in favor of some such numerical limit. The statute contemplates "significant risk to consumers' privacy or security," language which connotes larger concerns of aggregate risk, not every isolated presentation of risk to any individual consumer or small group of consumers.

Conclusion

We hope the above comments will be useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

Again, we appreciate the opportunity to comment.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association

From: Shanahan, Richard [redacted]
Sent: Monday, March 27, 2023 11:00 AM
To: Regulations
Cc: 嶋田恵一 / SHIMADA, KEIICHI; Tolentino, Melissa; Abdessamad, Hicham
Subject: PR 02-2023 Hitachi Comments
Attachments: 03272023_CCPA Comments.pdf

Dear Chair Urban,

Please find attached comments submitted by Hitachi Group companies doing business here in the U.S. on proposed rulemaking on cybersecurity audits, risk assessments and automated decision making.

We look forward to continuing the collaboration with the Board on these issues.

Best regards,

Richard Shanahan
Director | Government & External Relations
Hitachi, Ltd. | Washington, DC Corporate Office
t. [redacted] | m. [redacted]
[redacted]

HITACHI
Inspire the Next

March 27, 2023

The Honorable Jennifer Urban, Chair
California Privacy Protection Agency Board
2101 Arena Blvd.
Sacramento, CA 95834

RE: *INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING*

Dear Chair Urban:

The following comments are submitted by Hitachi Group companies ("Hitachi") doing business in the United States in connection with the *Invitation for preliminary comments on proposed rulemaking cybersecurity audits, risk assessments, and automated decision making*.

Background on Hitachi

Founded in 1910 and headquartered in Tokyo, Japan, Hitachi, Ltd. is a global technology corporation answering society's most pressing challenges through cutting-edge operational technology (OT), information technology (IT), and products/systems. A Social Innovation leader, Hitachi delivers advanced technology solutions in the mobility, human life, industry, energy, and IT sectors. The company's consolidated revenues for FY2021 (ended March 31, 2022) totaled $84.13 billion and 853 companies employ over 368,000 employees worldwide.

Since establishing a regional subsidiary in the United States in 1959, Hitachi has been a committed American partner. For over thirty years, it has invested heavily in research and development (R&D) in the U.S., and this continued reinvestment has resulted in 19 major R&D centers that support high-skilled jobs in manufacturing and technology. Dedicated to delivering the technologies of tomorrow, Hitachi opened a Center for Innovation in Santa Clara, California to explore applications in machine learning, artificial intelligence, Internet of Things (IoT) devices, data analytics, and autonomous vehicles among other advanced technologies. Hitachi is also proud of its human capital investment with more than 25,000 employees across 81 companies in the U.S. At 15% of total revenue, North America is Hitachi, Ltd.'s second largest market, following only the Japanese market, with $12.7 billion in revenue in FY2021.

Hitachi continues to appreciate the opportunity to engage with the Board and for the ability to offer comments and reactions proposals. Regulations need to be fair, equitable, and protect the public while also fostering innovation in the State of California and across the country. We would also encourage CPPAB to adopt a position that data is a property right that people own and thus can make decisions on the use of that data. This position aligns with proposals on U.S. consumer privacy and the FTC deceptive practices regulations.

We do note that the six-week timeline for submitting comments is very short for the vast amount of information requested. We strongly urge the Board to take a methodical and meaningful approach to rulemaking, offering many more opportunities for us to respond to requests and longer time frames so we can adequately provide the Board with information as you consider the balanced approach needed in this sphere. Rushing into rulemaking could potentially hurt California's reputation as a innovation hub and we would ask you consider extending this current request to allow for more comments.

Responses to Questions

Audits for Cybersecurity

Many businesses are already conducting their own cybersecurity audits. For compliance purposes, companies have cybersecurity audit process in place if they are under CCPA. These are best practices to ensure our customers are being protected and our own systems are not being attacked and they align with ISO and NIST practices. NIST created their Cybersecurity Framework, and have provided updates to this Framework, and it is an appropriate vehicle for companies of all sizes to utilize as they are constructing their own cybersecurity defenses. All of the following reports should be considered as attestation for CPPAB for internal cybersecurity audit: internal audits aligned to cybersecurity best practices, contractual requirements, or CPPAB requirements; PCI compliance audits; SOC 2 Type II reports focused on COSO, FFIEC reports; GDPR attestation reports; ISO27001 reports and/or internal IT security audits reports, CPPAB would be wise to direct businesses to the resource instead of creating new regulations.

Cybersecurity audit requirements now are usually part of a contractual relationship with the customer and not regulatory. Hitachi would be concerned about requirements for 3rd parties to conduct audits that do not align with what we have previously agreed to with our customers. While some companies may choose to pursue that, it could be a major financial burden for small companies and take resources away from their innovation strategy. Any reporting requirements to CPPAB should be minimal to avoid potential breaches which could hurt competition between companies. Those requirements should also be very clearly defined on data required to fulfill reporting requirements and the audits to be performed. Those definitions would do well to help companies, especially companies with multiple corporate entities, understand the scope to create a compliance program more successfully around data governance. A best practice for data security is to only collect the essential data needed, and CPPAB would be wise to follow this best practice in their own data collection activities. In other industry, reporting requirements are only applicable for specific investigations and that would be a good practice for CPPAB to adopt as well.

When the cloud is involved, most companies work with their cloud providers to share the risk of the platform. Those providers have their own examination processes to assure baseline infrastructure security requirements. Companies establish processes and procedures to review those reports when it comes to critical assets that may contain sensitive information. When gaps a rise, once source of issues is lack of clarity from the regulation or the law as to the requirements or poor communication on what is actually needed or desired. Information delivered in clear, concise, and transparent methods help demonstrate opportunities for companies to improve upon their current cybersecurity protections.

It is Hitachi's recommendation that CPPAB consider different levels of cybersecurity audits dependent upon the size of the company, its territorial scope, and the amount of PII records they are dealing with. The Graham-Leach-Bliley law provides companies an avenue to create baseline levels and then improve their security processes annually. That is a positive method to help each company improve and create an optimal security process.

Risk Assessments

Risk assessments should be no more burdensome than those under the GDPR or the Quebec Privacy Law. A single format is the least burdensome approach, particularly since companies have to comply with risk assessments across multiple regulations for the same set of data. Companies can demonstrate accuracy of the information by having the reports endorsed by a chief privacy officer, chief information security officer, or someone experienced in data privacy. The CCPA doesn't currently have a DPO requirement, but that would be far easier to comply with that than having the assessments signed under penalty of perjury.

A company with an effective risk program in place should have a data classification process, BIA and a continuous risk assessment process as part of the protection for critical assets with sensitive data (PII,

business sensitive data). Taking that into consideration, internal IT audit processes should be key to identify gaps of controls and identify security maturity rating of the company, where levels of risks (appetite and tolerance of risk) are also identified and communicated to the senior management.

Companies with a risk management program should have a risk assessment methodology for calculation of levels of risks. This is part of the NIST AI Risk Management Framework recently published. In terms of the calculation of the current risk (risk after controls are applied), the audit IT process will add assurance input to handle with the identification of how much the inherent risk is being mitigated after current company controls have been applied. Any required risk management program should enhance the positive impact for the security of consumer PII and not create a situation where excessive data collection is necessary to comply with the risk management reporting requirements. A company should be encouraged and supported in their efforts to follow best practices for the size of the company, their exposure to PII, and their territorial reach. Hitachi recommends CPPAB consider COSO Enterprise Risk Management Framework and ASIS Security Risk Management Framework, where prioritization of risks and accountability of asset is the main driver. Companies should prioritize risk regarding critical assets with sensitive information (PII, Financial, business sensitive, pre-release products, etc).

The harms to individuals or communicates are various, and contingent upon individual circumstances, when individuals are submitting very sensitive data in a 3rd party environment. For example, multiple financial risks are associated when a SSN is stored without the proper security. Impersonation is one of the most popular threat vectors that attackers use to gain benefits, and the more sensitive the data is, the more the damage that the attackers can bring to individuals and communities.

The EU-US Privacy Shield agreement should be taken into consideration as CPPAB considers risk. In the U.S., HIPAA, GLBA, and FISMA are examples of laws that should be considered to set the scope of who and how companies will be required to demonstrate compliance. Cybersecurity audits and risk assessment processes are different: cybersecurity audit processes are related to assurance of controls and controls gap analysis while risk assessment process are business artifacts that enable the business to take well-informed risk based strategic business decisions. These are totally a different activities and the audit process is one of the many inputs that risk management considers to calculate risks. Audit processes should have a model of different levels of control effectiveness and security control maturity.

Drawbacks when considering GDPR or the Colorado Privacy Law are related to the different scopes and market of the companies in California. Companies would use internal audit processes and their risk management assessment tools to demonstrate CCPA compliance. Those internal audit processes that use security controls protect assets, are tested regularly, and gaps are communicated to help improve the risk calculation and response. If required to submit reports to CPPAB, an annual or biannual process is encouraged. The summaries could include PCI compliance process, and a CCPA risk assessment report, taking as a risk scenario the risk of PII leaked. The report should explain the methodology of the assessment that has been used, the framework or best practices that the company has decided to follow, the status of open items, treatment decision and remediation plan. PDA or legal attestation signed by senior management, for accountability, communication and acknowledge of compliance risks and information security risks could be part of the reporting.

Automated Decision Making

Automated decision-making systems are still in the early development phase. Because of the continuing development of the systems, it is not easy to point to one definition for CPPAB to adopt that would provide clarity to the regulations that might be adopted. It is more advisable for CPPAB to be more deliberative before jumping to adoption of any definition and allow the industry and associated standards setting bodies the ability to coalesce around clear definitions. NIST recently released its *AI Risk*

Management Framework, and the OECD is working on definitions for terminology and many areas. There are others working on standards in the artificial intelligence areas, all important to help companies of all sizes apply the most logical risk management assessments to their potential AI products. CPPAB should avoid getting ahead of those bodies and stifling innovative research within California. Standards allow flexibility in a rapidly changing environment whereas regulations can be rigid, failing to adapt fast enough to potential vulnerabilities that risk management standards could.

Regulations pose a financial burden on companies, especially those small and medium-sized ventures that are the core of innovative research into ADM systems. If companies have a complex regulatory environment that they have to first navigate that produces unclear definitions, or require unnecessary steps due to inaccurate information or requirements, it pushes the innovation environment away from the state and hurts California's overall research climate. Instead, the voluntary and scalable NIST Frameworks can offer a method to protect consumer data in a way that reflects the potential risk associated with the ADM in development. A risk-based, flexible, regulatory environment will be much more productive for CPPAB to adopt rather than an overly prescriptive and sweeping rules.

Before rushing to create regulations or new laws, CPPAB should consider the many other bodies who already have regulations that would cover automated decision making. The Food & Drug Administration is working on rules about software in medical devices; the Equal Employment Opportunity Commission has issued guidance for ADA compliance in hiring processes; the Federal Trade Commission has existing laws applicable to credit reporting and extension of credit; Consumer Financial Protection Bureau has guidance for financial and credit institutions as does the Federal Reserve, FDIC, and OCC; and Department of Transportation has issued and updated their own guidance for autonomous vehicles. CPPAB should either yield to those bodies and others who are creating these guidelines and standards, or should point to and recognize those guidance documents instead of creating competing regulations. Anyone following these or the NIST AI Risk Management Framework should be provided safe harbor protections.

Conclusion

Hitachi lauds the Board's efforts and looks forward to continuing to work with the State of California as CCPA continues to evolve.

Sincerely,

[redacted]

Hicham Abdessamad
CEO & Chairman
Hitachi America, Ltd.

From:	Shaan Rizvi [redacted]
Sent:	Monday, March 27, 2023 11:25 AM
To:	Regulations
Subject:	PR 02-2023; Comments on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.
Attachments:	Comments on CPPA Invitation re Automated Decision Making 03.27.23 - Final .pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Dear CPPA:

Attached please find comments filed by the American Staffing Association, a national trade association, regarding PR 02-2023 – Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.

Please let me know if you have any questions or comments.

Shaan A. Rizvi, Esq.
Associate General Counsel
American Staffing Association
277 S. Washington St., Suite 200
Alexandria, VA 22314-3675
Office: [redacted]
[redacted]

American Staffing Association
277 South Washington Street, Suite 200 ▪ Alexandria, VA 22314-3675

703.253.2020
703.253.2053 fax
asa@americanstaffing.net
americanstaffing.net

VIA ELECTRONIC SUBMISSION TO
regulations@cppa.ca.gov

March 27, 2023

California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Re: PR-02-2023; Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decision making

The American Staffing Association (ASA) is a national trade association comprised of over 1,700 member staffing agencies that recruit, screen, and hire employees and place them on temporary and contract assignments with clients on an as-needed basis. Staffing is one of America's largest service industries, employing more than 15 million temporary and contract employees annually. Staffing agencies play a vital role in the U.S. economy by providing employment flexibility for workers and just-in-time labor for businesses. They provide workers with jobs, training, choice of assignments and work, flexibility, and a bridge to permanent employment for those who are just starting out, changing jobs, or out of work. Temporary and contract employees work in virtually every job category, including industrial labor, office support, health care, engineering, science, and information technology.

ASA appreciates the opportunity to respond to the Agency's invitation for preliminary comments on proposed rulemaking under the California Consumer Privacy Act of 2018 (CCPA) regarding cybersecurity audits, risk assessments, and automated decision making. Our comments focus solely on Part III relating to automated decision making.

ASA fully supports the broad policy goal of ensuring that algorithmic decision-making tools comport with existing anti-discrimination law. However, it is critical that rules relating to such tools consider the operational needs of employers. Failure to do so will result in overly broad, unworkable regulations that will impede legitimate business operations and do little to protect against the potential harms of AI decision-making tools.

The first part of this submission addresses Question 8 of Part III regarding whether access and opt-out rights with respect to businesses' use of automated decision-making technology should depend on certain factors like the industry that uses the technology. The second part does not address questions posed in the invitation; rather, it is a summary of concerns ASA has raised regarding certain state and local legislative proposals governing employer-use of automated decision-making tools. We believe that awareness of the unique concerns of the staffing industry would be helpful in the event the CPPA considers broader rule-making initiatives relating to automated decision making.

1. Access and opt-out rights regarding businesses' use of automated decision making should vary based on factors including the industries using the technology

We understand "access and opt-out rights" to mean the ability of individual job applicants to gain access to information relating to an employer's use of automated decision-making technology and to opt-out from having such technology applied to them. Question 8 of Part III asks whether those rights should vary depending upon factors such as the industry using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective.

ASA urges the CPPA to consider the disparate nature of various industries when promulgating rules involving access and opt-out rights. In the employment context, opt-out rights would theoretically allow job

applicants to opt-out of being evaluated by any automated decision-making tool. Instead, such applicants would have the right to have their applications segregated and individually evaluated by a human being. While well-intended, such alternative processes would be untenable for the staffing industry for several reasons.

First, among the various methods used to hire and place qualified candidates at client job sites, staffing firms rely on "job boards" such as Monster, LinkedIn, and Indeed to find qualified candidates on their behalf. Staffing firms post job descriptions to job boards; job boards then use their own proprietary AI software to recommend "top matching" resumes back to the staffing firms. Recommended candidates are often displayed in a ranked fashion, sometimes with a numerical score. Because these candidates come to staffing firms through third parties – in this case, job boards – it would be impossible for staffing firms to provide opt-out rights to such candidates. Once a staffing firm receives resumes of qualified candidates from a job board, it is too late to offer an "opt out" option to interested candidates; the automated decision-making tool used by the job board has already screened and selected the qualified candidates prior to their referral to the staffing firm. Such opt-out rights could only be meaningfully offered by the job boards themselves, *prior* to the job boards' evaluation and recommendation of certain candidates to staffing firms. Accordingly, any regulations should ensure that staffing firms are not responsible for providing opt-out rights for candidates referred to them by third party platforms.

Second, opt-out rights are problematic for the staffing industry because of the sheer quantity of employees the industry places on temporary assignments on an annual basis. Some of the largest staffing firms place approximately half a million distinct individuals in various temporary jobs within a calendar year. Further, such firms maintain a repository of millions of candidate resumes from prior job placements. Accordingly, when a new temporary job becomes available, staffing firms often use third-party applicant tracking software (ATS) – a type of automated decision-making tool – to scour their own internal database of previously placed candidates to determine if any are qualified for the new job; the firms then contact qualified candidates to gauge their interest and availability in the new job. In such situations, to offer interested job candidates an "opt-out" right would effectively create two separate but parallel evaluation processes; one for candidates willing to be evaluated by a firm's ATS and a second, smaller, group of opt-out candidates who insist on human evaluation. To ensure that all candidates are fairly compared, a human being would have to manually compare opt-out candidates with all ATS candidates, and then select the most qualified candidates from both groups for any given position. The practical consequence would be to completely negate the efficiency and value of using ATS, since in the end, a human being would have to manually evaluate every resume – even those from the vast majority of applicants who consented to evaluation by the ATS.

Third, opt-out rights for job applicants are problematic because of the *speed* with which the staffing firms often must place candidates at client job sites. Some staffing firm candidates may be offered an assignment starting the same day a position becomes available. For example, a staffing firm may use AI to search its internal database of candidates to fill a substitute teacher position the same day.[1] As noted above, to allow candidates to opt-out of evaluation by a firm's AI software would in effect create a separate process whereby such candidates must be evaluated manually. And again, fairness necessitates that such candidates be manually compared to those who chose *not* to opt-out. The laboriousness of such a comparison, if done manually, would almost certainly ensure that temporary jobs will no longer be available by the time the process is complete, frustrating staffing firms, their clients, and job-seekers alike.

Accordingly, ASA recommends that any rulemaking with respect to employers' use of automated decision-making technology give due consideration to the volume of an employer's job placements as well as the speed at which it often must place qualified applicants as exemplified by the temporary staffing industry.

[1] According to a 2019 ASA Operations Benchmarking Survey of staffing firms across various industries, staffing agencies typically fill temporary and contract staffing orders within one week, with a median fill time of seven days.

2. Staffing firms have unique concerns with proposed state and city regulation of automated decision making

a. Staffing Firms Should be Allowed to Notify Job Applicants of their Use of AI by Postings on Their Websites and Should Not Be Subject to Prescribed Waiting Periods

In response to certain state and city legislative proposals requiring notice to job applicants that AI software has been or will be used in connection with their job applications, ASA has urged that because of staffing firms need to fill jobs quickly, they should be allowed to provide such notice on their websites. Further, because of the time-sensitive demands of the staffing industry, advance notice requirements should not impose minimum waiting periods prior to a staffing agency's use of AI.

Regarding advance notice, as noted above, some staffing firm candidates may be offered an assignment starting the same day or within a couple of days of a position becoming available. In such cases, it would be impossible for staffing agencies to provide advance notice before filling the assignment; indeed, the jobs would be gone before the notice period expires. A far better approach would be to allow an employer to post a permanent notice available on its website, something allowed under New York City's proposed AI rules. Such notice would inform candidates of the use of AI without impeding time-sensitive job placements.

Regarding ex post facto notice, some proposals, such as Washington D.C.'s proposed AI legislation, would require employers to contact candidates for employment not selected by AI software *after the fact* and disclose the factors resulting in the non-selection. In addition to the burdens created by advance notice, ex post facto notices entail another complication: in many cases, staffing agencies are unaware of the particular candidates excluded by AI.

As noted above, staffing firms post job openings on job boards which then use their own proprietary AI software to recommend "top matching" resumes back to the staffing agencies. Staffing agencies cannot know who was excluded during this process because they have no access to such software; nor do they have access to the AI vendor's proprietary information that would disclose the factors resulting in the non-selection. Similarly, a staffing agency may purchase and utilize an ATS to scour job boards and other internet sites and suggest certain candidates while excluding others. Again, a staffing agency has no access to the proprietary analyses performed by the ATS. In such cases, it would be impossible for staffing agencies to provide any meaningful or detailed information about the logic involved or factors considered with regard to the ATS' consideration of an applicant's credentials.

b. Audits for AI Bias Should be Conducted by the AI Vendor or a Neutral Third Party, Not End Users

Certain recent legislative proposals maintain that AI software in the employment context must be tested for inherent bias on a regular basis. Proposed AI legislation in New Jersey, for instance, requires that AI software sold to various companies in the state be subject to a bias audit in the past year and that the software include, at no additional cost, an annual bias audit service that provides the results of the audit to the purchaser. ASA recognizes the importance of minimizing potential algorithmic bias, and such regular bias audits should be conducted by AI vendors themselves or neutral third parties, not end-users of AI software such as employers.

Audit responsibility should not fall on employers because they do not have access to the software vendor's proprietary information, including the various models it used in its algorithmic analysis. Even if an employer could access such information, it would be unnecessarily duplicative and financially wasteful to require hundreds of thousands of employers to conduct audits of the same third-party AI vendors. This is particularly true with respect to the thousands of staffing agencies that use the same AI vendors. Amplifying the problem of duplication and multiple audits is the fact that staffing agencies and other businesses often use multiple job boards which use their own AI in selecting candidates. Again, employers using those services have no access to the platform's algorithmic analyses, nor in some cases to the candidates screened, recommended, or rejected, thus making a meaningful bias audit impossible.

ASA appreciates the CPPA's consideration of the foregoing, and looks forward to working with the agency to address these important issues in a constructive way.

Contact:

Stephen C. Dwyer
Senior Vice President, Chief Legal and Operating Officer
American Staffing Association
[redacted]

From: Alvaro Marañon [redacted]
Sent: Monday, March 27, 2023 11:48 AM
To: Regulations
Subject: RE: PR 02-2023
Attachments: CCIA Comments to CPPA Invitation on Cyber ADS Risk .pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Hello,

Attached are the Computer & Communications Industry Association ("CCIA") comments regarding the Invitation for Preliminary Comments on Proposed Rulemaking that will implement the CPRA.

Thank you,
--

Alvaro Marañon
Policy Counsel
[redacted]
o: (202) 783-0070
@Alvaro_In_Tech
Computer & Communications Industry Association Open Markets. Open Systems. Open Networks.
ccianet.org | @CCIAnet

March 27, 2023

Via Electronic Mail (regulations@cppa.ca.gov)

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR 02-2023

The Computer & Communications Industry Association ("CCIA")[1] is pleased to respond to the California Privacy Protection Agency (the "Agency" or "CPPA") Invitation for Preliminary Comments on Proposed Rulemaking (the "Rules") that will implement the California Privacy Rights Act of 2020 (the "CPRA").

I. INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. The Association supports and appreciates the Agency's efforts to adopt and implement privacy regulations that will guide businesses and protect consumers. These comments focus on the topics and questions for public comments regarding Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.

To give businesses clear standards and meet consumer expectations, California should seek to harmonize its approach with other state laws. Virginia, Colorado, and Connecticut have all adopted privacy laws that incorporate automated decisionmaking opt-outs limited to "decisions that produce legal or similarly significant effects" and the forthcoming rules should be consistent with this emerging norm. Interoperability of state laws allows consumers to benefit

[1] CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

from consistent protections and avoids a complex patchwork of privacy laws that disproportionately impacts the compliance efforts of small and medium sized businesses.

II. CYBERSECURITY AUDITS

A. Question 2.

The National Institute of Standards and Technology continues to provide a forward-looking approach to cybersecurity as it develops its Cybersecurity Framework (CSF) 2.0, building upon the success of its CSF 1.0.[2]

B. Question 3.

Some existing laws allow businesses to submit an annual self-certification that the required audit has occurred – such as the New York Department of Financial Services.[3] The Agency should adopt a similar regulation, permitting organizations to submit annual self-certifications to the Agency. Moreover, if the processing that creates a significant risk (as eventually defined by the final Rules) is already the subject of another audit (such as the Payment Card Industry Data Security Standard (PCI-DSS) or Sarbanes-Oxley Act of 2002), then the existing audit should suffice for the CPRA regulations.

The Agency should allow businesses the option, as an alternative, not as the sole requirement, to submit proof of certification such as PCI, NIST, or International Organization for Standardization (ISO) that demonstrates their compliance with this requirement.

Businesses may already perform certain industry standard audits and reports. For example, the storage of payment cards on file is regulated in the industry by the PCI-DSS standards, and merchants are required to recertify every year. In those circumstances, businesses should be able to re-use such audits and certifications rather than duplicate their efforts, which

---

[2] Cybersecurity Framework, *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0*, NIST (March 1, 2023), https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.
[3] NYDFS Cybersecurity Regulation, 23 N.Y. Comp. Codes R. & Regs. Tit. 23 § 500 (2017).

would unduly add to the cost and burden of compliance. Businesses should be permitted to use certifications and audits related to cybersecurity from service providers to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

C. Question 4.

CCIA recommends that the Agency should allow companies to rely on reasonable industry standards. To ensure that audits are independent, companies should also be permitted to rely on internal bodies that have safeguards to ensure that they are thorough and independent.

D. Question 5.

The Agency should clearly define what type of processing creates a significant risk, preferably by limiting the types of personal information to which the cybersecurity audit requirement applies. Other sector-specific laws that require similar audits are limited to specific types of personal information such as payment data (as in the NYDFS Cybersecurity Regulation). For large businesses, conducting such an audit for lower-risk personal information that does not require such audits under other laws would create a significant expense with little benefit to consumers.

Many businesses already have self-audit mechanisms and other internal standards and protocols based on appropriate industry standards.[4] Further, larger businesses have internal teams that exist solely to conduct audits, often separate from the first-line teams that are actually implementing security controls. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates. These teams are designed to be thorough and independent. CCIA recommends that businesses should be able to leverage those existing processes to meet CPRA requirements.

[4] *See,* NIST, *Assessment & Auditing Resources*, Cybersecurity Framework, (Oct. 7, 2022) https://www nist.gov/cyberframework/assessment-auditing-resources

CCIA strongly urges that the final Rules do not require businesses to use third-party auditors as the burden and expense would be overly disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs. Notably, third-party audits may also present a security risk, as they may expose a business's confidential security practices and (depending on the nature of the audit) potentially also underlying data to one or more third parties.

III. RISK ASSESSMENTS

Risk assessments should seek parity with other states. With states increasingly incorporating requirements around risk assessments, these obligations must be streamlined to avoid businesses having to conduct multiple assessments for substantially similar processing activities. California could look to obligations such as those in Virginia and Connecticut to shape this requirement and avoid unnecessarily duplicative compliance burdens.

A. Question 3.

Question 3(d) asks, what processing does not present a significant risk to consumers' privacy or security.

From a privacy risk perspective, risk assessments should be limited to processing that presents a heightened risk of harm to a consumer. Risk assessments should be consistent with other states like VA and CT.

From a security risk perspective, risk assessments should be limited to the processing of data that, if compromised, is likely to result in real, concrete harm(s) to individuals. Examples may include identity theft or fraud, extortion, or physical injury from the disclosure of intimate or other objectively sensitive personal details such as one's sexual orientation.

However, the processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or otherwise to comply with legal obligations should be exempted from the scope of this definition/regulation. These activities protect

consumers' privacy and security and enable organizations to keep such activities confidential to prevent bad actors from gaining insight into the organizations' internal systems. The use of data tools and mitigation measures, such as pseudonymizing or encrypting the relevant data, can meaningfully reduce the risk with processing.

B. Question 4.

Question 4(a) explores the benefits and drawbacks of considering the data protection impact assessment (DPIA) content requirements under the General Data Protection Regulation and the Colorado Privacy Act.

A DPIA should be detailed enough for the business and the regulator to appreciate the risk, however, it should not be overly prescriptive or specific. This balanced approach would allow businesses to retain flexibility and scale existing processes, in particular where a wide variety of factors may apply.

The Agency could consider a similar approach to the one outlined in the EU's Article 29 Data Protection Working Group Report on the Guidelines for DPIAs.[5] The report describes that a "DPIA is not mandatory for every processing operation", but rather only when the process is "likely to result in a high risk to the rights and freedoms of natural persons." Furthermore, the "GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. […] However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them."

Ultimately, the DPIA should be viewed as a documentation requirement and not a substantive mandate that the company must mitigate or fix any identified risk. The DPIA should also be limited to the actual processing of data – it should not be used as a proxy to require a risk

[5] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA)*, (Oct. 13, 2017), https://ec.europa.eu/newsroom/article29/items/611236.

assessment of the feature itself as distinct from any processing of data that occurs as part of that feature. Finally, the Agency should permit a single risk assessment to cover multiple related types of data processing activities.

C. Question 5.

The Rules should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. To promote interoperability and minimize burdens to covered businesses, CCIA recommends that the regulations specify that the Agency will accept risk assessments that were originally conducted under a comparable legal requirement.

Privacy obligations and risk balancing should be consistent across jurisdictions relating to the same requirements. The Association suggests the Rules align with any data impact or risk assessments required under other similar laws, such as the Colorado Privacy Act and Virginia Consumer Data Protection Act. However, CCIA cautions against adopting in full any future regulatory guidance under other laws, including the GDPR. EU case law is evolving in unpredictable ways, and California should develop guardrails that would ensure that any future obligations on California businesses are appropriately balanced against any potential burden. A consistent standard across jurisdictions would allow businesses to continue to build robust systems to protect consumers' information. These systems will benefit from clear guidelines that allow businesses to innovate and develop their data protection assessments and properly assess their cybersecurity risks.

D. Question 6.

Regarding Question 6(a), as a threshold matter, the Agency should clarify that its function under the statute to provide "a public report summarizing the risk assessments filed with the agency" refers to the risk assessments identified in 1798.185(15)(b). The statute appears to mistakenly refer to 1798.185(15)(a), which concerns cybersecurity audits.

Concerning (a)(i), risk assessments should highlight the most significant privacy risks associated with the processing activity in question and the steps being taken to address and mitigate that risk. Companies should not be required to divulge commercially sensitive information or sensitive security information, including details on technical safeguards that would allow a bad actor to compromise the company's security practices.

For (a)(ii), the Agency should not overly prescribe the format in which the business must submit the risk assessment. Businesses may prepare and record assessments in different ways and in response to different jurisdictions, so they should retain the flexibility to submit the assessment without needing to alter the format or content to match California-specific requirements. An example of an overly-prescriptive format would be if the Agency mandated that a business submit the required information via a webform with answer bubbles that needed to be manually populated.

With respect to (a)(iii), the regulations should not require organizations to repeatedly conduct or submit risk assessments for processing activities that have not materially changed and that pose no new or heightened risks. Such a requirement would be operationally burdensome, particularly for small and medium-sized businesses, and could incentivize businesses to treat risk assessments as a mere 'check-the-box' compliance exercise. Therefore, the Agency's regulations should specify that businesses are only required to "regularly submit" assessments for new or materially changed processing practices that present a significant risk. If the Agency requires periodic updates absent any change, then such updates should not occur more frequently than once every three years.

E. Question 8.

Regarding the guidance for conducting risk assessments and weighing the benefits of processing against potential risks, the Agency should describe that the factors relevant to this balancing may include:

- Technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks;
- The reasonable expectations of consumers;
- The context of the processing concerning the relationship between the business and consumers.

The regulations should also include protections to ensure that businesses have the necessary confidence to use risk assessments to fully document and assess processing practices, and are not incentivized to treat their assessments as a defensive measure against potential future litigation. Therefore, in addition to the important carve out for trade secrets, the regulations should clarify that risk assessments conducted under the CPRA are confidential and exempt from public inspection and copying under the California Public Records Act and that submitting an assessment to the agency does not constitute a waiver of any attorney-client privilege or work-product protection. The Agency should also not be permitted to use the submitted assessment as evidence of wrongdoing or used to penalize the business for weighing the risks in a way with which the Agency disagrees.

IV. AUTOMATED DECISIONMAKING

Any regulation of automated decisionmaking technology must be grounded in an understanding of how personalization provides people with informative and relevant content, helping them achieve their goals. Personalization – through advertising, ranked search results, or tailored content recommendations – allows people to navigate through the vast amount of information online and connect with the content most relevant to them. When people find new music on their favorite streaming service or discover an interesting article in a news application, they are likely seeing personalized recommendations. Personalization benefits the entire internet ecosystem, from helping charities and non-profit organizations better reach the audience most interested in their offerings, to enabling individuals to connect and share interests to create online

communities and social movements. Personalization is essential to the core value of the internet, and without it, online services would be far less efficient, and possibly even unusable.

A. Question 1.

The Agency should keep in mind that automation is a subset of decisionmaking – and so existing laws (such as anti-discrimination frameworks) that govern how a company makes decisions generally would also apply to such automated systems.

Regarding laws targeted solely to automated decisionmaking, companies in the United States are subject to several existing, or enacted but not yet effective, privacy laws that already impose substantial obligations with respect to the consumer right to opt out of automated decisionmaking. This includes the CO, CT, and VA state privacy laws. Critically, each of these laws is limited to high-risk decisions, described as those which have "legal or similarly significant effects," and in the case of CT, target "solely" automated decisions.

To ensure interoperability with those laws and to strike the right balance between protecting consumers while enabling access to important technology, the Agency should likewise confirm through rulemaking that the profiling opt-out: (i) applies only to decisions with *legal or similarly significant effects* (ii) is limited to solely or fully automated decisions, and (iii) applies only after an automated decision is made.

Significant and High-Risk Decisions. The Agency should not regulate the use of low-risk automated decisionmaking technology, such as spell check, GPS systems, databases, spreadsheets, or transcription services. Requiring businesses to provide opt-outs for such low-risk technology could slow down their activities substantially, while not providing a meaningful benefit to consumers, who should expect that business activities are performed using well-accepted, widely used technology. Regulators should focus on high-risk use cases, such as using technology to make final decisions regarding access to housing, medical benefits, or other critical services without appropriate human involvement. For example, under the Virginia

Consumer Data Protection Act, the consumer's right to opt out of profiling is restricted to "[d]ecisions that produce legal or similarly significant effects concerning a consumer." This is defined as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."

Fully-Automated Decisions. This limitation avoids creating an unreasonable obligation on businesses, without impacting the right of a consumer to have their decisions assessed by a human.

Final Decisions. Businesses in every industry sector use automated systems to improve their competitiveness and enhance their products and services, including routine and low-risk applications such as filtering and spell-check. The use of such systems and algorithms has enabled small businesses to effectively market their products to the right consumers at affordable prices and allows for better customer experience and cheaper prices.[6] Furthermore, such automated systems have helped small businesses improve their efficiency and productivity, increase accuracy and reduced errors, and better collaboration and communication.[7] CCIA is concerned that a blanket approach to automated decisions would impose excessive costs and delays upon businesses in return for minimal consumer benefit, with an increased cost being more likely.

Mandating that companies must provide the option of human involvement even before any decision is made creates a huge burden on companies, which might not be able to support a

[6] Alessandra Alari, *As consumer decision-making gets more complex, automation helps to simplify*, Think with Google (Aug. 2021), https://www.thinkwithgoogle.com/intl/en-gb/marketing-strategies/search/consumer-decision-making-automation/.
[7] Shopify Staff, *How Workflow Automation Can Streamline Your Business*, Shopify (Feb. 24, 2023), https://www.shopify.com/blog/workflow-automation.

similar number of requests without incurring unreasonable expenses. For example, individuals receive faster access to services if businesses can quickly identify low-fraud risks. This is only possible at scale through the use of either simple algorithms – such as to approve the transaction with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use a manual review to make final decisions, for example, akin to an appeals process. In these situations, if non-final decisions – like those cases flagged only by algorithms for further human review – are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.

While such a pre-decisional requirement will result in higher costs and slower service times, it would not provide consumers with any benefits beyond those that a post-decisional opt-out would provide. For instance, if individuals apply for a loan and have a positive outcome on the first automated decision, which might take just a few seconds to be issued, they likely will not want or need to opt-out and request review (but they would retain the right to). Even if they have a negative outcome (again, which they might know in just a few seconds), they will still be able to exercise the right to contest that decision and have a human making a new decision. If laws force companies to have the opt-out even before a decision is made, the experience could take several days, without any actual gain/benefit for customers, because the decision will be issued by the same person that already had access in the first scenario.

B. Question 2.

Generally, companies do not have requirements, frameworks, or best practices that address access/opt-outs related to low-risk, everyday technology, even those that arguably make automated decisions. Access or opt-out rights for these types of automated decisions would slow down business substantially with no benefit to consumers. For example, businesses do not typically give consumers the right to opt-out of using optical character recognition on PDF

documents containing that consumer's personal information. Additionally, businesses do not give consumers the right to opt-out of having their information stored in an internal database that automatically sorts information alphabetically, and instead demand handwritten records be stored and sorted manually. Regulations should not dictate how businesses use or do not use everyday, low-risk technology.

However, to the extent that artificial intelligence (AI)/ machine learning (ML) is used in high-risk automated decisionmaking, that is an area where there are robust requirements, frameworks, and best practices that are continually being developed and deployed. In recent years there has been a proliferation of AI/ML international standards, such as those created by the International Organization for Standardization (ISO) and NIST. In January 2023, NIST released an Artificial Intelligence Risk Management Framework, a set of guidance for organizations designing, developing, deploying or using AI systems to help manage risk. Among many other measures, this framework discusses transparency, human oversight, and appealing system outcomes. Moreover, the NIST AI Playbook helps organizations navigate and incorporate the frameworks' considerations, such as trustworthiness in the design, development, deployment, and use of AI systems.

Importantly, technology companies remained focused on the responsible use of AI/ML. Some examples include Meta's five pillars of Responsible AI, AWS' guide on the Responsible Use of Machine Learning, and Google's Responsible AI practices. For example, AWS' guide provides considerations and recommendations for responsibly developing and using ML systems across three major phases of their lifecycles: design and development; deployment; and ongoing use. Lastly, where useful and meaningful to mitigate risk, companies have provided information or guidance on technology that may be related to automated decisions.

C. Question 3.

Regarding Question 3(a), CCIA urges policymakers to focus on automated decisionmaking systems that produce legal or similarly significant effects. Accordingly, automated decisionmaking should be defined as "final decisions that are made solely/fully with AI/ML technology with legal or similarly significant effects on an individual," and AI/ML technology should be defined as: "the use of machine learning and related technologies that use data to train algorithms and predictive models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, natural language processing, and speech recognition."

Regarding Question 3(c), as part of GDPR compliance, companies already allow EU customers to request a review of certain fully automated decisions. Companies can extend that process to U.S. customers as appropriate.

D. Question 4.

Businesses of all sizes and in nearly every industry sector use ADM to improve their competitiveness and enhance their product and service offerings, such as through the use of daily, low-risk applications like spellcheck and tabulations. For instance, algorithms may be used to recommend a book or song or allow a small business to market its products to the right consumers at affordable prices.

Regarding AI/ML, the adoption of AI across industries is widespread and growing. A 2021 McKinsey and Company study found that 56% of business leaders across the globe now report using AI in at least one business function.[8] The report highlights that the most common AI use cases are low-risk, involving service-operations optimization, AI-based enhancement of products, and contact-center automation.

E. Question 5.

[8] Report, *The State of AI in 2022—And A Half Decade in Review*, McKinsey (Dec. 6, 2022), https://www mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review#/.

Automated technology has significant benefits to both businesses and consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost savings, and increased efficiency. Accordingly, regulators should be very mindful about providing consumers with a right to opt-out of automated activities, as it could severely hamper businesses' and other consumers' ability to realize those advantages.

CCIA recommends the Agency provide businesses and organizations guardrails rather than broad opt-out rights. Specifically, if high-risk business offerings are essential or critical, and it is not reasonable for consumers to consider other options, businesses should have the ability to demonstrate the existence of operational guardrails instead of providing for an opt-out. Depending on the specifics of the use case, appropriate guardrails could include things like significant, rigorous testing; system monitoring, corroboration of results, or even a complaint process if reasonable.

Automation can serve as the offered service or product – often automation may be core to certain high-risk service offerings, making opt-outs infeasible. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance should not be required to provide a consumer with some sort of manual process that conducts the same task – that would defeat the purpose of the automated service. In these instances, businesses should have the ability to demonstrate the existence of operational guardrails that protect California consumers' interests instead of providing for an opt-out.

Automation may also be essential to products that involve less significant effects, while still providing high value with minimal risk to consumers. Examples include:

- calendars that provide you with updated travel times based on traffic patterns from your current location;
- voice services that improve understanding and performance based on interaction history (e.g., when you ask to "play Rush," you mean the band, not the pundit);
- robots that learn what your stairs look like so they do not fall.

Firms should not have to design objectively worse, and potentially even dangerous, versions of their products and services merely to give customers a right to opt-out of ADM. To avoid unnecessary interruption to consumer enjoyment of these products and services, CCIA recommends the Agency should follow the approach of other U.S. state privacy laws and limit the profiling opt-out to automation that has legal or similarly significant effects on an individual.

Opt-out option may also create significant risks. The regulations should recognize that some uses of automated decision-making that produce legal or similarly significant effects may be highly beneficial to consumers – and if turned off, creates the risk of potential harm. The statute did not intend for consumers to be able to opt-out of these uses. For example:

- a health-care system that uses an individual's address to select the closest ambulance dispatch location;
- a bank that uses income or account balance to assess available credit; or
- fraud detection and related activities in making financial or insurance decisions.

To protect California consumers' interests without burdening beneficial uses, the regulations should tailor the scope of "legal or similarly significant effects" to the harms regulators seek to protect against. And as noted above, the regulations should permit operational guardrails rather than requiring an opt-out.

F. Question 7.

Businesses should be allowed to use race, ethnicity and other demographic data with the user's consent for the narrow purpose of evaluating and preventing bias. Restricting the use of this data will unnecessarily inhibit progress in this field to achieve fairness and possibly reintroduce the failures of "fairness-through-unawareness."[9]

[9] Fairness through unawareness assumes that if one is unaware of protected attributes, like gender or race, while making decisions or omits it from the model, the decisions will be fair. This approach has been shown to not be effective in many cases. *See* Giandomenico Cornacchia, et al, *Auditing Fairness Under Awareness Through Counterfactual Reasoning*, 60 Info. Processing & Management 2 (2023), https://doi.org/10.1016/j.ipm.2022.103224.

CCIA also urges the Agency to consider a safe harbor for businesses that are trying to prevent bias. It is not possible to prevent bias without measuring the algorithm's impact on different user groups, including minority groups.

G. Question 8.

Yes. Given the vast use cases for automated decisionmaking technology and profiling, the Agency should largely defer to sector-specific regulatory schemes to address any concerns about the use of this technology. For example, the risks, concerns, and benefits pf using an AI translation service differ significantly from developing and using self-driving cars, which also differ significantly from the use of AI medical software. From a policy and regulatory perspective, each of these areas is best addressed through a specific examination of the sector in question. To the extent the Agency does promulgate rules in this space, it should consider the parameters set out in the aforementioned response to Question 3.1

Yet some use cases raise additional concerns about permitting an opt-out right even for high-risk service offerings. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance shouldn't be required to provide a consumer with some sort of manual process that conducts the same task – that would defeat the purpose of the automated service.

Finally, the Agency should recognize the ADM benefits of reducing the need for human review, in particular where such review may lead to human error in processing, risk of improper disclosure, review, or dissemination of consumer personal data, and bias.

To protect California consumers' interests without burdening beneficial uses, the regulations should tailor the scope of "legal or similarly significant effects" to the harms regulators seek to protect against (such as the provision or denial of lending services or housing). Regarding employee and business to business data, the profiling opt-out should exclude automation involving individual data in the employment or and commercial contexts.

Concerning the employment context, there are developing state and local laws that already specifically target the use of these technologies in the workplace, so California should let that regulatory activity run its course. Moreover, those laws are being tailored to the nuances of an employment context and, recognizing the potential unreasonableness of requiring specific opt-outs for every instance of automated decision-making, are mainly focused on transparency and human review. Lastly, any decision in the employment context arguably could have a "legal or similarly significant effect," including innocuous ADM-like task allocation that is intended to enable efficiency and scale.

H. Question 9.

Companies are still at an early stage in the development of automated decisionmaking system transparency tools. Rather than prescriptive and granular transparency requirements that do not necessarily provide consumers with meaningful disclosures, the rules should provide businesses with the flexibility to figure out what tools are most effective. Platforms must be given the ability to innovate with their transparency tools and provide information that is meaningful to people. CCIA is concerned that such prescriptive requirements will unnecessarily constrain this innovation.

Businesses should be able to fulfill consumer access requests by providing a general explanation of technology functionality, rather than information on specific decisions made. Businesses should be able to provide this information via a publicly available disclosure on their webpage.

In order to provide "meaningful" information about the logic involved in a decision, businesses should be permitted to describe the general criteria or categories of inputs used in reaching a decision. For example, if a rental company considers certain personal information when evaluating a housing application, those categories of information could be described. A more detailed description of any complex algorithms involved in automated decisionmaking will

not provide the average consumer with "meaningful" information on the logic involved in the processing. In addition, providing a detailed explanation of the algorithms involved runs the risk of imposing obligations that conflict with the intellectual property, trade secret, and other legal rights of the business in question. With respect to fraud or security decision-making, disclosures could instruct fraudsters or bad actors on circumventing the system.

Any regulation should also ensure that businesses are protected from disclosing proprietary information, such as that which is subject to intellectual property or trade secret protection, in response to consumer access requests.

I. Question 10.

The right to opt-out should be limited to automated decisions that pose the greatest risk. Online services routinely make several automated decisions to provide the services that people sign up for – automated recommendations enable personalization, which is the basis for a wide array of free and paid online services.

CCIA is concerned any rule implementing a blanket opt-out right of automated decisionmaking technology and profiling would significantly undermine companies' ability to provide personalized services to all users, regardless of whether they have opted-out. Rather, the focus should be on profiling based on automated decisions rather than the technologies used to derive those decisions. Profiling is simply data collected and processed about an individual. Businesses use the data they collect to provide consumers with richer, more engaging experiences.

The rules should avoid blanket restrictions on profiling and instead focus on how the data is collected, secured, and used. Profiling can enable numerous consumer and societal benefits such as helping:

- consumers find the TV shows and movies that they want to see out of the thousands of options available on a streaming service;
- nonprofit community organizations find volunteers who live nearby;

- small businesses compete against large incumbents without spending tens of thousands of dollars on traditional advertising.

Although, like much of what makes the internet valuable, some automated decisions involve risks such as those relating to individuals' privacy and data security. However, this possibility should not result in uncompromising rules that take control away from the consumer.

The GDPR strikes the right balance between ensuring consumers have access to reasonable controls and enabling beneficial uses of automated systems by limiting regulation to those that pose the greatest risks, specifically solely automated systems that produce "legal or similarly significant effects." In the US, privacy laws in Virginia, Colorado, and Connecticut incorporate a similar limiting principle, where the right to opt-out is limited to "profiling in furtherance of decisions that produce legal or similarly significant effects." These provisions are appropriately focused on decisions of significance to an individual's employment, financial status, health care, and California's opt-out right should mirror this approach.

An effective balancing of interests gives consumers control over how their data is used without creating all-or-nothing choices that are inconsistent with consumers' expectations. The best way to do that is by tailoring the opt-out around the highest-risk decisions. An opt-out that severely limits – or altogether eliminates – the ability to employ all automated decisionmaking will make it far less efficient, and in some cases impossible, for people to find what interests them or unlock the content most relevant to them (especially if they don't know what they are looking for).

A broad opt-out right could also have a significant impact on efforts to protect the safety and integrity of online platforms. It would not only harm the effectiveness of automated decisionmaking in protecting the safety of users (e.g., the removal of spam or other violative content), but also the ability to defend against security threats and other integrity risks posed by

bad actors. Rather, consumers should be offered a meaningful choice that respects their autonomy and allows them to make clear, understandable decisions about how their data is used.

Regulations should distinguish between the role of automated decision technology developers – companies that design and develop the technology – from deployers – companies that deploy the technology out in the world and with consumers. Regulations should clarify that developers do not have any standalone obligations about consumer access requests or opt-outs, but only an obligation to provide "reasonable" assistance to deployers, which could, among other things, be provided in the form of generally available documentation.

Any regulations around automated decisionmaking need necessary exceptions to access and opt-out to avoid abuse – as is already the case in CO, CT, and VA – that include to:

- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action.
- Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may be illegal.
- Provide a product or service a consumer requested or perform a contract with the consumer.
- Take immediate steps to protect an interest that is essential for the life of the consumer or another natural person, if the processing cannot be manifestly based on another legal basis.
- Process personal data for reasons of public interest in the area of public health, subject to certain conditions.
- Conduct internal research.
- Fix technical errors.
- Perform internal operations that are consistent with the consumer's expectations.

V. CONCLUSION

CCIA and its members thank the Agency for this opportunity to provide input on how to balance the next set of Rules in ways that protect consumers, are feasible to implement, and retain flexibility for personalization and innovation.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
[redacted]

March 27, 2023

From:	Parker, Sarah [redacted]
Sent:	Monday, March 27, 2023 11:59 AM
To:	Regulations
Cc:	Tabitha Edgens; Gregg Rozansky; Canter, Libbie
Subject:	PR 02-2023: Preliminary Comments on Proposed Rulemaking
Attachments:	BPI_Comments on Pre-Rulemaking Activities.pdf

To whom it may concern:

On behalf of Tabitha Edgens and the Bank Policy Institute, please find attached preliminary comments on the proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking. Thank you.

Best,
Sarah

Sarah Parker
Pronouns: She/Her/Hers

Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
T[redacted] | [redacted]
www.cov.com

COVINGTON

March 27, 2023

Via electronic mail

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: **Preliminary Comments on Proposed Rulemaking Under the California Consumer Privacy Act (PR 02-2023)**

The Bank Policy Institute[1] appreciates the opportunity to submit preliminary comments to the California Privacy Protection Agency on the proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking under the California Consumer Privacy Act, as amended by the California Privacy Rights Act.[2]

I. Executive Summary

BPI's members are financial institutions that have invested significant time and resources into building data protection and information security compliance systems that align with federal and state financial privacy, consumer protection, and other financial services laws. BPI members are committed to promoting robust privacy protections for California consumers. Drawing on the experience of its members operationalizing privacy and security safeguards for their customers, BPI has provided comments on each of the three areas that will be addressed in the forthcoming rulemaking: cyber audits, risk assessments, and automated decisionmaking.[3] In particular, BPI urges the Agency to consider:

- Exempting federally-regulated financial institutions from any new audit, risk assessment, and automated decisionmaking requirements, to avoid duplication, conflict, or interference with the existing financial services regulatory scheme;

- Specifying, at a minimum, that financial institutions' existing auditing and risk assessment activities satisfy any new regulatory requirements and are not required to be disclosed to the Agency;

---

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

[2] Cal. Civ. Code § 1798.100 *et seq.*

[3] While BPI has provided its responses in a narrative form, it has listed the relevant questions addressed in its comments at the start of each section below.

- Harmonizing any new requirements with existing banking regulation and supervision in these areas, as well as with similar audit and risk assessment provisions in the U.S. and international jurisdictions and other consumer protection and privacy frameworks; and

- Creating necessary exemptions for opt-out and access rights for automated decisionmaking, including where there is the involvement of a human in decisionmaking, where the outcome does not result in legal or similar detriment to the consumer, for automation that is used in furtherance of regulatory compliance goals or for security and fraud-prevention purposes, and for trade secrets.

The regulations should recognize the paramount role that financial regulators play in regulating national and state banks and savings associations and their affiliates.[4] These institutions already are subject to robust regulation and active supervision in these three areas, including by federal prudential regulators (i.e., Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency) and, for state-chartered financial institutions, state banking regulators. [5] Information security and use of artificial intelligence are evaluated as part of financial regulators' comprehensive and ongoing supervision of banks' risk management systems and compliance with applicable laws and regulations. Federal supervision requires that all banks have internal controls and information systems that are appropriate to the size of the institution and the nature, scope, and risk of its activities. Banks are also required to have an internal audit system appropriate to the nature and scope of a bank's activities and that is informed by a risk assessment process.

The CCPA statute exempts many federally-regulated financial institution activities because it explicitly exempts personal information subject to the Gramm Leach Bliley Act.[6] However, most of the regulatory frameworks and requirements discussed in this letter apply broadly to all information assets of an institution – not just those that are subject to the GLBA.[7] Thus, the Agency should expressly exempt federally-regulated financial institutions from any new audit, risk assessment, and automated

---

[4] For purposes of this letter, BPI uses the term "federally-regulated financial institutions" to refer to entities regulated by the federal prudential regulators, *i.e.*, the Board, FDIC, and OCC, (collectively, referred to as "banks") and their affiliates. Both terms encompass state banks that are chartered at the state level, as such banks remain subject to supervision and examination by federal prudential regulators – the Federal Reserve in the case of banks that have joined the Federal Reserve System, and the FDIC in the case of other state-chartered banks.

[5] In addition, the National Credit Union Administration, Securities and Exchange Commission, Commodity Futures Trading Commission, Federal Trade Commission, Consumer Financial Protection Bureau, and the Federal Housing Finance Agency all have regulatory, supervisory, enforcement, and/or examination authority over cybersecurity matters with respect to entities within their jurisdiction. Other regulatory bodies include individual state banking, insurance, and securities regulators as well as non-governmental self-regulatory organizations, such as the Financial Industry Regulatory Authority, National Futures Association, and the Municipal Securities Rulemaking Board.

[6] The CCPA exempts information collected, processed, sold, or disclosed subject to the GLBA and implementing regulations or the California Financial Information Privacy Act. *See* Cal. Civ. Code § 1798.145(e).

[7] *See, e.g.,* FFIEC, IT EXAMINATION HANDBOOK: INFORMATION SECURITY, at 1 (Sept. 2016), https://ithandbook ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf ("Information Security Booklet") (noting that the booklet "addresses regulatory expectations regarding the security of all information systems and information maintained by or on behalf of a financial institution"); 12 C.F.R. § 30, Appendix A (OCC) ("OCC Interagency Guidelines Establishing Standards for Safety and Soundness"); 12 C.F.R. § 208, Appendix D-1 (Board); and 12 C.F.R. § 364, Appendix A (FDIC).

decisionmaking requirements to avoid any duplication, conflict, and interference with existing financial services regulatory schemes.[8]

In particular, for national banks and federal savings associations, visitorial rights restrict the ability of states to inspect, examine, or regulate these entities' activities that are authorized under federal banking law.[9] There would be serious questions about the permissibility of state requirements to conduct – and, certainly, to share with state privacy regulators – audits and risk assessments that involve the processing of personal information in connection with activities that affect lending, deposit taking, and other national bank and federal savings association operations. It is thus crucial that banks and savings associations are exempt from any new audit and risk assessment requirements and any expectations to make such materials available to California regulators.

In addition, to the extent that any federally-regulated financial institutions are not categorically exempt from the substantive audit and risk assessment requirements, the Agency should harmonize any new requirements with existing banking regulation and supervision in these areas, as well as with similar audit and risk assessment requirements in the U.S. and international jurisdictions such as Europe and the United Kingdom.

Similarly, any new California privacy requirements related to automated decisionmaking should not be applied to federally-regulated financial institutions to avoid disrupting or interfering with existing financial regulation and supervision. At a minimum, the Agency should be careful not to limit the ability of banks to use automation in various ways that further important public policy interests, such as security and prevention of fraud and other financial crimes. To the extent federally-regulated financial institutions are not exempted, any applicable requirements should be interoperable with other consumer protection and privacy frameworks.

II. Cybersecurity Audits

- *What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits?*
- *What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1,*

[8] The Agency clearly has the authority to exempt these industries, as the statute does not compel implementation of new requirements in industries or contexts where the record does not support it. Moreover, the CCPA should not restrict a business's ability to comply with federal laws, Cal. Civ. Code § 1798.145(a)(1), or conflict with federal law, *id.* § 1798.196.

[9] *See* 12 U.S.C. § 484 ("No national bank shall be subject to any visitorial powers except as authorized by Federal law, vested in the courts of justice or such as shall be, or have been exercised or directed by Congress or by either House thereof or by any committee of Congress or of either House duly authorized."). Visitorial powers are defined as (i) examination of a bank; (ii) inspection of a bank's books and records; (iii) regulation and supervision of activities authorized or permitted pursuant to federal banking law; and (iv) enforcing compliance with any applicable federal or state laws concerning those activities. Notably, examination of a bank's books and records is not limited to on-site inspection. *See* 12 C.F.R. § 7.4000; *see also Watters v. Wachovia Bank, N.A.*, 550 U.S. 1, 21 (2007) ("[S]tate regulators cannot interfere with the 'business of banking' by subjecting national banks or their OCC-licensed operating subsidiaries to multiple audits and surveillance under rival oversight regimes."). These requirements have been explicitly extended to federal savings associations and their subsidiaries. *See* 12 CFR § 7.4010(b).

or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2?

- *With respect to the laws, cybersecurity audits, assessments, or evaluations identified in response to questions 1 and/or 2, what processes help to ensure that these audits, assessments, or evaluations are thorough and independent?*

As part of the robust regulation described above, banks are already subject to comprehensive cybersecurity auditing requirements, including obligations to maintain their own audit programs and, significantly, on-site examinations by their prudential regulators that cover cybersecurity. Accordingly, federally-regulated financial institutions should be exempted from any cybersecurity audit regulations promulgated by the Agency or, in the alternative, permitted to rely on their existing cybersecurity audits. As discussed above, an exemption also helps avoid raising potential inconsistencies with visitorial powers for national banks and federal savings associations.

A number of federal financial services laws and regulations require banks and other financial institutions to manage cyber risks, including through an appropriate audit program. These include but are not limited to the information security provisions of GLBA and its implementing regulations and guidance.[10] For example, GLBA regulations require banks to not just maintain an information security program, but to regularly monitor, evaluate, and adjust their information security program in light of internal and external threats and other factors.[11] As a practical and administrative matter, the information security programs are necessarily designed to cover and protect all of a bank's information assets, and not just personal data subject to GLBA. Moreover, banks are also subject to general "safety and soundness" requirements, under which banks are required to maintain internal controls, information systems, and an internal audit system that are appropriate to the size of the institution and the nature, scope, and risk of its activities.[12]

Building on these legal obligations, the federal prudential regulators have developed an extensive inventory of policy statements, toolkits, and other guidance that set regulatory expectations for banks' information security programs. Among other requirements, a bank's information security program should be tested and evaluated through internal audits, self-assessments, and tests.[13] Moreover, perhaps uniquely among other industries, external bank examiners from the federal prudential regulators regularly examine the adequacy of bank information security programs, information systems, and audit programs – along with other topics – based on standards set forth in the Federal Financial Institutions Examination

---

[10] *See* 15 U.S.C. § 6801(b); 12 C.F.R. § 30, Appendix B (OCC) ("OCC Interagency Guidelines Establishing Information Security Standards"); 12 C.F.R. § 208, Appendix D-2 and § 225, Appendix F (Board); and 12 C.F.R. § 364, Appendix B (FDIC).

[11] *See, e.g.,* OCC Interagency Guidelines Establishing Information Security Standards at Sections II, III.

[12] 12 U.S.C. §§ 1818, 1831p-1; OCC Interagency Guidelines Establishing Standards for Safety and Soundness; 12 C.F.R. § 208, Appendix D-1 (Board); and 12 C.F.R. § 364, Appendix A (FDIC).

[13] *See* Information Security Booklet at 53; *see also* OCC, COMPTROLLER'S HANDBOOK: INTERNAL AND EXTERNAL AUDITS, at 2 (July 2019), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/internal-external-audits/pub-ch-audits.pdf ("Comptroller's Handbook"); OCC Bulletin 2003-12: Interagency Policy Statement on Internet Audit and Internal Audit Outsourcing; OCC Bulletin 99-37: Interagency Policy Statement on External Auditing Programs; and FFIEC, IT EXAMINATION HANDBOOK: AUDIT (April 2012), at A-1–A-17, https://ithandbook ffiec.gov/media/274709/ffiec_itbooklet_audit.pdf ("Audit Booklet").

Council's Information Technology Examination Handbook ("IT Handbook").[14] These examiners will assign a rating to the bank, identify deficiencies that must be remedied, work with management to obtain corrective action, and pursue enforcement related to their findings as necessary.[15]

Financial institutions also need to navigate a broader cyber regulatory environment. State financial regulators in some jurisdictions have set out robust requirements that state-chartered banks maintain a cybersecurity program that is based on a risk assessment and tested and audited.[16] Among them, the New York Department of Financial Services has robust requirements that mandate annual certifications of compliance.[17] As another example, broker dealers and others within the jurisdiction of the Securities and Exchange Commission are subject to a separate set of information security rules, which the SEC currently is in the process of strengthening.[18]

a) Bank Audit Programs

As noted above, banks are expected to maintain an effective information security program that is tested through an internal audit program that is appropriate to the size and complexity of the institution.[19]

Under interagency guidelines, as part of its information security program, a financial institution must conduct cybersecurity audits and risks assessments to determine foreseeable risks and threats, both internal and external, to the security, confidentiality, and integrity of customer information. For example:

- Conducting periodic reviews of access controls;
- Inventorying data, systems, applications, devices, platforms, and personnel;
- Ensuring customer information is encrypted at-rest and in-transit;

[14] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve, FDIC, OCCCFPB and NCUA. *See* FFIEC, Homepage, https://www.ffiec.gov/ (last accessed March 15, 2023).

[15] *See, e.g.,* Information Security Booklet at 74; 12 U.S.C. § 1818(b) (outlining procedure for a cease-and-desist order to issue against a bank if its prudential regulator believes that it is engaging or has engaged, or has reasonable cause to believe that it is about to engage, in an unsafe or unsound practice or violation of a law, rule, regulation, or condition imposed in writing upon the bank by the regulator).

[16] *See, e.g.,* 23 NYCRR § 500 (setting out robust cybersecurity requirements, including risk assessments).

[17] *See id.*

[18] *See* 17 C.F.R. § 248.30 (Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information); SEC, SEC Proposes Changes to Reg S-P to Enhance Protection of Customer Information, https://www.sec.gov/news/press-release/2023-51 (March 15, 2023). *See also* 16 C.F.R. § 314 (setting out information security requirements for financial institutions subject to the FTC's GLBA jurisdiction, including risk assessment requirements).

[19] *See, e.g.,* Information Security Booklet at 53; Audit Booklet at 1; and OCC Interagency Guidelines Establishing Information Security Standards at Sections II, III.

- Identifying and assessing the risks to customer information in each relevant area of a company's operation, such as with respect to service providers and changes in the firm's operations;

- Managing and controlling risk, including regularly testing key controls, systems, and procedures of the information security program. Tests must be conducted or reviewed by independent third parties or independent staff;

- Overseeing service provider arrangements, including conducting due diligence and reviewing audits, risk assessments, and tests of service providers and their information security programs;

- Implementing a program to respond to and mitigate data breaches involving customer data, including providing federal regulators, relevant law enforcement, and consumers notification of breaches; and

- Providing at least annually a report to the board or an appropriate committee of the board the overall status of the information security program and compliance with relevant regulations.[20]

To assist with self-assessments, the prudential regulators have developed a Cybersecurity Assessment Tool for banks to use to evaluate their cyber maturity that is consistent with and provides mapping to the National Institute of Standards and Technology Cybersecurity Framework (along with mapping to the FFIEC IT Handbook).[21]

In respect of a more formal cybersecurity audit program, banks are expected to maintain an audit program that is appropriate to the size and complexity of the institution.[22] These programs must meet specific requirements, such as the adequate monitoring of the system of internal controls through an internal audit function, independence and objectivity, qualified persons, and adequate testing and review of information systems.[23] Most large banks are also subject to the OCC's supplemental requirements referred to as "heightened standards."[24]

---

[20] *See, e.g.,* OCC Interagency Guidelines Establishing Information Security Standards at Section III; Comptroller's Handbook at 22.

[21] *See* FFIEC, CYBERSECURITY ASSESSMENT TOOL (May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf. NIST's Cybersecurity Framework is well-aligned with the processes and goals articulated in the CCPA. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* made the NIST Cybersecurity Framework mandatory for all US federal government agencies. The NIST Cybersecurity Framework was designed specifically for companies that are part of the US critical infrastructure. As a comprehensive framework, the NIST Cybersecurity Framework provides industry standards, guidelines, and practices that allow for communication of cybersecurity activities and outcomes across an organization from the executive level to the implementation and operations levels.

[22] *See, e.g.,* OCC Interagency Guidelines Establishing Information Security Standards at Section II.B (requiring "an internal audit system that is appropriate to the size of the institution and the nature and scope of its activities").

[23] *See, e.g., id.* They also must be independent; for example, other OCC guidance suggests that "[b]ank audit programs must be performed by independent and competent staff who are objective in evaluating the bank's control environment." Comptroller's Handbook at 2.

[24] *See* 12 C.F.R. § 30, Appendix D. For example, large OCC-regulated banks are, among other requirements, required to maintain a complete and current inventory of all material processes, product lines, services, and

Together, these audit program requirements address the management of cyber risks broadly and go beyond consumer personal information.[25] Further, banks are directed to use an industry cybersecurity control framework, such as the NIST Cybersecurity Framework or Committee of Sponsoring Organizations of the Treadway Commission framework, as the basis for audit scope and objective.[26] As a practical matter, banks also must assess their information program against the FFIEC IT Handbook standards against which banks are examined by their regulators.

Finally, banks are examined by their regulators for the adequacy of their audit programs. Examiners will assess the qualifications of the IT audit staff, quality of the audit, and level of audit independence.[27] The assessment includes some level of audit validation, including verification procedures as necessary, and examiners may expand their supervisory activities if they identify concerns with the internal audit.[28]

b) FFIEC IT Examinations

Banks (and their technology service providers) are also subject to direct examination by the federal prudential regulators on their information security programs pursuant to the FFIEC examination standards.[29] These exams cover, for example, information security program governance and management; information security policies, standards and procedures; classification of technology assets; user security controls; and other topics, as set forth in the IT Handbook.[30] Further, examiners may conduct on site-reviews, including independent testing of the bank's cybersecurity, such as through penetration testing. Examiners then prepare an examination report, assign ratings to the bank's activities, and identify any deficiencies that must be remedied by the bank.[31] These examiners will work with management to obtain corrective action, but the regulators can also pursue enforcement related to deficiencies.[32] Federal

---

functions and assess the risks associated with each; establish and adhere to an audit plan that is periodically reviewed and updated; establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis; and establish a quality assurance program that ensures internal audit's policies, procedures, and processes comply with applicable regulatory and industry guidance, are appropriate for the size, complexity, and risk profile of the covered bank, are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry internal audit practices, and are consistently followed. *Id.* at II.C.3.

[25] *See, e.g.,* OCC Interagency Guidelines Establishing Standards for Safety and Soundness (placing no restrictions on the scope of the required audits); 12 U.S.C. § 1831p-1 (requiring the federal banking agencies to prescribe standards relating "internal controls, information systems, and internal audit systems" with no limitation to consumer personal information).

[26] *See, e.g.,* Comptroller's Handbook at 112.

[27] *See* Audit Booklet at A-1–A-17.

[28] *See, e.g.,* Comptroller's Handbook at 2.

[29] *See* Information Security Booklet (provides guidance to examiners and addresses how examiners evaluate information security risks); FFIEC, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS (Oct. 2012), https://ithandbook ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

[30] *See* Information Security Booklet.

[31] *See, e.g., id.* at 74; Comptroller's Handbook at 70.

[32] *See, e.g.,* 12 U.S.C. § 1818(b).

financial regulators are thus heavily involved in both assessing a bank's internal audits and in conducting their own examinations, and may require banks to address any deficiencies that are identified through these internal and external audits.

c) Recommendations: Exemption & Interoperability

To sum, banks are subject to extensive auditing for cyber security and are examined by prudential regulators with expertise pertinent to this highly-regulated industry. Under the existing federal standards, banks already perform cybersecurity audits in any scenario where processing might present "significant risk" to consumers' privacy or security. They also perform cybersecurity audits even where such "significant risks" are not present. Further, these audits clearly meet the "thorough and independent" standard set forth in California law.[33]

For banks, any new cybersecurity audit requirement would at best be duplicative of, and at worst conflict with, the comprehensive and robust financial regulatory frameworks governing information security and cyber security audits for banks. For national banks and federal savings associations, such requirements would raise serious questions with respect to the OCC's exclusive visitorial powers. More generally, such application would frustrate federal policy goals: as noted in the FFIEC's authorizing statute, the FFIEC was created with the goal to "promote consistency in such examination and to insure progressive and vigilant supervision."[34] It also would not be consistent with the statutory design of the CCPA, which sought to avoid interference with federal regulation.[35] Finally, new cybersecurity audit requirements would be duplicative without adding any value for consumers.

BPI therefore urges that the Agency exempt federally-regulated financial institutions from any new cyber audit requirements. At a minimum, it should be clear that such institutions' existing auditing and information security activities satisfy any new regulatory requirements, although such audits must remain internal and should not be accessible to state privacy regulators. For similar reasons, the Agency should provide flexibility to conduct audits using an internal audit team. In no circumstances should such audits be made public. These audits contain highly sensitive information that, if compromised, could increase cyber risk for the banking system. Indeed, such institutions themselves are prohibited by law from disclosing the results of bank examinations performed by financial regulators as confidential supervisory information.[36]

III. Risk Assessments

- *What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?*
- *What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?*
- *What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?*
- *In what format should businesses submit risk assessments to the Agency?*

---

[33] Cal. Civ. Code § 1798.185(a)(15)(A).

[34] 12 U.S.C. § 3301.

[35] Cal. Civ. Code §§ 1798.145(a)(1), 1798.145(e).

[36] *See, e.g.,* OCC Bulletin 19-15: Supervisory Ratings and Other Nonpublic OCC Information: Statement on Confidentiality.

As part of the regime described above, banks are also required to conduct risk assessments in relation to processing activities involving personal information. In addition, the OCC's visitorial rights restrict the ability of states to inspect or examine national banks and federal savings associations for processing activities authorized under federal banking law. Thus, federally-regulated financial institutions (and, in particular, national banks and federal savings associations) should be exempted from any risk assessment regulations promulgated by the Agency. In any event, BPI supports regulations that are interoperable with the requirements for data protection assessments under the General Data Protection Regulation, other state privacy laws, and self-regulatory standards, and include sufficient protections for the confidentiality of these audits, as described further below.

a. Existing Risk Assessment Obligations

Banks are subject to risk assessment requirements as part of their information security program. For example, under the GLBA framework, banks must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, assess the likelihood of damage from these threats, and assess the sufficiency of policies, procedures and other measures to control these risks.[37] In addition, the FFIEC examination standards require a "risk assessment process to describe and analyze the risks inherent in a given line of business" that occurs at least annually.[38] This process is conducted prior to banks' internal audits, in an effort to "document a bank's significant business activities and associated risks" to prioritize the allocation of audit resources.[39] And, separately, financial institutions also must have identity theft prevention programs under the Fair Credit Reporting Act, which involve the identification of red flags for identity theft and protocols to address identity theft.[40] While these regimes also have broader goals, they serve in part to regulate and supervise banks' use and implementation of risk assessments in these areas.

b. Recommendations: Exemption & Interoperability

BPI strongly urges the Agency to either provide a categorical exemption from any new risk assessment requirements for federally-regulated financial institutions, or to specify that risk assessments that are conducted pursuant to other international, federal, or state privacy or banking laws or regulations satisfy any expectations for risk assessments in California and do not need to be provided to the California regulators.

BPI further urges the Agency to make any rules on risk assessments interoperable with the requirements for data protection assessments under the GDPR, the other state privacy laws, and self-regulatory standards. The European Data Protection Board's *Guidelines on Data Protection Impact Assessment* ("EDPB Guidelines") appropriately focuses resources on risk assessments where there is a

---

[37] *See, e.g.,* OCC Information Security Standards at Part III.B.

[38] Audit Booklet at 8.

[39] *See, e.g.,* Comptroller's Handbook at 23–26 (outlining OCC's audit risk assessment methodology and requirements).

[40] *See, e.g.,* 12 C.F.R. § 41, Subpart J (Red Flags Rule).

higher risk of harm to consumers.[41] In particular, the standard in the EDPB Guidelines requires an assessment where processing is "likely to result in a high risk."[42] Similarly, some other state privacy laws require assessments for "processing activities that present a heightened risk of harm to consumers[.]"[43] Likewise, California should focus its requirements on where there is likely to be a high or heightened risk of harm to consumers, in line with the "significant risk" standard in the statute.[44] Further, it should be clear that these assessments only apply to processing activities that are commenced prospectively.

c. Confidentiality Issues

If banks are not categorically exempt from risk assessment obligations, then they should nonetheless be exempt from any obligation to share these assessments with the Agency given the existing oversight of prudential regulators and the importance of protecting confidentiality. On this point, BPI notes that the GPDR only requires prior consultation with data protection authorities in limited circumstances.[45]

The regulations should also specify, as do other state privacy laws, that the assessments are confidential and exempt from public inspection and copying, and that the disclosure of a risk assessment does not constitute a waiver of any attorney-client privilege or work-product protection that otherwise might exist with respect to the assessment.[46] This final requirement is necessary to avoid suppressing the ability of businesses to obtain legal counsel related to potential privacy risks and safeguards. However, it is equally important to preserve general confidentiality from the public, as risk assessments conducted by financial institutions may contain highly sensitive information that could increase cybersecurity risks, harm consumers, and undermine the safety and soundness of financial institutions. Financial institutions themselves are prohibited by law from disclosing the results of bank examination, as well as other materials prepared for use by supervisors, as confidential supervisory information. This information is also protected from disclosure under the Freedom of Information Act.[47]

To sum, the Agency should exercise this opportunity to set the precedent now for interoperability across regimes and protection of confidential and privileged information.

IV. Automated Decisionmaking

- *What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?*
- *How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them?*

---

[41] *See* EUROPEAN DATA PROTECTION BOARD, GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND DETERMINING WHETHER PROCESSING IS "LIKELY TO RESULT IN A HIGH RISK" FOR THE PURPOSES OF REGULATION 2016/679 (April 4, 2017), *available at* https://ec.europa.eu/newsroom/article29/items/611236.

[42] *Id.* at 8–14.

[43] Va. Code Ann. § 59.1-576(A)(5); *see also* Colo. Rev. Stat. § 6-1-1309(1).

[44] Cal. Civ. Code § 1798.185(a)(15).

[45] Regulation 2016/679, OJ L 119/1, Art. 36.

[46] *See* Colo. Rev. Stat. § 6-1-1309(4); Va. Code Ann. § 59.1-576(C).

[47] *See* 5 U.S.C. § 552(b)(8).

The financial services industry is subject to federal laws and regulations that prohibit discrimination and provide transparency and accountability in the use of automated decisionmaking and artificial intelligence, including for employment purposes and extending credit, marketing, and other financial services. These legal requirements mitigate and protect against the same underlying concerns about discrimination and transparency as the CCPA's automated decisionmaking provisions, making additional regulation of federally-regulated financial institution's automated decisionmaking processes unnecessary. At a minimum, however, the Agency should ensure that the rules are interoperable with existing frameworks and narrowly circumscribed, to ensure that they do not restrict banks' ability to use automation for important public policy purposes.

a. Existing Protections

Banks and other financial institutions are subject to a number of additional laws, regulations, and guidance that promote accountability and accuracy in automated decisionmaking. Among them, the Equal Credit Opportunity Act and Regulation B prohibit unlawful discrimination against protected classes in "any aspect of" credit transactions, including through automation.[48] ECOA and Regulation B also provide certain data access rights. These include a right to a statement of reasons for a creditor taking adverse action, including reasons based on automated decisionmaking tools, and a copy of any written appraisals and valuations for certain mortgage loan applications.[49] Automated decisionmaking technologies that produce outcomes with legal or similarly significant effects on an individual (e.g., the denial or provision of financial and lending services) may be subject to these provisions or to provisions of the Fair Credit Reporting Act.[50] Further, the federal Fair Housing Act prohibits discrimination in the sale or rental of housing, residential real estate transactions, or the provision of real estate brokerage services,[51] and Title VII, the Civil Rights Act of 1964, and the Age Discrimination in Employment Act of 1967 protect employees and job applicants from discrimination.[52]

In addition, the Dodd-Frank Wall Street Reform and Consumer Protection Act prohibits unfair, deceptive, or abusive acts or practices ("UDAAP"), and the Federal Trade Commission Act prohibits unfair or deceptive acts or practices ("UDAP").[53] Prohibited UDAAP/UDAPs could include, for example, making false representations to customers about the use of automated technologies in processing customer data or deploying automated technologies in a way that harms customers. These laws are enforced against banks by the Consumer Financial Protection Bureau and the federal prudential regulators.

---

[48] *See* 15 U.S.C. § 1691 *et seq.*; 12 C.F.R. § 1002.

[49] *See* 15 U.S.C. § 1691(d), (e); 12 C.F.R. §§ 1002.9(b)(2) and .14; *see also* CFPB, Consumer Financial Protection Circular 2022-03 (addressing adverse action notice requirements in connection with credit decisions based on complex algorithms).

[50] *See 15 U.S.C. §§ 1681 et seq.*

[51] *See* 42 U.S.C. § 3601 *et seq*.

[52] *See* 42 U.S.C. § 2000e *et seq*. (prohibiting employment discrimination based on race, color, religion, sex and national origin); 29 U.S.C. § 621 *et seq.* (prohibiting employment discrimination against persons 40 years of age or older).

[53] *See* 12 U.S.C. § 5531; 15 U.S.C. § 45.

Further, banks are required to comply with regulatory requirements governing their use of models.[54] Consequently, banks review the models that underlie automated technologies closely, including to monitor model performance, adjust or revise models over time, and supplement model results with other analysis and information as needed.[55] Federal regulators also continue to monitor financial institutions' use of artificial intelligence as part of ongoing risk-based supervision, with an eye towards ensuring that financial institutions use automation in a "safe and sound manner" and in compliance with applicable laws and regulations.[56] The financial regulatory agencies have specifically indicated that they will review banks' use of automated data in credit underwriting, and that they expect robust compliance management of consumer compliance risk, including appropriate testing, monitoring and controls.[57] Thus, the federal financial regulators have made clear that they will continue to address banks' use of automated decisionmaking as needed.

b. Recommendations: Exemption & Interoperability

In order to avoid duplication and ambiguity related to these existing requirements, BPI urges the Agency to exempt federally-regulated financial institutions from the CCPA's requirements related to profiling and automated decisionmaking. In the alternative, it is important that the rules be interoperable with the existing framework and narrowly circumscribed, so that they do not inadvertently restrict banks and other financial institutions' ability to use automation for important public policy purposes.[58]

Among other important limits: such rules should make clear that any new opt out rights do not extend either where (1) there is the involvement of a human in decisionmaking, or (2) the outcome does not result in legal or other similar detriment to the consumer.[59] In addition, there should be an exemption for automation that is used in furtherance of regulatory compliance goals or for security and fraud-

---

[54] *See* OCC Bulletin 11-12: Supervisory Guidance on Model Risk Management; Board SR Letter 11-7: Guidance on Model Risk Management.

[55] *See* OCC Bulletin 11-12 at 4.

[56] *See* OCC et al., Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning, 86 Fed. Reg. 16837, 16840 (March 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence; Testimony of Kevin Greenfield, Deputy Comptroller for Operational Risk Policy, OCC, before the Task Force on Artificial Intelligence, U.S. House of Representatives Committee on Financial Services.

[57] BOARD, CFPB, FDIC, NCUA, AND OCC, INTERAGENCY STATEMENT ON THE USE OF ALTERNATIVE DATA IN CREDIT UNDERWRITING (2019), https://www.occ.gov/news-issuances/news-releases/2019/nr-ia-2019-142a.pdf.

[58] The Agency should be aware of both the requirements described above and of other emerging voluntary frameworks that banks and other institutions may look toward, such as the new NIST AI Framework, which includes guidance on explainability, transparency, and trustworthiness. *See* NIST, ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0), at 12–17 and 29–30 (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[59] This would mirror the GDPR, as well as aligning with other state privacy laws that restrict only profiling "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Va. Code Ann. § 59.1-473(A)(5); Colo. Rev. Stat. § 6-1-1306(1)(a)(I)(c).

prevention purposes by financial institutions and their service providers.[60] There should also be an explicit exemption from any access requirements for a business's trade secrets, confidential or proprietary information, or any other intellectual property or corporate or technological information that is confidential, proprietary, or otherwise restricted from public disclosure.

A contrary result could limit the ability of banks and other financial institutions to use automation in various ways that further important public policy goals, including to detect suspicious transactions and fight against financial crimes, such as fraud, bribery, money laundering, and terrorist financing.[61] For example, banks use automation to identify and report identity theft and suspicious money laundering and terrorist financing activities; prevent parties that are subject to economic sanctions from accessing the U.S. banking system; review payment card transactions to identify and prevent fraud and complete chargebacks for challenged transactions; apply lending standards; and alert customers to account overdraft risk. Banks may also use artificial intelligence to increase access to credit for those who may not be able to obtain credit in the mainstream credit system, as well as to generally increase efficiency, such as in processing of ACH transactions or credit applications, and thus lower costs for consumers.[62] Automated decisionmaking is essential to these activities, given the vast universe of payment and customer data at issue.

*****

The Bank Policy Institute appreciates the opportunity to submit these preliminary comments to the California Privacy Protection Agency on the proposed rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking under the California Consumer Privacy Act, as amended by the California Privacy Rights Act. If you have any questions, please contact the undersigned by phone at [redacted] or by email at [redacted]

Respectfully submitted,

/s/ Tabitha Edgens

Tabitha Edgens
Senior Vice President
Senior Associate General Counsel
Bank Policy Institute

---

[60] The Agency could consider building on existing language in the state privacy laws for this exemption, such as: "A business shall not be required to honor the rights addressed in this subsection if doing so would restrict the business's ability to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action." *See* Va. Code Ann. § 59.1-578(A)(7); *see also* Cal. Civ. Code § 1798.140(ac).

[61] *See, e.g.,* 31 U.S.C. § 5311 *et seq.*; 12 U.S.C. § 95 and 50 U.S.C. § 4301 *et seq.*; 50 U.S.C. § 1701; and 18 U.S.C. §§ 1956, 1957. These activities are often expressly sanctioned and expected by the banking regulators. *See* BOARD ET AL., JOINT STATEMENT ON INNOVATIVE EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING (2018), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20181203a1.pdf.

[62] *See* BOARD, CFPB, FDIC, NCUA, AND OCC, INTERAGENCY STATEMENT ON THE USE OF ALTERNATIVE DATA IN CREDIT UNDERWRITING (2019).

From: Dylan Hoffman [redacted]
Sent: Monday, March 27, 2023 12:02 PM
To: Regulations
Cc: Lia Nitake
Subject: PR 02-2023
Attachments: FINAL TechNet Preliminary Rulemaking Comments-Audits, Risk Assessments, ADS.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Hi,

Please find TechNet's comments on the Preliminary Rulemaking on Cybersecurity Audits, Risk Assessments, and ADS attached. Let me know if you have any questions.

Best,

--
Dylan Hoffman
Executive Director | California & the Southwest
TechNet | The Voice of the Innovation Economy
(c) [redacted] | [redacted]
Twitter: @TechNetSouthwest

TechNet Southwest | Telephone 505.402.5738
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PRELIMINARY COMMENTS ON PROPOSED RULEMAKING: CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISION-MAKING

Dear Board Members,

TechNet appreciates the opportunity to provide the California Privacy Protection Agency ("CPPA/the Agency") preliminary comments on its Proposed Rulemaking pertaining to Cybersecurity Audits, Risk Assessments, and Automated Decision-making. We believe these comments will help to enhance interoperability across state lines for compliance purposes.

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from revolutionary start-ups to some of the most recognizable companies in the world. TechNet represents over five million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

Cybersecurity Audits

Existing Legal Mechanisms, Practices, or Frameworks

First and foremost, any new requirements via the rulemaking process should be risk-based and consistent with California's existing data security requirements, as established in Cal. Civ. Code. § 1798.81.5. This permits businesses to appropriately leverage existing cybersecurity parameters, and avoids contradictory requirements within California.

Businesses should be able to conduct internal audits, as many businesses already have internal audit mechanisms using appropriate industry standards and they should be able to leverage those existing processes to meet CPRA requirements. A company's internal audit can be independent and thorough if certain requirements are met, such as the audit team is comprised of independent objective experts; the audit team works with the team that implements the controls and processes being audited, supervised by an independent leadership committee at the Company such

as the Board of Directors; and audit findings and needed remediation are reported to leadership of the impacted business unit and to other necessary company leaders to ensure deficiencies are remedied.

Notably, California law already contemplates that internal audits can be thorough and independent. *See* Cal. Ins. Code. § 900.3.

Additionally, many businesses may also already perform certain industry standard audits and reports, and they should be able to leverage these certifications to meet the CPRA audit requirement in a manner that is less onerous than a separate third-party or internal audit.

Cybersecurity audits should accept cybersecurity programs that reasonably conform to the current version of any of the following or any combination of the following: the ISO 27000 series certification, NIST Framework for Critical Infrastructure Cybersecurity, NIST special publications 800-53 and 800-53a, NIST special publication 800-171, the Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework, the Center for Internet Security Critical Security Controls for Effective Cyber Defense, the annual Payment Card Industry merchant certification, CIS 20 Controls, Service Organization Control audits by internal and third parties, and security programs established pursuant to consent decrees with regulators such as the FCC or FTC. Businesses should be able to re-use such audits/certifications rather than duplicate their efforts, which would unduly add to the cost and burden of compliance.

Further, businesses should be permitted to use certifications and audits related to cybersecurity from service providers, such as those in the cloud computing space, to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

<u>Reliance on Existing Audits</u>

Some existing laws allow businesses to submit an annual self-certification that the required audit has occurred. The Agency should adopt a similar regulation and allow annual self-certification to the Agency. Further, if the processing that creates a significant risk (as eventually defined by the regulation) is already the subject of another audit (e.g. PCI or SOX), then the existing audit should suffice for the purposes of the CPRA regulations.

Businesses should also be given the option (as an alternative, not as the sole requirement) to submit proof of a certification to a standard or framework such as PCI-DSS, the APEC Cross-Border Privacy Rules ("CBPR") System, the Privacy Recognition for Processors system ("PRP"), NIST Cyber Security Framework, or ISO 27001 that demonstrates their compliance with this requirement.

Businesses may already perform certain industry standard audits and reports. For example, storage of payment cards on file is regulated in the industry by the PCI-

DSS standards and merchants are required to re-certify to their compliance with it every year. In those circumstances, businesses should be able to re-use such audits/certifications rather than duplicate their efforts, which would unduly add to the cost and burden of compliance.

Businesses should be permitted to use certifications and audits related to cybersecurity from service providers to help meet their requirements to conduct cybersecurity audits and provide risk assessments.

Processes for Independent and Thorough Audits

The Agency should allow companies to rely on reasonable industry standards. To ensure that audits are independent, companies should also be permitted to rely on internal bodies that have safeguards to ensure that they are independent.

As noted above, businesses should be able to conduct self-audits, as many businesses already have self-audit mechanisms using appropriate industry standards and they should be able to leverage those existing processes to meet CPRA requirements. Notably, California law already contemplates that self-audits can be thorough and independent in the insurance context. *See* Cal. Ins. Code. § 900.3. Moreover, third-party audits are burdensome and expensive, making a mandate inappropriate as the burden and expense would be disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs.

Additionally, many businesses may also already perform certain industry standard audits and reports, and they should be able to leverage these certifications to meet the CPRA audit requirement in a manner that is less onerous than a separate third-party or internal audit. Existing certifications that are robust and rigorous include: the ISO 27000 series certification, the NIST Cybersecurity Framework, the annual Payment Card Industry merchant certification, CIS 20 Controls, and Service Organization Control audits by internal and third parties. Businesses should be able to re-use such audits/certifications rather than duplicate their efforts, which would unduly add to the cost and burden of compliance.

Other Considerations

The Agency should clearly define what type of processing creates a significant risk, preferably by limiting the types of personal information to which the audit requirement applies. Other sector-specific laws that require similar audit are limited to specific types of personal information such as payments data. For large businesses, conducting such an audit for lower risk personal information that do not require such audits under other laws would create significant expense with little benefit to consumers.

Many businesses already have self-audit mechanisms and other internal standards and protocols based on appropriate industry standards. And larger businesses have

internal teams that exist solely to conduct audits and that are separate from the first-line teams that are actually implementing security controls. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates. These teams are designed to be thorough and independent. Businesses should be able to leverage those existing processes to meet CPRA requirements.

Businesses should not be required to use third party auditors as the burden and expense would be disproportionate to any downstream consumer benefit. Paradoxically, third-party audits may also present a security risk, as they may expose a business's confidential security practices and (depending on the nature of the audit) potentially also underlying data to one or more third parties.

Risk Assessments

We encourage the CPPA to be guided by two principles when developing rules for risk assessments: (1) Privacy standards should be consistent across state lines, and (2) the CPRA directs the Agency to cooperate with other states to ensure a consistent application of privacy protections. As such, we suggest aligning any data impact or risk assessments aligned with other laws that will come into effect in 2023, such as the Virginia Consumer Data Protection Act's (VCDPA) and the Colorado Privacy Act's Data Impact Assessment.

There should be a consistent standard for assessing what constitutes a significant risk across state lines to allow for businesses to continue to build robust processes to protect consumers' information.

In determining what constitutes 'significant risk,' regulators should look at the security and data governance practices that companies have implemented. Almost all online businesses (and many offline businesses) today "process personal information," so we should go beyond just checking to see whether that information is processed, and instead ask how it is processed and what steps are being taken to mitigate any risk to that information.

The scope of the risk assessment should be determined by a privacy risk perspective – this provision should be limited to high-risk processing that has a legal or similarly significant effect on an individual- i.e. where the impact will produce a decision that will impact housing, education, employment and other areas where laws protect individuals from unlawful discrimination.

Any processing of personal information that do not pose the above risks should not be included in the audit and risk assessment requirements, particularly the processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or to otherwise comply with legal obligations should be exempted from the scope of this definition/regulation. These activities

protect consumers' privacy and security and should be kept confidential to prevent bad actors from gaining insight into our internal systems.

Identifying Significant Risks

From a privacy risk perspective, risk assessments should be limited to processing that has a legal or similarly significant effect on an individual, i.e. where it materially affects a decision that will impact housing, education, employment and other areas protected from discrimination under the law. This should exclude incidental processing of personal data that is not a primary factor in the decision that has the legal or similarly significant effect, such as processing to fulfill a business's legal or contractual obligations, maintain operations such as fraud detection and cybersecurity, and processing as permitted or required by law. Additional data protection measures, such as pseudonymizing or encrypting the relevant data, can meaningfully reduce the risk of processing.

From a security risk perspective, risk assessments should be limited to processing of data that, if compromised, is likely to result in real, concrete harms to individuals. Examples may include identity theft/fraud, extortion, or physical injury from disclosure of intimate or other objectively sensitive personal details (e.g., sexual orientation).

Processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or to otherwise comply with legal obligations should be exempted from the scope of this definition/regulation. These activities protect consumers' privacy and security and we keep such activities confidential to prevent bad actors from gaining insight into our internal systems.

Further, it is worth noting that the definition of 'significant risk' can also vary based on an organization's risk tolerance. This is particularly true for vendors or service providers, as different parties may have different risk tolerances and thereby categorize a technology differently. If all impact assessments are submitted to the Agency, service providers and vendors will want to make sure their assessments align with the assessments of their clients.

Content of Risk Assessments

Risk assessments should be detailed enough for the business and the regulator to appreciate the risk. However, it should not be overly prescriptive or specific. This will allow businesses to retain flexibility and scale existing processes, in particular where a wide variety of factors may apply.

The Agency should consider a similar approach as the EU's Article 29 Data Protection Working Group Report (2017):

> "*The GDPR provides data controllers with flexibility to determine the precise structure and form of the DPIA in order to allow for this to fit*

with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, whatever its form, a DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them."

The risk assessment should be viewed as a documentation requirement, and not a substantive requirement that the company must mitigate or fix any identified risk. The risk assessment should also be limited to the actual processing of data—it should not be used as a proxy to require a risk assessment of the feature itself as distinct from any processing of data that occurs as part of that feature. Finally, the Agency should permit a single risk assessment to cover multiple related types of data processing activities.

Reliance on Other Data Protection Impact Assessments

The regulations should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. In order to promote interoperability and minimize burdens to covered businesses, the regulations should specify that the Agency will accept risk assessments that were originally conducted pursuant to a comparable legal requirement.

Privacy obligations and risk balancing should be consistent across jurisdictions relating to the same requirements. As such, we suggest aligning with any data impact or risk assessments required under other similar laws, such as the CPA and VCDPA. However, the Agency should be wary of adopting in full any future regulatory guidance under other laws, including the GDPR. EU case law is evolving in unpredictable ways, and California should develop guardrails that would ensure that any future obligations on California businesses are appropriately balanced against any potential burden.

A consistent standard across jurisdictions would allow businesses to continue to build robust systems to protect consumers information. These systems will benefit from clear guidelines that allow businesses to innovate and develop their data protection assessments and properly assess their cybersecurity risks.

Submitting Risk Assessments

The regulations recognize that single risk assessment may address a comparable set of processing operations and may encompass the business's privacy program as a whole. With respect to (a)(i), a risk assessment should highlight the most significant privacy risks. They should not require the company to divulge commercially sensitive information or sensitive security information, such as details about how technical safeguards that would allow a bad actor to compromise the company's security practices.

With respect to (a)(ii), the Agency should not overly prescribe the format in which the business must submit the risk assessment. Businesses may prepare and record assessments in different ways and in response to different jurisdictions, and so they should retain flexibility to submit the assessment without needing to alter the format or content to match California-specific requirements. An example of an overly-prescriptive format would be if the Agency mandated that a business submit the required information via a webform with answer bubbles that needed to be manually populated.

With respect to (a)(iii), the regulations should not require organizations to repeatedly conduct or submit risk assessments for processing activities that have not materially changed and that pose no new or heightened risks. Such a requirement would be operationally burdensome, particularly for small and medium sized businesses, and could incentivize businesses to treat risk assessments as a mere 'check-the-box' compliance exercise. Therefore, the Agency's regulations should specify that businesses are only required to "regularly submit" assessments for new or materially changed processing practices that present a significant risk. If the Agency requires periodic updates absent any change, then such updates should not occur more frequently than once every three years.

Other Considerations

In providing guidance for conducting risk assessments and weighing the benefits of processing against potential risks, the regulations should provide that the factors relevant to this balancing may include: technical and organizational measures and safeguards implemented by the business to mitigate privacy and security risks; the reasonable expectations of consumers; and the context of the processing with respect to the relationship between the business and consumers.

The regulations should also include protections to ensure that businesses have the necessary confidence to use risk assessments to fully document and assess processing practices, and are not incentivized to treat their assessments as a defensive measure against potential future litigation. Therefore, in addition to the important carve out for trade secrets, the regulations should clarify that risk assessments conducted pursuant to the CPRA are confidential and exempt from public inspection and copying under the California Public Records Act and that submitting an assessment to the Agency does not constitute a waiver of any attorney-client privilege or work-product protection. The Agency should also not be permitted to use the submitted assessment as evidence of wrongdoing or used to penalize the business for weighing the risks in a way with which the Agency disagrees.

Automated Decision-making

Existing Legal Mechanisms, Practices, or Frameworks

The Agency should consider that as companies adopt automated tools to streamline business processes, existing legal frameworks such as anti-discrimination laws) will apply to both automated decision-making (ADM) and traditional approaches alike.

With respect to laws targeted solely to automated decision-making, companies in the US are subject to several existing (or enacted but not yet effective) privacy laws that already impose substantial obligations with respect to the consumer right to opt out of automated decision-making. This includes the Colorado, Connecticut, and Virginia state privacy laws. Critically, each of these laws is limited to high risk decisions, described as those which have "legal or similarly significant effects," and in the case of Connecticut, target "solely" automated decisions.

To ensure interoperability with those laws and to strike the right balance between protecting consumers while enabling access to important technology, the Agency should likewise confirm through rulemaking that the profiling opt out (1) applies only to decisions with "legal or similarly significant effect", (2) is limited to solely or fully automated decisions, and (3) applies only after an automated decision is made.

Regarding significant and high-risk decisions, the Agency should not create an overly broad opt-out right that would include low risk automated decisions, such as spell check, GPS systems, databases, spreadsheets, or transcription services. Requiring businesses to provide opt outs for such low-risk technology could slow down their activities substantially, while not providing a meaningful benefit to consumers, who should expect that business activities are performed using well-accepted, widely used technology. Moreover, without a carefully tailored opt-out , there could be significant impacts to many business's integrity and security efforts that rely on automated systems to streamline processes for accuracy and efficiency.

Regulators should instead focus on high-risk use cases, such as using technology to make final decisions of significance to individuals, such as regarding access to housing, medical benefits, or other critical services without appropriate human involvement. For example, under the Virginia privacy law, the consumer's right to opt out of profiling is restricted to "[d]ecisions that produce legal or similarly significant effects concerning a consumer." This is defined as "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water." The CPPA should similarly limit the opt-out right to those categories.

The opt-out right should be limited to fully-automated decisions and only to final decisions.

Companies should be able to efficiently rely on automated processes that do not lead to a final decision on an individual, such as by setting rules and thresholds to

parse large amounts of data that a human would not be able to process in time. This capacity helps companies quickly identify and triage initial risks so that the human decision-maker down the line can be presented with the necessary information to review. Non-final decisions, such as fraud flags, require automation to accommodate high volumes of transactions.

For example, individuals receive faster access to services if businesses can quickly identify low fraud risks. This is only possible at scale using either simple algorithms – e.g., approve transaction with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use manual review to make final decisions, for example through an appeals process. In these situations, if non-final decisions – e.g., cases flagged only by algorithms for further human review – are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.

While such a pre-decisional requirement will result in higher costs and slower service times, it would not provide consumers with any benefits beyond those that a post-decisional opt-out would provide. For example, if individuals apply for a loan and have a positive outcome on the first automated decision, which might take just a few seconds to be issued, they likely will not want or need to opt-out and request review (but they would still have the right to). Even if they have a negative outcome (again, which they might know in just a few seconds), they will still be able to exercise the right to contest that decision and have a human issuing a new decision. If laws force companies to have the opt-out even before a decision is made, the experience could take several days and without any actual gain for customers, because the decision will be issued by the same person they already had access to in the first example.

Practically speaking, companies do not typically have requirements, frameworks, or best practices that address access/opt outs related to low-risk, every day technology, even those that arguably make automated decisions (for example, spellcheck correcting a typo in the user's name). Access or opt out rights for this type of automation would slow down businesses substantially with no benefit to consumers. For example, businesses do not typically give consumers the right to opt out of using optical character recognition on PDF documents containing that consumer's personal information. Or, they do not give consumers the right to opt out of having their information stored in an internal database that automatically sorts information alphabetically, and instead demand handwritten records be stored and sorted manually. Regulations should not lead to dictating how businesses use (or don't use) everyday, low-risk technology.

However, to the extent that artificial intelligence or machine learning is used in high-risk automated decision-making, that is an area where there are robust requirements, frameworks, and best practices are continually being developed and deployed.

In recent years there has been a proliferation of artificial intelligence or machine learning international standards, such as those created by the International Organization for Standardization (ISO) and the U.S. National Institute of Standards and Technology (NIST). In January 2023, NIST released an Artificial Intelligence Risk Management Framework, a set of guidance for organizations designing, developing, deploying or using AI systems to help manage risk. Among many other measures, this framework discusses transparency, human oversight, and appealing system outcomes. Many companies are focused on the responsible use of this technology and where useful and meaningful to mitigate risk, companies have provided consumers and the public with information or guidance on technology that may be related to automated decisions.

Regarding existing definitions, automated decision-making technology is not a universally defined term and could encompass a wide range of technology that has been broadly used for many decades, including spreadsheets and nearly all forms of software. We caution against overly broad regulation of a broad category of technology that would impede the use of socially beneficial, low-risk, and widely accepted tools, to the significant detriment of both California consumers and businesses. Every day technology like calculators, word processing software, and scantron machines could be considered automated decision-making technology. Even newer and more complex automated decision-making technology, like artificial intelligence, is used routinely in business and includes things like email spam filters and autocorrect features.

To avoid a sweeping definition that captures all technology or software, policymakers should focus on automated decision-making that uses machine learning to fully automate decisions that produce legal or similarly significant effects. Machine learning is the type of technology that generally implicate transparency, bias, and explainability considerations.

Accordingly, automated decision-making should be defined as "final decisions that are made solely or fully with machine learning technology with legal or similarly significant effects," and "legal or similarly significant effects" should be defined as: "decision made by the business that results in the provision or denial by the business of financial and lending services, housing, insurance, education enrollment, criminal justice, health care services, or access to basic necessities, such as food and water."

Business Uses of Automated Decision-making

Businesses in every industry sector use ADM to improve their competitiveness and enhance their product and service offerings, including routine and low-risk applications such as spellcheck and tabulations. For instance, algorithms may be used to recommend a book or song, or allow a small business to market its products to the right consumers at affordable prices.

With respect to artificial intelligence and machine learning, it is important to note that the adoption of AI across industries is now so widespread that a 2021 McKinsey and Company study[1] found that 56% of business leaders across the globe now report using AI in at least one business function. The McKinsey report highlights that the most common AI use cases are low risk, involving service-operations optimization, AI-based enhancement of products, and contact-center automation.

Consumer Use of Automated Decision-making

Automated technology has significant benefits to both businesses and consumers, including enhanced accuracy and consistency, safer and more innovative products, scalability, cost savings, and increased efficiency. Accordingly, regulators should be very mindful about providing consumers any right to opt out of automated activities, as it could severely hamper businesses' and other consumers' ability to realize those advantages.

We suggest providing guardrails for consumers rather than an opt out without limitations. If high risk business offerings are essential or critical, and it is not reasonable for consumers to consider other options, businesses should have the ability to demonstrate the existence of operational guardrails instead of providing for an opt out. Depending on the specifics of the use case, appropriate guardrails could include things like significant, rigorous testing; corroboration of results; system monitoring; and providing an appeals or complaint process.

There should also be different considerations when automation is the offered service or product. Automation may be core to certain products or services, making opt-outs infeasible. Automated fraud detection that prevents unauthorized transactions and identity theft is a critical example where the benefits of timely action outweigh a potential opt-out. In these instances, businesses should have the ability to demonstrate the existence of operational guardrails that protect California consumers' interests instead of providing for an opt out.

Automation may also be essential to products that involve less significant effects, but which nonetheless provide high value with minimal risk to consumers. Examples include 1) Calendars that provide you with updated travel times based on traffic patterns from your current location; 2) voice services that improve understanding and performance based on interaction history (e.g., when you ask to "play Rush," you mean the band, not the pundit); 3) robots that learn what your stairs look like so they don't fall down them. Companies shouldn't have to design objectively worse (and potentially even dangerous) versions of their products and services merely to give customers a right to opt out of ADM. To avoid unnecessary interruption to consumer enjoyment of these products and services, the Agency

[1] Available at https://www.mckinsey.com/capabilities/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021

should follow the approach of other US state privacy laws and limit the profiling opt out to automation that has legal or similarly significant effects.

The Agency should also consider that providing an opt-out option may create significant risks in some cases. The regulations should recognize that some uses of automated decision-making that produce legal or similarly significant effects may be highly beneficial to consumers—and if turned off, creates the risk of potential harm. The statute did not intend for consumers to be able to opt out of these uses.

For example:

- a health-care system that uses an individual's address to select the closest ambulance dispatch location; or
- fraud detection and related activities in making financial or insurance decisions.

To protect California consumers' interests without burdening beneficial uses, the regulations should tailor the scope of "legal or similarly significant effects" to the harms regulators seek to protect against (e.g., discrimination against protected classes in access to housing or credit). And as noted above, the regulations should permit operational guardrails rather than requiring an opt out.

Opt-out Right to Address Bias

Businesses should be allowed to use race/ethnicity and other demographic data for the narrow purpose of evaluating and preventing bias. Regulators should consider a safe harbor for businesses that are trying to prevent bias. It's not possible to prevent bias without measuring the algorithm's impact on different user groups, including minority groups.

Variance of Access and Opt-out Rights

Access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling, should vary depending upon the circumstances. Given the vast use cases for automated decision-making technology and profiling, the Agency should largely defer to sector-specific regulatory schemes that take into account the industry that is using the technology, the technology being used, the type of consumer to whom the technology is being applied, the sensitivity of the personal information being used, and the situation in which the decision is being made to address any concerns about use of this technology. For example, the risks, concerns, and benefits from using an AI translation service differ significantly from developing and using self-driving cars, which also differ significantly from use of AI medical software. From a policy and regulatory perspective, each of these areas are best addressed through a specific examination of the sector in question. To the extent the Agency does promulgate rules in this space, it should consider the parameters set out in the above section on existing legal mechanisms, practices, or frameworks.

Yet some use cases raise additional concerns about permitting an opt-out right even for high-risk service offerings. For example, an in-car safety system that automatically senses a crash and immediately connects a driver with assistance shouldn't be required to provide a consumer with an additional manual process that conducts the same task – that would defeat the purpose of the automated service.

The regulations should also recognize that some uses of automated decision-making that produce legal or similarly significant effects may be highly beneficial to consumers—and if turned off, creates the risk of potential harm, as noted above.

Finally, the Agency should recognize the ADM benefits of reducing the need for human review, in particular where such review may lead to (i) human error in processing, (ii) risk of improper disclosure, review, or dissemination of consumer personal data, and (iii) bias.

Employee and B2B Data

The profiling opt out should exclude automation involving individual data in the employment and commercial contexts. With respect to the employment context: First, there are developing state and local laws that already specifically target the use of these technologies in the workplace, so California should let that regulatory activity run its course. Second, those laws are being tailored to the nuances of an employment context and, recognizing the potential unreasonableness of requiring specific opt-outs for every instance of automated decision-making, are mainly focused on transparency and human review.

Access Requests

Businesses should be able to fulfill consumer access requests by providing a general explanation of technology functionality, rather than information on specific decisions made. Businesses should be able to provide this information via a publicly available disclosure on their webpage.

In order to provide "meaningful" information about the logic involved in a decision, businesses should be permitted to provide a description of the general criteria or categories of inputs used in reaching a decision or categories of decisions. For example, if a rental company considers certain personal information when evaluating a housing application, those categories of information could be described.

A more detailed description of any complex algorithms involved in automated decision-making will not provide the average consumer with a "meaningful" information on the logic involved in the processing. In addition, providing a detailed explanation of the algorithms involved runs the risk of imposing obligations that conflict with the intellectual property, trade secret, and other legal rights of the business in question. With respect to fraud or security decision-making, disclosures could instruct fraudsters or bad actors on circumventing the system.

Any regulation should also ensure that businesses are protected from disclosing proprietary information, such as that which is subject to intellectual property or trade secret protection, in response to consumer access requests.

Additional Processes for Access and Opt-Out Rights

Any regulations should distinguish between the role of automated decision technology developers (companies that design and develop the technology) versus deployers (companies that deploy the technology out in the world and with consumers). Regulations should clarify that developers do not have any standalone obligations with regard to consumer access requests or opt-outs, but only an obligation to provide "reasonable" assistance to deployers, which could, among other things, be provided in the form of generally available documentation.

Any regulations around automated decision-making need necessary exceptions to access/opt out to avoid abuse (as is already the case in Colorado, Connecticut, and Virginia). For example:

- Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action.
- Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may be illegal.
- Provide a product or service a consumer requested or perform a contract with the consumer.
- Take immediate steps to protect an interest that is essential for the life of the consumer or another natural person, if the processing cannot be manifestly based on another legal basis.
- Process personal data for reasons of public interest in the area of public health, subject to certain conditions.
- Conduct internal research.
- Fix technical errors.
- Perform internal operations that are consistent with the consumer's expectations.

We appreciate your consideration of these critically important delineations. As privacy laws proliferate throughout the United States, it is even more critical to enhance the clarity and interoperability of laws and regulations that will allow companies to comply to the requirements set out by various locales. We believe the comments outlined above balance industry operability not only with the CPRA, but with existing omnibus privacy legislation throughout the world. If you have any questions regarding our comments, please contact Dylan Hoffman at [redacted] or [redacted].

TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

Sincerely,

[redacted]

Dylan Hoffman
Executive Director for California and the Southwest
TechNet

From: Notari, Melanie A. [redacted]
Sent: Monday, March 27, 2023 12:11 PM
To: Regulations
Cc: Kagan, Odia
Subject: PR 02-2023
Attachments: CCPA New Regs comments(144094726.1)-C.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Hello,

Please find attached comments in response to the Agency's invitation for preliminary comments on proposed rulemaking cybersecurity audits, risk assessments, and automated decisionmaking. No hard copy will follow unless requested.

Thank you in advance for your consideration.

Melanie Notari (she/her/hers)
Associate
Fox Rothschild LLP
1001 Fourth Ave.
Suite 4400
Seattle, WA 98154-1065
[redacted]
(206) 389-1708 – fax
[redacted]
www.foxrothschild.com

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

To whom it may concern,

On behalf of our client, Anonos[1], we are pleased to submit comments to the "Invitation for preliminary comments on proposed rulemaking cybersecurity audits, risk assessments, and automated decisionmaking" specifically on the issue of pseudonymization and its significance with respect to deidentification.

In short, Anonos recommends that the California Privacy Protection Agency ("Agency") take the following into account when drafting regulations on cybersecurity audits, risk assessments, and automated decisionmaking:

- Pseudonymization (and specifically Statutory Pseudonymization as defined by the EDPB and explained below), deidentification, and encryption should be listed as additional safeguards for the protection of personal information that can be implemented as part of risk assessments, as is already done in other jurisdictions.
- Pseudonymization should be listed as one of the Agency's suggested cybersecurity measures for reasonably protecting personal information and should be an important factor in cybersecurity audits due to its potential to mitigate harmful effects of a data breach.

Below is a more detailed discussion of each of these points:

Risk assessments (aka data protection impact assessments) should take "Statutory Pseudonymization" requirements into account as done in EU and in Colorado:

The GDPR refers to pseudonymization as an appropriate data protection safeguard in many circumstances. For example, the GDPR recognizes that pseudonymization may be an appropriate safeguard where a business seeks to determine whether processing for another purpose is

[1] Anonos Inc. ("Anonos", see https://www.anonos.com) is a U.S. company organized under the laws of Delaware. Anonos and its affiliates hold 26 granted domestic and international patents on de-identification, anonymization, and pseudonymization: Patent Nos. CN ZL201880044101.5 (2022); JP 7,064,576 (2022); CA 3,061,638 (2022); AU 2018258656 (2021); US 11,030,341 (2021); EU 3,063,691 – Austria, Belgium, Croatia, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Switzerland and United Kingdom (2020); CA 2,975,441 (2020); US 10,572,684 (2020); CA 2,929,269 (2019); US 10,043,035 (2018); US 9,619,669 (2017); US 9,361,481 (2016); US 9,129,133 (2015); US 9,087,216 (2015); and US 9,087,215 (2015); plus 70+ additional domestic and international patent assets.

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

compatible with the purpose for which the data was initially collected.[2] This is because pseudonymized data is lower risk data than non-pseudonymized data. Companies who hold vast amounts of pseudonymized data are less likely to cause harm to consumers in the event of a data breach. Anonos recommends the Agency issue regulations listing pseudonymization as a cybersecurity auditing measure utilizing the EDPB's current Statutory Pseudonymization framework.

New U.S. state privacy laws in Colorado, Virginia, Utah, Connecticut, as well as the California Privacy Rights Act ("CPRA"), all include a definition of the term "pseudonymization."[3] Article 4(5) of the EU General Data Protection Regulation ("GDPR") was the first time pseudonymization was defined under EU law. This EU definition was carried over verbatim in these U.S. state privacy laws. All of these laws contain three definitional requirements for Statutory Pseudonymization: (1) the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, (2) storing such additional information separately and (3) imposing technical and organizational measures on such information to ensure that the personal data are not attributed to an identified or identifiable natural person.[4] But the definition of pseudonymization has evolved since the GDPR was originally enacted.

The European Data Protection Board ("EDPB") recently provided further guidance on the requirements for Statutory Pseudonymization in the context of complying with requirements for lawful international transfer of EU personal data to the United States. While pseudonymization was previously understood to generally refer to replacing direct identifiers with tokens for individual fields independently within a data set, the EDPB Recommendations 01/2020 for lawful international data transfers[5] make it clear that Statutory Pseudonymization now requires all of the following:

---

[2] Art. 6 GDPR.
[3] *See* Cal. Civ. Code § 1798.140 (aa); VA Code Ann. § 59.1-571; Colo. Rev. Stat. § 6-1-1303; Utah Code Ann. § 13-61-101(28); Conn. Pub. Acts No. 22-15 5 of 27.
[4] *See* Cal. Civ. Code § 1798.140 (aa).
[5] *See* EDPB Recommendations on Measures that Supplement Transfer Tools at Use Case 2: Transfer of Pseudonymised Data (pp. 31-32) at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf ("EDPB Recommendations")

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

- **Protecting all data elements**: Footnotes 83 and 84 of the EDPB Recommendations 01/2020, which echo the GDPR definition of pseudonymization, highlight that achieving Statutory Pseudonymization status must be evaluated for a data set as a whole, not just particular fields.[6] This requires assessing the degree of protection for all data elements in a data set, including more than direct identifiers, extending to indirect identifiers and attributes. This is underscored by the definition of "Personal Data" under EU GDPR Article 4(1) as more than immediately identifying information and extending to "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[7] CPRA contains similar, equally broad, definitions for personal information: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[8]

- **Protecting against singling out attacks**: Paragraph 85 of the EDPB Recommendations 01/2020 mandates protection against "singling out" of a data subject in a larger group effectively making the use of either k-anonymity or aggregation mandatory.[9]

- **Dynamism**: complying with the requirements in Paragraphs 79, 85, 86, 87 and 88 of the EDPB Recommendations 01/2020 to protect against the use of information from different datasets to re-identify data subjects may necessitate the use for differing purposes of different replacement tokens at different times (i.e. dynamism) to prevent re-identification by leveraging correlations among data sets without access to the "additional information held separately" by the EU data controller;[10]

- **Non-algorithmic lookup tables**: Paragraph 89 of the EDPB's Recommendations 01/2020 requirement to consider the vulnerability of cryptographic techniques (particularly over

[6] *Id*. at p. 31.
[7] Art. 4 GDPR (1) at https://gdpr-info.eu/art-4-gdpr/,
[8] Cal. Civ. Code § 1798.140 (v)
[9] *See* EDPB Recommendations at p. 31.
[10] *See* EDPB Recommendations at pp. 29, 31-32; *see also* https://www.MosaicEffect.com.

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

time) to brute force attacks and quantum computing risk may necessitate the use of non-algorithmic derived look-up tables in many instances;[11] and

- **Controlled re-linkability**: The combination of the four preceding items may be necessary to meet the requirement in Paragraph 85(1) of the EDPB Recommendations 01/2020 that, along with other requirements, the standard of EU GDPR pseudonymization can be met only if "a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information."[12]

In many cases, organizations and businesses will have to reevaluate their approach to pseudonymization to achieve Statutory Pseudonymization requirements. The extent and specificity of the technical requirements necessary to achieve Statutory Pseudonymization are often significantly underappreciated.[13]

If implemented as such, Anonos recommends that the Agency designate Statutory Pseudonymization as an important tool for risk assessments (aka "data protection impact assessments"). This is already addressed in the Colorado Privacy Act ("CPA") Rules. The rules recognize the existence of additional safeguards for personal data as a mitigating factor when controllers seek to utilize data for a secondary use.[14] They also list the use of De-identified data and compliance with controller obligations—including data minimization, retention limitation, and limited secondary uses—as measures to consider for risk reduction in a data protection impact assessment.[15] Statutory Pseudonymization assists with all these purposes. The importance of pseudonymization in data protection impact assessment is also addressed in the EDPB guidance

[11] *See* EDPB Recommendations at p. 32.
[12] EDPB Recommendations at p. 31, ¶ 85(1).
[13] *See Technical Controls That Protect Data When in Use and Prevent Misuse* by Magali Feys, Joseph W. Swanson, Patricia M. Carreiro and Gary LaFever, published in *Journal of Data Protection & Privacy,* Vol. 5 No. 3 (2022) ISSN (print) 2398-1679; ISSN (web) 2398-1687, available at Pseudonymization.com/TechnicalControls. The European Union Agency for Cybersecurity (ENISA) has also published recommendations for achieving Statutory Pseudonymisation (*e.g., see* https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions; *see also*https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices).
[14] *See* 4 CCR 904-3 ("CPA Regulations") Rule 6.08 (C)(7): https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf at p. 23.
[15] CPA Regulations Rule 8.04 7(a) ("Measures and safeguards the Controller will employ to reduce the risks identified by the Controller . . . include. . . The use of De-Identified data."); CPA Regulations Rule 8.04 7(b).

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

on Data Protection Impact Assessments ("DPIAs") which discusses using pseudonymization and encryption of personal data as examples of measures to reduce risk during a DPIA.[16]

Statutory Pseudonymization should be listed as one of the mitigating measures that can be considered as part of a cybersecurity audit

When setting parameters for cybersecurity audits, Anonos recommends that the Agency draft regulations to specifically reference Statutory Pseudonymization as one of the techniques useful in risk assessments, de-identification, and the general compliance toolbelt. Statutory Pseudonymization should be used throughout the data lifecycle when adopting a data protection by design and by default approach and, if it is, this should be considered as a mitigating factor in cybersecurity audits. This has already been recognized both under GDPR and in the EDPB guidance (see below).

Statutory Pseudonymization is a strong mitigation factor that businesses can rely on to lower the risk profile of certain data because Statutory Pseudonymization is in line with the concept of data utility. While anonymization is meant to reduce the risk of re-identification to zero, that is both not feasible most of the time and, if feasible (for example, through aggregation), much of the functionality and usability of the data is lost. On the other hand, using Statutory Pseudonymization helps to maintain the balance between the risk and the potential reward thus increasing the data's value and utility.[17] Statutory Pseudonymization can also help to reduce risk and facilitate compliance with data minimization, retention limitation, and purpose limitation.

- *Risk Mitigation*: Even pseudonymization that falls short of the legal standard for Statutory Pseudonymization still mitigates risk better than maintaining the information in a fully identified form. Using Statutory Pseudonymization is a way in which information can be maintained in re-identifiable (re-linkable) format by the business itself, while still preventing re-identification (re-linkability) by unauthorized third parties. If information is truly Statutorily Pseudonymized, even though the key holder can easily re-identify the information, third parties with whom the Statutorily Pseudonymized information is shared are not able to re-link it

[16] *See* Guidelines on Data Protection Impact Assessment (DPIA): https://ec.europa.eu/newsroom/article29/items/611236/en at p. 19).
[17] *See* data utility benefits highlighted in *Technical Controls That Protect Data When in Use and Prevent Misuse,* at Note 12.

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

without access to the information held separately and securely by the data controller or authorized designee.

- *Increased information security*: Under the GDPR, Statutory Pseudonymization is listed specifically as part of the way to ensure compliance with the Article 32 obligations to maintain adequate technical and operational measures to safeguard the data.[18] Anonos recommends that the California regulations make a similar reference. In addition, information which is Statutorily Pseudonymized is less likely to be breach reportable in the event of a data breach incident as it reduces the chance that exposure would lead to a risk to the rights or freedoms of individuals.[19] The EDPB states this in the draft guidelines on data breach: "Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) GDPR as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person') can also reduce the likelihood of individuals being identified in the event of a breach."[20] Anonos recommends that the California regulations similarly note the increased information security benefits of Statutory Pseudonymization.

- *Data minimization*: This is the requirement to collect only the identified information which you need for the purposes.[21] When personal data is Statutorily Pseudonymized, this reduces the risk profile of identified data and helps the business only retain/collect what it needs. Per the ICO guidance referenced above, Pseudonymization is a way to "make better use of data (e.g., for archiving, scientific and historical research, and statistical purposes; other compatible purposes; and general analysis)."[22] Anonos recommends that the California regulations specify Statutory Pseudonymization as one way to address data minimization.

[18] Art. 32 GDPR (1)(a) at https://gdpr-info.eu/art-32-gdpr/.
[19] *See* Art 34 GDPR (3) at https://gdpr-info.eu/art-34-gdpr/.
[20] Guidelines 9/2022 on personal data breach notification under GDPR https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf at p. 24.
[21] *See* CPRA Regulations § 7002 (d).
[22] https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf, at p. 2.

Fox Rothschild LLP
ATTORNEYS AT LAW

2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150

- *Retention limitation*: Under the CPRA, information can only be retained in an identified manner for as long as required.[23] Information which is Statutorily Pseudonymized, while still being personal information, reduces the risk profile of information which is retained. Anonos recommends that the California regulations specify Statutory Pseudonymization as one way to address retention limitation.

- *Fewer issues with "sale"/sharing*: Under the CPRA, sharing personal information in certain cases is deemed a "sale" and that subjects the disclosure to additional obligations.[24] Anonos recommends that the CPRA regulations address the fact that sharing a Statutorily Pseudonymized set, provided that the code is never shared and the recipient truly does not have the ability to re-identify, may reduce the likelihood that a sharing is a 'sale' because the information could be effectively anonymized to the recipient (while still being re-identifiable to the sharing party). It would be helpful to add guidance on the relevant factors: *e.g.* (1) the ability of the recipient to use other information to enable identification (either something in their possession, or in the public domain; (2) the likelihood of identifiability, considering things like the cost of and time required for identification and the state of technology at the time of the processing; and (3) the techniques and controls placed around the data once in the recipient's hands.

We thank you for your consideration of these comments.

Odia Kagan
Partner, Chair of GDPR Compliance and International Privacy

Fox Rothschild LLP
March 27, 2023

[23] *See* CPRA Regulation § 7002 at California Privacy Protection Agency - Final Regulations Text (pp. 6-7).
[24] Cal. Civ. Code §1798.140 (ad); CPRA Regulation §7002 (bb); CPRA Regulation §7002 (hh); CPRA Regulation §7004; CPRA Regulation §7011; CPRA Regulation §7012.

From: Allison Adey [redacted]
Sent: Monday, March 27, 2023 12:23 PM
To: Regulations
Cc: Melissa O'Toole
Subject: PR 02-2023: PIFC/NAMIC Response Letter
Attachments: PIFC_CPPA Question Responses[98].pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Good afternoon,

Attached please find the letter responding to the Department's questions regarding cybersecurity audits, risk assessment, and automated decision making on behalf of the Personal Insurance Federation of CA (PIFC) and the National Association of Mutual Insurance Companies (NAMIC).

Thank you,

Allison

Allison Adey
Legislative Advocate
Personal Insurance Federation of CA
M: [redacted]
W: www.pifc.org
E: [redacted]
1201 K Street, Suite 950
Sacramento, CA 95814

Date: March 27, 2023

To: Members, California Privacy Protection Agency

SUBJECT: RESPONSE TO QUESTIONS RELATED TO CYBERSECURITY AUDITS, RISK ASSESSMENT, AND AUTOMATED DECISION MAKING

Dear Members of the Board,

The Personal Insurance Federation of California (PIFC) is a statewide trade association that represents nine of the nation's largest property and casualty insurance companies. These companies include State Farm, Farmers, Liberty Mutual Insurance, Progressive, Mercury, Nationwide, Allstate, CONNECT by American Family Insurance and Kemper as well as associate members CHUBB, NAMIC, and Interinsurance Exchange of the Automobile Club (Automobile Club of Southern California). Collectively, these insurance companies write the majority of personal lines auto and home insurance in California.

We appreciate the opportunity to provide comments on the questions that the Consumer Privacy Protection Agency (the Agency) has posted regarding cybersecurity audits, risk assessment, and automated decision making.

As we have raised in our previously submitted comments regarding the proposed regulations, definitions continue to be an issue in these questions. Critical terms that will define compliance standards (algorithmic discrimination, profiling, automated decision making, and significant risk) require clear definitions to ensure that there is adequate notice as to their meaning.

Cybersecurity Audits

Internal audits should suffice for this requirement for companies of a certain size or with the resources to perform such audits. There are various kinds of cyber audits and risk assessments (e.g., SOC Type 1/Type 2, ISO/IEC 27000 series), as well as privacy impact assessments (PIA) and privacy risk assessments that organizations already conduct and report to their regulator. The CPPA should align their regulations to utilize what is already in existence and allow companies to leverage audits or assessments they already conduct, rather than add a new layer or new obligations (i.e., defer to the business risk assessments done in ordinary course). Furthermore, independent audits/annual audits should only be required of an entity too small to perform them on their own, or one that has been sanctioned by another regulator. Finally, to minimize the burden placed on businesses, audits should not be required annually; every 2-3 years should suffice.

2. In addition to any legally required cybersecurity audits identified in response to question 1, what other cybersecurity audits, assessments, or evaluations that are currently performed, or best practices, should the Agency consider in its regulations for CCPA's cybersecurity audits pursuant to Civ. Code § 1798.185(a)(15)(A)?
When drafting its regulations for CCPA's cybersecurity audits, the Agency should consider longstanding, nationally recognized frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and related best practice standards, such as COBIT, CIS, CSC, ISA. Compliance with such a framework or standard should be considered for a compliance safe harbor, in order to avoid conflicting or competing layers of obligations on the part of businesses subject to CCPA.

Risk Assessments

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?
The insurance industry is already subject to substantial oversight for cybersecurity and privacy in California under the California Code of Regulations 10 Section 2689.16 and 2689.17(c).

Additionally, this industry has long been subject to federal law and outside state regulations on these topics (see National Association of Insurance Commissioners (NAIC) Model Cybersecurity Law (implemented in multiple states) Sections 1.N., 4.A., 4.C., 4.D., 4.E.(2)(b), New York Codes, Rules, Regulations Title 23 Sec. 500.9).

a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in California Civil Code § 1798.185(a)(15)(B)?
Currently there is no articulated alignment between the California Code of Regulations 10 2689.16 and 2689.17(c) and California Civil Code § 1798.185(a)(15)(B) except that both are concerned with cybersecurity, risk assessment, and privacy management.

b. What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA's risk-assessments requirements (e.g., product reviews)?
Insurance companies have varied practices. Some practices that have been implemented to comply with risk assessment requirements include ongoing oversight of processing activities including supplier reviews, marketing engagements and changes to the collection and processing of consumer information.

c. What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments?
Insurers are seeking specific guidance for their industry needs, particularly in the area of high-risk processing of consumer information. Additionally, greater clarity for definitions will ensure that compliance concerns can be mitigated preemptively.

d. What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments?

The greatest concern stems from potential conflicts with multi-state jurisdictional requirements. The greater the variations between jurisdictional requirements, the larger the compliance burden on the companies.

2. What communities or individuals are more susceptible to harm from a business's data processing practices? Why are they more susceptible to harm from these data processing practices?
The insurance industry does not have a unique perspective on this question.

3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civ. Code § 1798.185(a)(15):
a. What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment (GDPR)?
The GDPR approach is comprehensive and could provide a blueprint for how to implement this requirement.

b. What other models or factors should the Agency consider?
New York and Virginia have both developed models that would be worthwhile to consider.

c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? If so, how?
Yes, a risk assessment should occur prior to the implementation or changes made to the process. Whereas an audit does, and should, occur after implementation to ensure the process is functioning correctly.

5. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?
One consideration is that different, additional, or more prescriptive burdens (including GDPR-styled requirements not applicable to many domestic insurers) on the insurance industry will not materially increase protections for consumers. Instead, such burdens may drive up operating expenses and, hence, insurance costs for consumers.

Additionally, requirements for businesses subject to CCPA should not vary by business revenue. A business with relatively little revenue could have a huge amount of personal information regarding a huge number of Californians. Less revenue might suggest that the business has devoted fewer resources to risk assessment and cybersecurity in the past, resulting in less robust, mature protections and more risk to Californians. Therefore, businesses with smaller revenues should be just as regulated as businesses with more revenue.

6. How should businesses submit risk assessments to the Agency?

a. If businesses were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business), what should these summaries include?

Businesses should only be required to submit full risk assessments to the Agency on an as needed/as requested basis (e.g., in the course of Agency investigations or enforcement proceedings). If the Agency were to require businesses to submit full risk assessments on a regular basis, the Agency risks making itself a target for threat actors who would seek to use submitted risk assessments as blueprints of attack against businesses. This defeats the intended purpose of the risk assessments. Summaries containing high level statistics (as described below in Answer 6.a) achieve the purpose of demonstrating compliance, while mitigating any potential risk associated with threat actors. Risk assessments, whether full or summary, should be treated by the Agency with the strictest of confidentiality and not be available to the general public.

b. How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk-assessment requirements (e.g., summaries signed under penalty of perjury)?

Reports and summaries would be signed under penalty of perjury, and more information/records may be made available on request.

8. What else should the Agency consider in drafting its regulations for risk assessments?

A few considerations in regard to risk assessments include:
1) Assessments should only be conducted upon a showing of need for an assessment, rather than on a scheduled basis;
2) Satisfactory cyber audits should be treated as exemptions to risk assessments;
3) Risk assessments called for by the Agency should be restricted to the information under the scope of the CCPA, CPRA, and CPPA's authority and;
4) the Agency should consider using independent experts to review the findings of any submitted assessment.

Automated Decision Making

1. What laws requiring access and/or opt-out rights in the context of automated decision making currently apply to businesses or organizations (individually or as members of specific sectors)?

Other than the enumerated rights in CCPA/CPRA, Colorado and Virginia have rights which enable consumers to opt-out of "profiling in furtherance of decisions that produce legal or similarly significant effects" concerning the consumer. Connecticut additionally provides an opt-out right similar to Colorado and Virginia, but applies "solely [to] automated decisions," aligning it more closely with the GDPR.

2. What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decision making are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

- National Institute of Science and Technology's Risk Management Framework[1]
- National Association of Insurance Commissioners AI Principles[2]
- Business Roundtable Principles for Responsible AI[3]
- Organization for Economic Cooperation and Development Framework for Classification of AI[4]

3. With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:
a. How is "automated decision making technology" defined?
Generally, it has not yet been defined. PIFC would request that as a definition is considered, that routine tasks such as routing phone calls, routing mail, or chat bot interactions not be included in the definition, given the operational burden that it would create.

b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the processes and goals articulated in Civ. Code § 1798.185(a)(16)?
It would depend on the way the final regulations interpret this Section, how terms are to be defined, and whether those definitions comport with other states' laws and regs. The Section alone is too vague.

c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decision making technology requirements?
Some have established their own risk management frameworks or governance practices, many of which will be able to assist in CCPA compliance. However, that would require that the final regulations not deviate substantially from the current requirements and systems that the companies are subject to and using. It will also require sufficient lead time to implement any new systems that are necessary.

d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decision making?
Like the concerns raised above, the industry is seeking additional guidance to ensure that they can comply in a timely manner. Specifically, they seek additional clarity regarding the lack of definitions of terms and implementation timelines. Finally, additional clarity is necessary around the use of third party/vendor models and the tension between disclosure and what these third parties/vendors require to maintain the proprietary nature of their intellectual property.

[1] https://csrc.nist.gov/projects/risk-management/about-rmf
[2] https://content.naic.org/sites/default/files/inline-files/AI%20principles%20as%20Adopted%20by%20the%20TF_0807.pdf
[3] https://s3.amazonaws.com/brt.org/Business_Roundtable_Artificial_Intelligence_Policy_Recommendations_Jan2022_1.pdf
[4] https://www.oecd-ilibrary.org/docserver/cb6d9eca-en.pdf?expires=1674861688&id=id&accname=guest&checksum=FB9AE4CD90EB80860060C03BE08E3BB4

4. How prevalent is algorithmic discrimination based upon classifications/classes protected under California or federal law (e.g., race, sex, and age)? Is such discrimination more pronounced in some sectors than others? If so, which ones?
Intentional discrimination based on a protected characteristic is prohibited under the California Unruh Act at Civil Code Section 51.

5. How can access and opt-out rights with respect to businesses' use of automated decision making technology, including profiling, address algorithmic discrimination?
The 2019 negotiations on CCPA ensured that meaningful consent was enshrined and would allow individuals to continue to access websites while utilizing the full extent of their rights under the CCPA.

6. Should access and opt-out rights with respect to businesses' use of automated decision making technology, including profiling, differ for consumers across industries and technologies? If so, how should they differ, and why?
Yes, different industries are subject to different regulatory burdens, federal laws, and engage in different types of transactions. Considerations should include whether personal information used to determine cost, product eligibility, etc., is determinative for the transaction.

7. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decision making processes and the description of the likely outcome of the process with respect to the consumer?
Necessary information that is pertinent to the transaction involved that would not implicate security or intellectual property should be included.

For insurers, the existing regulatory landscape is extensive. PIFC continues to seek clarity regarding the forthcoming regulations - particularly on the present questions. We appreciate the opportunity to provide input and feedback. Finally, we ask that the implementation burden, both time and cost, be considered as you move forward with regulations. We look forward to working collaboratively with the Agency and Board to develop fair regulations that can be implemented in a manner that best serves Californians.

Sincerely,

[redacted]

Allison Adey
Legislative Advocate
Personal Insurance Federation of California

[redacted]

Christian J. Rataj
Senior Regional Vice President
National Association of Mutual Insurance Companies

From: Jake Parker [redacted]
Sent: Monday, March 27, 2023 12:35 PM
To: Regulations
Subject: PR 02-2023
Attachments: SIA Comment PR 02-2023 03.27.2023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

See attached comments from the Security Industry Association (SIA).

Jake Parker
Senior Director, Government Relations
Security Industry Association (SIA)
[redacted]

March 27, 2023

California Privacy Protection Agency (CPPA)
Attention: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

To Whom It May Concern:

Re: Proposed Rulemaking on Cybersecurity Audits, Risk assessments, and Automated Decisionmaking (PR 02-2023)

The Security Industry Association (SIA) appreciates the opportunity to submit comments on the development of regulations to implement the statutory provisions of the California Consumer Privacy Act regarding cybersecurity audits, risk assessments and automated decisionmaking.

SIA Represents nearly 200 companies headquartered in California that provide a wide array of products essential to protecting the physical safety of people property, businesses, schools, and critical infrastructure in the state and throughout the nation. This includes access control, alarm systems, security camera systems, screening and detection equipment, and many other applications. Our member companies are deeply committed to safeguarding personal information and protecting people through their own business practices as well as the design of the products and services they provide that collect and process information.

Summary

The California Privacy Protection Agency ("CPPA" or "Agency") is seeking comments[1] as it begins the process to implement rules addressing automated decisionmaking technology under the California Privacy Rights Act of 2020 ("CPRA").[2] In considering these rules, the Agency should recognize the vast potential benefits of automated decisionmaking technologies and their ability to be used in ways that help consumers. Any rules should apply only in limited, high-risk circumstances, exclude human-involved processes, have clear exceptions for safety and security applications, and recognize that federal risk-based guidance for Artificial Intelligence ("AI") is still in the process of being developed and adopted.

The Agency is also seeking comments on rules to address cybersecurity audits and risks assessments. Any such rules should align with similar requirements under other privacy frameworks—from the GDPR to other state privacy laws. Any such rules should also draw from and align with longstanding and widely adopted industry standards and best practices.

Automated Desicisionmaking Technology

1. **Any rules for automated decisionmaking technology should be risk-based and avoid suppressing uses of the technology that benefit consumers, consistent with the risk-based approach followed by the federal government and other states.**

[1] CPPA, *Invitation for Preliminary Comments on Proposed Rulemaking*, (Feb. 10, 2023) https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf ("Invitation for Comments").
[2] Cal. Civ. Code § 1798.185(a)(15)-(16)

The Agency should use its charge to establish a clear and focused definition of, and overall regulatory approach for, "automated decisionmaking technology"—which the CPRA does not define—that promotes the consumer protection goals of the CPRA, including by avoiding counterproductive regulation of beneficial uses of technology.[3] The approach should be risk-based and consistent with clear federal and state policy to promote the responsible development and deployment of important AI technologies, and allow for AI technology to be deployed in ways that help consumers. As explained below, the Agency should focus any regulation on high-risk use cases, exclude uses of technology that involves human review, provide clear exceptions for safety and security and for trade secrets, and recognize the development of voluntary risk-based approaches.

2. Automated decisionmaking technology provides tremendous benefits for consumers and society, including in protecting public safety and security.

The Agency must keep in mind that automated decisionmaking technologies can provide great benefits to consumers and society, and will continue to develop in beneficial ways, and any proposed regulations consider those benefits and avoid unintentionally suppressing beneficial uses. Congress has expressed its policy preference for promoting innovation in AI. The National AI Initiative Act of 2020 calls for "a coordinated program across the entire Federal government to accelerate AI research and application for the Nation's economic prosperity and national security."[4] Following this goal, the Administration is seeking to update the National AI R&D Strategic Plan, which is critical to fostering innovation.[5] Similarly, the Department of Commerce has sought comments to aid its efforts on a "top priority to drive U.S. innovation and global competitiveness in critical and emerging technologies such as [AI]."[6] This focus on innovation is inconsistent with a rigid regulatory approach. In general, the National Institute of Standards and Technology ("NIST") has pointed out that "[r]emarkable surges in artificial intelligence (AI) capabilities have led to a wide range of innovations with the potential to benefit nearly all aspects of our society and economy – everything from commerce and healthcare to transportation and cybersecurity."[7]

The possibilities of automated decisionmaking tools are particularly notable in public safety and security applications. AI enables its users to respond to and analyze potential safety and security risks in a substantially quicker and more accurate manner than traditional, manual methods. There are many applications of AI for safety and security, including streamlining 911 call center response, transcribing incident reports, and efficiently analyzing video feeds for high-risk safety and security situations.

Other types of automated decisionmaking capabilities have transformed safety and security solutions. Widely used biometric identity verification capabilities such as fingerprint or facial recognition support a tremendous volume of online commerce on a daily basis. These capabilities are also used for physical security such as access control and facility security screening, and even support rapid and contactless travel experiences such as clearing customs and aviation security screening. Law enforcement also leverages biometric capabilities to generate investigative leads, rapidly assess large data sets of potential suspects or victims, prevent and investigate fraud, and investigate child sexual exploitation. Any forthcoming rules should account for these benefits.

Another key potential benefit of automated decisionmaking is that it can be leveraged to prevent bias and discrimination in human decisions.[8] AI capabilities can also support increased access to financial services,[9] support

[3] The CPRA's definition of "profiling" ("any form of automated processing of personal information")[3] also is subject to further definition under these regulations, so the Agency is empowered to adapt the statutory definition of profiling to support a clear and focused definition.
[4] https://www.ai.gov/.
[5] https://www.ai.gov/strategic-pillars/innovation/.
[6] https://www.federalregister.gov/documents/2022/08/16/2022-17576/request-for-comments-on-artificial-intelligence-export-competitiveness.
[7] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf.
[8] *See Mitigation of AI/ML Bias in Context*, NCCoE, https://www.nccoe.nist.gov/projects/mitigating-aiml-bias-context ("Automated decision-making is appealing because artificial intelligence (AI)/machine learning (ML) systems produce more consistent, traceable, and repeatable decisions compared to humans[…]").
[9] FinRegLab, *AI in Financial Services*, https://finreglab.org/ai-machine-learning.

sustainability efforts,[10] and support advanced medical diagnostics and care.[11]

3. The Agency should tailor any automated decisionmaking rules to high-risk and purely automated decisions, as overly-broad automated decisionmaking rules would have direct unintended negative impacts on California consumers and would be out of sync with the clear policy consensus across other states.

Every state that has established consumer rights associated with automated profiling under their omnibus privacy framework has focused on automated processing deployed in high-risk contexts that involve decisions regarding important benefits or necessities, or other particularly sensitive activities with significant societal implications. For example, in Virginia, the automated profiling opt-out right applies only with respect to "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."[12] "Legal or similarly significant effects concerning the consumer" is further defined to include only "a decision made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."[13]

Connecticut and Colorado's profiling opt-out rights have a similar scope. Connecticut and Colorado both limit the application of the opt-out right to "decisions that produce legal or similarly significant effects concerning the consumer."[14] Other states and localities—including California itself—have chosen only to regulate automated processing/AI technology in specifically defined, high-risk settings.

For example, California's disclosure requirements for using an "automated online account," or "bot,"[15] are narrowly tailored to situations in which the bot is used "with intent to mislead a person […]about its artificial identity" and only for the purpose of "knowingly deceiving" a person "to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election."[16] The Illinois Artificial Intelligence Video Review Act[17] regulates employers' use of artificial intelligence only in the context of an "artificial intelligence analysis" of an applicant-submitted video when an employer asks applicants to record video interviews. New York City Local Law 144 regulates use of "automated employment decision tool[s]" by employers and employment agencies in New York City. It applies only in the context of an employment decision "to screen candidates for employment or employees for promotion."[18]

In each of these laws, the limitations on use of automated tools or processing capabilities are applied only in a limited set of circumstances and specific purposes, not to *all* purposes of automated processing, where there would be impact to consumer benefits. This risk-based approach is the most beneficial approach for consumers. Focusing automated decisionmaking rules on automated processing in high-risk contexts offers important consumer protections, but does not stifle automated technology development and deployment that does not present significant risks to consumers.

Focusing on high-risk use cases allows for any automated decisionmaking rules to protect against specific and tangible

---

[10] *See* AMP Robotics, *AMP Robotics Installs its First Recycling Robots in the United Kingdom and Ireland with Recyco* (Sept. 22, 2021), https://www.amprobotics.com/newsroom/amp-robotics-installs-its-first-recycling-robots-in-the-united-kingdom-and-ireland-with-recyco; Adam Zewe, *Preventing poaching: AI software that predicts poaching hotspots now being deployed to wildlife parks*, Harvard John. A. Paulson Sch. of Eng'g and Applied Scis. (June 16, 2020), https://www.seas.harvard.edu/news/2020/06/preventing-poaching \.

[11] *See generally* Eric Topol, *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*, Basic Books (2019).

[12] Va. Code. Ann. § 59.1-577(A)(5).

[13] Va. Code. Ann. § 59.1-575.

[14] Conn. Pub. Act 22-15, §4(a)(5) (effective July 1, 2023); Colo. Rev. Stat. § 6-1-1306(1)(A)(I)(C)(2021). This term is defined in Colorado as "a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services." Colo. Rev. Stat. § 6-1-1303(10)(2021); Connecticut's definition is "decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services." Conn. Pub. Act 22-15, §1(12) (effective July 1, 2023).

[15] Cal. Civ. Code § 17940(a).

[16] Cal. Civ. Code § 17941(a).

[17] 820 Ill. Comp. Stat. 42/1.

[18] N.Y. City Admin. Code § 20-870.

risks without impeding the vast benefits of AI, including common business uses that improve efficiency such as classifying and interpreting massive volumes of data,[19] or providing conveniences such as customer service or music and video recommendations.[20]

At the same time, continued innovation in the automated decisionmaking and AI space will increase the likelihood that concerns about the equitable and accurate application of the technology will be overcome. Indeed, risk-based, flexible, and voluntary standards and best practices are growing to help ensure the "trustworthy" deployment of AI, as detailed further below. A focus on high-risk use cases is consistent with the federal government's longstanding risk-based approach to emerging technologies and emphasis on promoting the potential benefits of AI uses. For these reasons, regulations on the use of automated decisionmaking tools should be limited to narrowly-defined high-risk use cases.

4. **The Agency should ensure that "automated decisionmaking technology" is defined to exclude technology involving human review.**

The CPPA asks how other laws define "automated decisionmaking technology" and whether it should adopt any of those definitions.[21] In general, any automated decisionmaking rules should focus on "solely" automated decisionmaking processes, consistent with the approach of states like Colorado and Connecticut.

Under the Connecticut Data Privacy Act (CTDPA), the profiling opt-out right only applies to "solely automated decisions."[22] In Colorado, following an extensive rulemaking process, the Attorney General's Office in that state has finalized rules that establish a clear exception from the profiling opt-out rule for automated processing where a human reviews or ultimately controls the decision the automated processing supports. The exception gives a data processor discretion as to whether to accept an opt-out request from a consumer when the processor uses "Human Involved Automated Processing," defined as "the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing."[23]

Focusing on solely automated decisions is the best approach for protecting consumers. A key concern with automated decisionmaking is it can cause harms without adequate human input or review. However, when humans are involved, their conduct can be reviewed directly and is subject to regulation (if applicable, depending on the use case). Additionally, technology can *help* them make decisions. Overly broad rules would work against the Agency's underlying policy goals, and could have the unintended consequences of contributing towards less accurate decisions and preventing businesses from utilizing technology to identify and prevent against human bias.

AI helps address several common weaknesses in human decisionmaking, including the inability to collect and evaluate all relevant information, at speed.[24] AI is particularly well suited to tasks requiring repetitive work and pattern recognition.[25] These features enable AI to improve the accuracy of decisionmaking by considering all relevant information, following a set of rules or procedures rapidly and uniformly, and avoiding some of the decision shortcuts that can lead to suboptimal decisions. Broad regulations could discourage development and deployment of the technology that generally improves accuracy.

There is also a growing body of research that shows that automated decision tools, such as AI, can identify and mitigate

[19] NIST, "Artificial Intelligence in Manufacturing: Real World Success Stories and Lessons Learned," (Jan. 7, 2022) https://www.nist.gov/blogs/manufacturing-innovation-blog/artificial-intelligence-manufacturing-real-world-success-stories.
[20] *See, e.g.*, Netflix, "Deep Learning for Recommender Systems: A Netflix Case Study," (Feb. 4, 2022) https://research.netflix.com/publication/%20Deep%20Learning%20for%20Recommender%20Systems%3A%20A%20Netflix%20Case%20Study.
[21] Invitation for Comments at 6.
[22] Conn. Pub. Act 22-15, §4(a)(5)(C) (effective July 1, 2023).
[23] 4 Colo. Code. Regs. §904-3, Rules 2.02 and 9.04 (adopted Feb. 23, 2023)(available at: https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf)("Colorado Privacy Act Rules").
[24] Choi et. al., "How Does AI Improve Human Decision-Making? Evidence from the AI-Powered Go Program," (July 2021) at 4 https://mackinstitute.wharton.upenn.edu/wp-content/uploads/2022/03/Choi-Sukwoong-et-al._How-Does-AI-Improve-Human-Decision-Making.pdf.
[25] *Id*. at 5.

against bias in *human decision making*, [26] thereby moving toward the goal of promoting equity, consistent with the overall goals of the Agency.[27] As an example, FRT in collaboration with humans can produce the most accurate outcomes.[28] Limiting the scope of any automated decisionmaking rules to "solely" automated processing will allow the Agency to address potential risks that are unique to processing that does not include human involvement, while protecting against overbroad rules that could impede basic automation tools that merely assist human processing.

5. **Automated decisionmaking rules should have clear exceptions. This should include technology used to promote safety and security.**

Consumers directly benefit when data is used to enhance safety and security, including but not limited to the safety and security benefits from use of AI and biometric data, as discussed above. Overbroad automated decisionmaking rules, absent an exception for safety and security, would potentially render safety and security use cases impractical and undermine use of the technology. For example, criminals and fraudsters would try to use any opt-out rights to their advantage. Accordingly, any automated decisionmaking rules from the Agency should include a clear and robust exception for automated decisionmaking technology used to promote safety and security. Such an exemption would be consistent with other state regimes.

For example, Colorado, Connecticut, Utah, and Virginia's privacy laws exempt safety and security activities. Each has provisions specifying that the rules are not to be construed to limit rules entities' ability to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity or security of systems or investigate, report, or prosecute those responsible for any such action.[29] Without such an exemption for safety and security, future rules could be interpreted as limiting these important services, which would have direct negative impacts on California consumers. The benefits of exempting practices and technologies related to providing safety and security outweigh any potential risks.

6. **Rules should include strong protections for trade secrets.**

Any rule the Agency develops for automated decisionmaking should make clear that companies do not have to make disclosures that would reveal trade secrets. The authorizing statute for the rules specifies that businesses shall not be required to disclose trade secrets,[30] and tasks the Agency with establishing exceptions via rule "with the intention that trade secrets should not be disclosed in response to a verifiable consumer request."[31] These protections would also be consistent with other states that have addressed automated decisionmaking systems—for example, Connecticut also provides an exception from access and portability rights to protect trade secrets.[32] Exempting trade secrets from disclosure would foster innovation and protect the competitiveness of U.S. companies from foreign adversaries that

[26] *E.g.,* Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. of Legal Analysis 113, 120 (Apr. 22, 2019), https://academic.oup.com/jla/article/doi/10.1093/jla/laz001/5476086 ("Our central claim, stated in simple form, is that safeguards against the biases of the people who build algorithms, rather than against algorithms per se, could play a key role in ensuring that algorithms are not being built in a way that discriminates (recognizing the complexity and contested character of that term). If we do that, then algorithms go beyond merely being a threat to be regulated; they can also be a positive force for social justice.").

[27] California Privacy Protection Agency Board, Transcription of Recorded Public Meeting (Dec. 16, 2022) at 126 (Board Member Le noting that one of the purposes of the automated decisionmaking regulation is to "address algorithm discrimination") https://cppa.ca.gov/meetings/materials/20221216_transcript.pdf.

[28] Jonathon Phillips, et al., *Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms*, PNAS Vol. 115 No. 26 (May 29, 2018), https://www.pnas.org/doi/10.1073/pnas.1721355115.

[29] Colo. Rev. Stat. § 6-1-1304(1)(x); Connecticut also exempts actions "prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action". Conn. Pub. Act 22-15, §10(9)(effective July 1, 2023); Virginia's exemption is nearly identical, exempting a data controller or processor's efforts to "[p]revent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action"; Utah also specifies that its rules do not restrict a controller or processor's ability to " detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; or […] investigate, report, or prosecute a person responsible [such] action […] preserve the integrity or security of systems; or […] investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable." Utah Consumer Privacy Act, S.B. 227 (2022), §11 (effective Dec. 31, 2023).

[30] Cal. Civ. Code § 1798.100(f).

[31] Cal. Civ. Code § 1798.185(a)(3).

[32] Conn. Pub. Act 22-15, §4(a)(1),(4) (effective July 1, 2023).

may seek to steal these advanced technologies.[33]

7. The Agency should avoid broad access and opt-out mandates for automated decisionmaking.

The Agency has asked about existing laws that require access and/or opt-out rights in the context of automated decisionmaking.[34] First, it is important to highlight that there is a clear federal policy preference to promote risk management and innovation with respect to AI, as opposed to strict, regulatory mandates that would require providing consumers with overly broad opt-out rights or detailed information about how the tools work. As directed by Congress, NIST recently finalized its AI RMF 1.0, which is a voluntary and flexible tool for organizations to identify and manage AI risks, while facilitating AI benefits. The RMF is "intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems."[35] NIST is also developing a companion AI RMF Playbook, which "includes suggested actions, references, and documentation guidance for stakeholders to achieve the outcomes."[36] The AI RMF specifically addresses risks related to bias and privacy.

NIST has multiple other efforts underway to promote trustworthy AI, including efforts to produce training data, algorithms, and other tools to test or train AI systems.[37] NIST likewise has ongoing studies focused on measures of accuracy and robustness, as well as other types of AI-related measurements and evaluations under investigation such as bias, interpretability, and transparency.[38] NIST has developed other risk-based guidance in this space, including explainability and non-bias work. NIST's *Four Principles of Explainable Artificial Intelligence* provides baseline guidance, while noting that "the field of explainable AI is an area of active research.[39] NIST further points out that the principles must be flexible to address the needs of difference audiences.[40] With respect to mitigating the risk of bias in AI, NIST recently published a report entitled "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence"[41] and has launched a new project regarding "Mitigation of AI/ML Bias in Context."[42]

As these ongoing NIST projects demonstrate, there are robust federal-led efforts informed by stakeholder input to develop risk management guidelines. It would be premature and inappropriate to establish a regulatory mandate for broad access to detailed information about individual decisions made by automated decisionmaking tools when fundamental issues such as bias, transparency, and explainability are still nascent. Though it continues to evolve, it is clear this existing federal guidance seeks to protect consumer privacy in a risk-based manner that can adapt to technological advances without stifling innovation.

Second, to date, states that have established statutory requirements under omnibus privacy frameworks have generally focused on opt-out rights and data protection assessments, and have not imposed strict requirements regarding access to detailed information about technological mechanisms. Connecticut residents have the right to opt out of the processing of their personal data for targeted advertising, sale, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.[43] Connecticut also requires a data protection assessment for data processing activities that may pose a "heightened risk of harm," such as profiling where there is a "reasonably foreseeable" risk of substantial injury to or unfair or deceptive treatment of consumers.[44]

---

[33] *See, e.g.*, National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace,* (2018) at 11, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf (citing Artificial Intelligence and big data analysis as among the highest interest items for foreign intelligence services).

[34] Invitation for Comments at 6 ("What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)").

[35] https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development-request-information.

[36] https://pages.nist.gov/AIRMF/.

[37] https://www.nist.gov/document/ai-fact-sheet.

[38] https://www.nist.gov/programs-projects/ai-measurement-and-evaluation.

[39] NIST, *Four Principles of Explainable Artificial Intelligence*, NISTIR 8312 (Sept. 2021) https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf.

[40] *Id*. at 4.

[41] https://doi.org/10.6028/NIST.SP.1270.

[42] https://www.nccoe.nist.gov/projects/mitigating-aiml-bias-context

[43] Conn. Pub. Act 22-15, §4(a) (effective July 1, 2023).

[44] *Id*. at §8(a).

Similarly, Virginia law provides Virginia consumers with the right to opt out of the processing of their personal data for targeted advertising, sale, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.[45] Virginia also mandates a data protection assessment for data processing activities that may pose a "heightened risk of harm," such as profiling where there is a "reasonably foreseeable" risk of substantial injury to or unfair or deceptive treatment of consumers.[46] The Colorado statute has similar opt-out and data protection assessment requirements for certain automated profiling.[47]

Cybersecurity Audits and Risk Assessments

1. **Any risk assessment requirement related to the processing of personal information should be consistent with existing regulatory regimes and flexible, risk-based standards - and the trigger for any personal information processing risk assessment should be consistent with other U.S. state law approaches.**

The CPRA contemplates any such risk assessment rules to apply only where "businesses . . . process[] . . . consumers' personal information [in a way that] presents significant risk to consumers' privacy and security."[48] To properly tailor these requirements to maximize consumer benefit and promote the practical establishment of privacy protection programs while minimizing the burden on businesses unnecessarily, the Agency should ensure that any rules it proposes on these topics are aligned with existing frameworks that companies are already subject to.

The Agency has asked about existing laws that require risk assessments for data processing.[49] Data protection assessment (DPA) requirements have been adopted by several states as part of those state's omnibus privacy frameworks. Generally, those DPA requirements apply based on potential harms associated with the processing in question—not all data processing activities are subject to an assessment requirement.[50] Specifically, Colorado, Connecticut, and Virginia's privacy laws identify a "heightened risk of harm" to trigger the requirement for a data protection assessment.[51] Examples of such processing activities triggering an assessment include targeted advertising, sale of personal data, processing sensitive data, and profiling that presents a "reasonably foreseeable risk" of unfair or deceptive treatment, disparate impact, or financial, reputational, physical, or other substantial harm.[52]

Data protection impact assessments are also required in certain circumstances under the European Union's Global Data Protection Regulation (GDPR) as well as a significant number of countries globally that have adopted a privacy framework substantially similar to GDPR. Similar to the U.S. state law frameworks, the GDPR also sets a risk-based trigger for these assessments.[53] As GDPR was adopted in 2016, many businesses have established privacy protection compliance programs leveraging the regulation as a compliance baseline.

Under existing data protection frameworks, both U.S. state laws as well as international laws and regulations, there is no requirement that a business submit assessments regulatory authorities. Rather, the assessment is performed by the

[45] Va. Code Ann. §59.1-577.
[46] Va. Code Ann. § 59.1-580.
[47] Colo. Rev. Stat. §§ 6-1-1309, 6-1-1313. Note that recently adopted Colorado regulations also include certain transparency requirements for automated profiling activities, which are not specifically outlined in the statute. Colorado Privacy Act Rules.
[48] Cal. Civ. Code § 1798.185(15)
[49] Invitation for Comments at 4 ("What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments").

[51] Conn. Pub. Act 22-15, §8(a) (effective July 1, 2023).
[52] Colo. Rev. Stat. §§ 6-1-1309; Conn. Pub. Act 22-15, §4(a) (effective July 1, 2023); Va. Code Ann. § 59.1-580.
[53] The GDPR requires an assessment "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons." In particular, a data protection impact assessment is required under the GDPR in the following, higher risk circumstances: "(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale." Regulation (EU) 2016/679, (2016), §3, Art. 35, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

business and documented so that it may be provided to a customer or regulatory authority upon request. There often is no "one size fits all" model for an appropriate assessment across businesses, products or services, and the administrative burden for businesses as well as for the state regulatory authority would far outweigh the benefits of broad submission requirements.

California should not stray from existing approaches, as businesses already comply with similar requirements under other state and international privacy laws. Given these existing frameworks, consumers would be best served by rules that provide companies with consistency across jurisdictions. Businesses that would be impacted by this regulation are already conducting data protection assessments based on risk, and straying from existing frameworks would substantially increase compliance costs while creating confusion and uncertainty in the national marketplace.

2. Any requirements for risk assessments should align with current flexible, risk-based best practices.

In developing any rules for risk assessments for processing personal information, the Agency should avoid granularly prescribing the content of such assessments beyond establishing the risks relevant to determining when processing requires an assessment, consistent with the standard set by data privacy laws in Virginia and Connecticut.

3. Any cybersecurity audit should be consistent with existing regulatory regimes and flexible, risk-based standards.

Forthcoming rules should follow existing privacy legislation which make cybersecurity audits permissive rather than mandatory. Most privacy legislation imposes an obligation on all parties that process personal information to implement appropriate measures to ensure a level of security for the personal information appropriate to the level of risk.[54] An audit of those security practices typically comes into play under existing laws when a "controller" has engaged a "processor" to perform processing of the personal information. In this context, the controller is generally obligated to ensure its processors are safeguarding the personal information and are, therefore, granted the right to audit the security practices of the third party they have engaged.[55] However, because such an audit is typically not mandatory, controllers may utilize other means to verify that appropriate security measures are being taken.[56]

Any rules should align with existing privacy legislation and recognize the importance of aligning security audits to recognized standards that include an audit procedure. In order for any cybersecurity audit to be of value, particularly if the results are to be compared to those of others undergoing the same audit, the controls or standard against which a party is audited *must* contain an audit procedure. Absent an audit procedure, results of an audit can vary dramatically, and are ripe for manipulation. A defined audit procedure provides both consistency and the ability to make meaningful comparisons between audits.

Both Colorado and Virginia have recognized this importance in their privacy legislation. Both states require that audits or assessments be performed "using an appropriate and accepted control standard or framework *and assessment procedure* for such assessments."[57] (emphasis added). Accordingly, any forthcoming rules that may require a cybersecurity audit should align with standards and that include audit procedures. This approach will allow companies to align their audits with those that are already widespread throughout industry.[58]

---

[54] *See e.g.,* Colo. Rev. Stat. § 6-1-1302(c)(II)(B), Va. Code Ann. § 59.1-578(A)(3), Regulation (EU) 2016/679 (2016), § 2, Article 32.

[55] Colo. Rev. Stat. § 6-1-1305(II)(B); Va. Code Ann. Sec. 59.1-574(A)(3), 59.1-575(B)(4).

[56] The annual International Association of Privacy Professionals (IAPP) and Ernst-Young Privacy Governance Report 2021, page 74 included statistics related to managing the verification of data processing vendors' compliance to security and privacy requirements by controllers. The Report states: "To ensure vendors are meeting their commitments, most organizations rely on contractual assurances (90%), the completion of a questionnaire (67%) or documentation from a third-party audit (48%) to keep them accountable."

[57] Va. Code Ann. § 59.1-579(B)(4), *see also* Colo. Rev. Stat. § 6-1-1305(II)(B) with same requirement for audits being conducted "using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable."

[58] Invitation for Comments at 3 ("what other cybersecurity audits, assessments, or evaluations that are currently performed, or best practices, should the Agency consider in its regulations for CCPA's cybersecurity audits").

Two widely recognized information security standards with an associated audit procedure are the ISO/IEC 27001 information security standard,[59] and SOC 2-Type 2 report, which assesses a company's information security control design and operating effectiveness.[60] Further, as additional frameworks with audit procedures evolve to address industry specific concerns, flexible language such as that in Virginia and Colorado will the permit adoption of such frameworks. Doing so will ensure that companies are being evaluated under a consistent set of standards or guidelines that are widely used and can account for differences in company size, sector, and sophistication.

Finally, any cybersecurity audit rules should retain flexibility for companies when conducting the audits, as such evaluations are highly complex and context dependent. There should be no prescriptive requirements included in the audit requirement. Such prescriptive requirements should be left to the various standards to define.

Conclusion

The Security Industry Association (SIA) appreciate the opportunity to provide input to the Agency on these matters. We stand ready to provide any further assistance as may be required to ensure effective regulations protecting data privacy, which are consistent with statutory authority and promote uniformity, consistency functionality, and clarity in implementation. Please let us know if you have any questions or if we can provide any additional information that would be helpful.

Respectfully Submitted,

[redacted]

Don Erickson
Chief Executive Officer
Security Industry Association
Silver Spring, MD
www.securityindustry.org

Staff Contact: Jake Parker, [redacted]

[59] International Standards Organization, *ISO/IEC 27001 and related standards: Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html.
[60] *See* Association of International Certified Professional Accountants, "SOC 2® - SOC for Service Organizations: Trust Services Criteria," https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.

From: David Phillips [redacted]
Sent: Monday, March 27, 2023 12:33 PM
To: Regulations
Subject: PR 02-2023; CCPA Public Comment
Attachments: May 27_DWP Public Comment on ADM Regs_PR 02-2023.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Dear CCPA,

Please find my attached public comments on the CCPA proposed regulations on automated decisionmaking technology. Please contact me if you have any questions or wish to discuss further.

Thank you for your consideration.

Sincerely,

David Wendell Phillips
Larkspur, California

March 27, 2023

VIA EMAIL to regulations@cppa.ca.gov
California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Boulevard
Sacramento, California 95834

Re: **PR 02-2023;** Comment on CA Regulations Governing Automated Decisionmaking Technology

Dear California Privacy Protection Agency,

I appreciate the opportunity to comment on California Privacy Protection Agency's ("CPPA") regulation of automated decisionmaking ("ADM") technology as mandated by the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA").[1] These comments reflect my personal opinions, but they are informed by more than two decades of professional experience in data privacy and automation technologies as a registered inhouse and general counsel for California-based and other technology companies. I offer these comments, because I believe meaningful regulation of ADM technology at this critical juncture is essential for the privacy and the well-being of Californians.

My comments focus primarily on the definition of automated decisionmaking ("ADM") technology and its regulatory scope. As detailed below, I urge the CPPA to define ADM technology broadly as a process for making decisions using automated means without significant human involvement and with significant potential effects on a California resident or household.

Justifying the necessity for such a broad definition of ADM technology requires us to step back briefly for a broader perspective. Vast increases in data availability and advances in ADM technology, including rapid developments in Artificial Intelligence (AI) and Machine Learning (ML), are significantly changing organizations' decisionmaking processes. ADM technology and consumer profiling impact California residents by influencing or determining high stakes decisions, such as who gets a job interview, a loan approval, or a gig worker assignment. Other, seemingly less impactful uses of ADM technology and profiling processes, such as auto freezing an active account, or algorithmically distributing news or social media content, may also produce potentially significant effects, particularly if evaluating the potential or cumulative impact.

Broadly defining ADM so that significant reliance on ADM technology for decisionmaking triggers minimal regulatory protection, such as rights of notice, explanation, opt-out and human appeal, will help mitigate potential harms to California residents and households. ADM technology has no common sense. ADM processes can ignore important intangible ethical, moral, and other human considerations that should guide high stakes decisions about people's lives. Promoting transparency and significant human input into ADM processes and requiring explanations in understandable terms is crucial for perceived legitimacy

[1] C v Code § 1798.185(a)(16). As part of ts ru emak ng respons b t es, the Agency s d rected to ssue "regu at ons govern ng access and opt-out r ghts w th respect to bus nesses use of automated dec s onmak ng techno ogy, nc ud ng prof ng and requ r ng bus nesses response to access requests to nc ude mean ngfu nformat on about the og c nvo ved n those dec s onmak ng processes, as we as a descr pt on of the ke y outcome of the process w th respect to the consumer.'

and fairness.[2] For these reasons, California's ADM technology regulations should require covered businesses using ADM and profiling processes to provide consumers with a simple way to opt-out of profiling and obtain human reconsideration of an automated decision.

Mandating risk assessments, and ongoing audits for ADM technology prior to deployment also supports ethical use of algorithm-assisted decisions. Compliance teams require these measures to lift the cover on opaque and complicated ADM processes, allowing them to assess risks and tradeoffs and implement mitigation strategies before deployment. Risk assessments must specifically document human involvement in decision-making, assessing ADM technology usage at various stages, and establish regular governance structures to assess algorithmic accuracy, safety, fairness, transparency, and accountability within organizations.

As ADM technology grows increasingly complex and integrated into organizational decisionmaking at all levels, human input, oversight and redress help protect core ethical human values, including privacy, accountability, fairness, and agency. ADM technology regulations should protect the ***contextual privacy rights*** of all California residents, ensuring fairness and transparency in processing of personal information, including the use of such data in training large language models (LLMs). Clearly defined and enforced ADM technology regulations will help protect Californians' privacy rights and guarantee essential human accountability for ADM technology and processes.

Automated Decisionmaking:

1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

Before the EU's General Data Protection Regulation (GDPR) was implemented in 2018, EU data protection laws already governed automated decision-making systems. Considering this extensive history and the CCPA's adoption of GDPR's ADM regulatory principles, it is essential to thoroughly examine the application of these principles by EU courts and data protection authorities (DPAs).

Article 22 of the GDPR restricts the use of automated decision-making systems where they are 1) "solely automated" and 2) have "legal" or "similarly significant" effects. On the first threshold, the following factors determine whether an ADM process is "solely automated": 1) whether the decision is supported by a written assessment made by a human; 2) whether the decision is reviewed by a human supervisor; 3) whether the company's employees have been specifically trained and given detailed guidance on decision-making considerations; and 4) whether the decision was an interim one that is still subject to final human review.

In determining whether an ADM process has "legal or significant effects" on the data subject, the European Data Protection Board ("EDPB") has proclaimed that a “legal effect” must affect someone’s legal rights, such as the freedom to associate with others, vote in an election, or take legal action under a contract. A decision has a "significant effect" if it has the potential to significantly affect the circumstances, behavior or choices of the individuals concerned; have a prolonged or permanent impact; or lead to exclusion or discrimination.

[2] See A gor thms and Autonomy: The Eth cs of Automated Dec s on Systems. A an Rube , C nton Castro, Adam Pham, Cambr dge Un vers ty Press, 2021 at p.68: "[R]easonab e endorsement of [an ADM system] s a funct on of whether systems are re ab e, whether they turn on factors for wh ch subjects are respons b e, the stakes nvo ved, and whether they mpose unjust f ed re at ve burdens on persons.

EU based courts and DPAs have construed significant effects broadly including impacts to individual circumstances, behavior or choices where there is a prolonged or permanent impact, including when 1) the decisionmaking significantly affects a resident's rights and freedoms or legitimate interests; 2) the decisionmaking significantly affects a resident's economic situation, social situation, health, personal development, reputation, or other important interests; or 3) the decisionmaking significantly affects a resident's physical or mental health.

Under the GDPR, organizations applying automated decision-making tools must implement "suitable measures to safeguard the data subjects' rights and freedoms and legitimate interests." Such measures include the right to obtain human intervention by the controller, a right to contest the decision and "the right to explanation" (i.e., "meaningful information about the logic involved" in the ADM process). Additional protections require regularly checking datasets used for bias and introducing safeguards to prevent errors and inaccuracies. The United Kingdom's Information Commissioner's Office ("UK ICO") provides practical guidance for organizations implementing automated decision making and profiling that is centered on conducting data protection information assessments or "DPIAs" to consider and address the risks before starting any new automated decision-making or profiling.[3]

The guidelines to automated decision-making and profiling issued by the Article 29 Data Protection Working Party, now the ECPB ("Guidelines"), note that "complexity is no excuse for failing to provide information." Organizations should provide "factors taken into account for the decision making process," "their respective weight at an aggregate level," as well as information on: 1) the categories of data that have been or will be used provided to individuals, 2) why these categories are pertinent, 3) how any profile using the automatic decision making process is built including any statistics used in the analysis, 4) why the profile is relevant to the automated decision making process, and 5) how it is used for a decision concerning the individual. The Guidelines advise that organizations need not provide a complex mathematical explanation about how the algorithms work or disclose the algorithm, but the explanation must be sufficiently for the individuals to act upon it to contest decisions or to correct inaccuracies or request erasure.

Despite high threshold triggers to qualify for Article 22 protection, EU based courts and DPAs examine the underlying lawfulness of the data processing for the ADM process, thus going beyond the scope of strict Article 22 construction under the "solely automated" and "significant effect" triggers. EU based courts and DPAs strictly scrutinize ADM use to ensure lawful data processing and broad accountability. As the Future of Privacy Forum's detailed case research report concluded, EU based courts and DPAs frequently go beyond Article 22 in an ADM inquiry to require transparency measures, fairness and non-discrimination documentation, and strict conditions for valid consent.[4] These include specific transparency and access requirements for ADM processes under Articles 13, 14 and 15, and mandates to conduct DPIAs for ADM processes under Article 35.

---

[3] See ICO Pub cat on: "R ghts re ated to automated dec s on mak ng nc ud ng prof ng". Bus nesses must " dent fy whether any of your process ng fa s under Art c e 22 and, f so, make sure that you: g ve nd v dua s nformat on about the process ng; ntroduce s mp e ways for them to request human ntervent on or cha enge a dec s on; carry out regu ar checks to make sure that your systems are work ng as ntended."

[4] Future of Pr vacy Forum (FPF) b og: GDPR and the AI Act Interp ay: Lessons from FPF ADM Case: "[o]ur research h gh ghted that the GDPR s protect ons for nd v dua s aga nst forms of ADM and prof ng go s gn f cant y beyond Art c e 22... [t]hese range from deta ed transparency ob gat ons to app y ng the fa rness pr nc p e to avo d s tuat ons of d scr m nat on and str ct cond t ons for va d consent n ADM cases." See FPF Report: Automated Dec s on-mak ng under the GDPR – A Comprehens ve Case Law Ana ys s.

(3) With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:

a. How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?

b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?

c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decisionmaking technology requirements?

d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?

e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?

f. Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, how?

The Agency should adopt a definition of "automated decision-making technology" that encompasses a wide range of automated decision-making technology applications and processes, including automated processes, algorithms, artificial intelligence, and machine learning systems that use personal data and are used in decisionmaking. Unlike Article 22 of the GDPR, the CPPA's statutory mandate to issue ADM regulations is not limited to "solely" automated decisions and those with "legal" or similarly significant effects. The CPPA should take notice that the higher thresholds under the GDPR Article 22 requiring "solely" automated decisions that have "legal" or "similarly significant effect" are mitigated by application of other robust GDPR safeguards, which are broadly applied to EU ADM cases. As referenced above, ADM inquiries by EU based courts and DPAs have frequently scrutinized lawful data processing requirements under the GDPR far beyond the scope of narrowly constructed Article 22 triggers.[5]

Because the CPPA does not provide similar far-reaching protections and remedies, the definition of ADM technology under the CCPA needs to be sufficiently broad and flexible without application of rigid trigger thresholds such as "solely automated" or "legal or similarly significant effect."

For the reasons detailed below, CPPA should define automated decisionmaking technology broadly as making decisions using automated means 1) without **significant human involvement**; and 2) where the decisionmaking has a **significant potential effect** on a California resident or household.

This definition is broad enough to encompass a wide range of automation technologies that are used to make decisions, from simple algorithms to advanced machine learning models. It clarifies the scope of

[5] Accord ng to the Future of Pr vacy Forum's we -researched report on Art c e 22: [T]he GDPR s protect ons for nd v dua s aga nst forms of automated dec s on-mak ng (ADM) and prof ng go s gn f cant y beyond Art c e 22. In th s respect, there are severa safeguards that app y to such data process ng act v t es, notab y the ones stemm ng from the genera data process ng pr nc p es n Art c e 5, the ega grounds for process ng n Art c e 6, the ru es on process ng spec a categor es of data (such as b ometr c data) under Art c e 9, spec f c transparency and access requ rements regard ng ADM under Art c es 13 to 15, and the duty to carry out data protect on mpact assessments n certa n cases under Art c e 35." FPF Report: Automated Dec s on-mak ng under the GDPR – A Comprehens ve Case Law Ana ys s.

ADM regulation and ensures that all relevant technologies are covered. The nuances of this definition can be further parsed around three key questions: 1) What is "decisionmaking"; 2) What is "significant human involvement" in decisionmaking, and 3) What is a "potentially significant effect" of decisionmaking?

1. "Decisionmaking": A decision can be defined as a choice made or action taken from a range of options, including the act of selecting one course of action from several possibilities. Decisionmaking encompasses the entire process of making decisions, including the steps of identifying a problem, inputting information, and evaluating options and additional inputs and data processing to produce an output or render a choice or action. It's clear that decisionmaking can be a complex process with multiple stages and steps.[6] In the real world, ADM technology and processes interact upstream and downstream with profiling technology and processes. For example, an automated decision-making system might use profiling to make predictions about which consumers are likely to be approved for a loan; or a profiling system might integrate with an ADM technology to make decisions about which individuals to target with a special promotionally priced offer.

The regulations should make clear that any inquiry into whether a decisionmaking process is automated and has significant effect should focus on the entire decision-making process, not just a final stage of a decision. ADM technology regulations need to apply to the entire decisionmaking process and protections should apply to circumstances where automated processing has foreclosed downstream consideration, despite human input in the so-called final decision. Under the CPRA, the CPPA is free to define decision-making to encompass the entire process through which a covered business or organization evaluates, considers, or renders a decision, including upstream processing of personal information and profiling. An automated decision can include decisions that are claimed to be temporary or interim if they have a significant effect on the California resident or household. For example, a decision to freeze a user's account based on suspected fraud can have a significant effect even if it is claimed by the company to be "interim" and not final. A broad definition of decisionmaking will ensure that all types of automated decision-making processes are held accountable for their potential impacts on privacy and consumer rights.

2. "Significant Human Involvement": The Proposed Regulations should clarify that an organization must demonstrate "significant human involvement" in the decision-making process by providing adequate documentation or support of human input. While this is similar to the EU's application of the "*meaningful* human involvement standard", the inquiry should be interpreted more broadly to examine the entire decision-making process, not just isolating the final stage of a decision. The regulations should avoid adopting an overly narrow or mechanistic approach that focuses only on whether there was adequate human input in the final step.[7] This means applying the "significant human involvement" inquiry to the entire decisionmaking processes, including where an upstream automated processing has foreclosed downstream consideration despite human input. This broad consideration of the entire "decisionmaking process," including its interaction with profiling, is discussed further below in in subpart 2 "significant effect" and subpart 3 "decisionmaking."

---

[6] See Reuben B nns & M chae Vea e: *Is that your final decision? Multi-stage profiling selective effects and Article 22 of the GDPR*, Internat ona Data Pr vacy Law (2021).

[7] See B nns, Vea e, supra note 6, at 329: "It s therefore understandab e that we m ght ook to the f na step n a dec s on-mak ng process, and f that step s automated, judge the ent re process to be automated. Converse y, a human mak ng the f na dec s on renders the process non-so e y automated. However, as some of the prev ous cases suggest, ne ther nference w a ways ho d true."

Determining whether there's "significant human involvement" in the decisionmaking requires a broad inquiry into the overall organizational environment underlying the decisionmaking, including an organization's structure, reporting lines, chains of approval, staff training, and internal policies. The burden should be on businesses using ADM technology to demonstrate adequate human involvement in the the ADM process. To incentivize businesses to review their entire decisionmaking process for human involvement, the regulations should emphasize the importance of conducting data protection risk assessments or DPIAs and documenting mitigation measures to reduce risks from ADM technology processes. The CPPA should take note of the EU's strict scrutiny of complex ADM technology, such as LLMs, that defy interpretability and can result in "automation bias."[8] Captured by "intelligent" technology that appears to be our ally, and incapable of explaining ADM processes in human understandable terms, employees can develop a deference to ADM technology that sometimes resembles mysticism. Automation bias combined with the increasing pervasiveness and scale of ADM technology necessitate a broad scope of regulation where there's no significant human involvement in the decisionmaking.

3. "Potentially Significant Effect": Determining whether an automated decision has the requisite "potentially significant effect" on a California resident or household should not be restricted to specific rigid types or domains of decisionmaking, nor should it be narrowly focused on only fully realized effects. Under the CPRA, in contrast to other pending state ADM regulation, there is no statutory language suggesting that a decision's impact be limited to defined areas of impact, such as financial services, housing, insurance, education, employment opportunities, healthcare services or access to basic necessities. Rather, it is appropriate to interpret "potentially significant effect" with reference to the CPRA's explicit and broader definition of profiling as "performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."

The ADM technology definition also should not be limited to actual realized harms from a so-called final decision, but potential harms such as the potential for an upstream automation step in the decisionmaking process to foreclose a downstream outcome despite human input in the later stages of the process. For example, the automated ranking or filtering of a job applicant's materials may foreclose practical consideration to interview candidates by a human reviewer. The automated freezing of a gig driver's account forecloses tangible income opportunities even if the account suspension is deemed temporary and subject to ultimate review by a human. In such cases, the ADM has a significant effect. ADM technology use also often includes and relies upon upstream profiling that is expressly included in the definition of automated decisionmaking under the language of the CPRA. The larger point is that the express use of the word "decisionmaking" and "profiling" in the statutory language suggests regulation of a larger ADM process that often includes upstream profiling, rather than trying to isolate the location of a distinct and final "decision" in a multi-stage process that includes automated and human components.

The regulations should expressly clarify there are significant effects when a "decision" produces immediate and non-temporary consequences for individuals, including affecting an individuals' income-making opportunities.

---

[8] The comp ex ty of ADM Techno ogy n the EU has become a factor n tr gger ng Art c e 22 protect ons. EU regu ators have found over y comp ex ADM processes that are opaque and can operate beyond pract ca human contro nc ud ng through so-ca ed "automat on b as" and ack of " nterpretab ty". "Automat on b as" refers to the tendency of human users to rout ne y re y on the output generated by computer dec s on-support systems w thout further scrut ny. "Interpretab ty " n th s context refers to whether an ADM process s suff c ent y transparent such that deve opers can observe the nner mechan cs and understand how a mode s generat ng pred ct ons, for examp e. nterpret ng the mode s we ghts and features to determ ne a g ven output. ADM techno ogy that s comp cated, such as LLMs that emp oy neura networks and deep earn ng techn ques, often produce automat on b as or ack of nterpretab ty and he ghtened Art c e 22 scrut ny.

ADM Technology Regulation & Large Language Transformer Models (LLMs): A "decision" can be an action, choice or output based on factual data, including the automated generation of content based on inferred data and profiling as discussed below. The regulations should protect the privacy of individuals whose data is used to train automated decision-making models. The regulations should also require businesses to conduct a privacy impact assessment (PIA) before deploying automated decision-making technology. ADM technology employing large language transformer models ("LLMs") has been trained on massively scraped data sets to produce outputs that can be inaccurate and are difficult to interpret, predict or explain. They can produce material factual errors that can harm personal privacy and reputational integrity, as well as decision outputs that are biased and harmful.

LLMs have been trained based on permissionless data scraping that violates personal privacy. Even if the personal information scraped by LLMs were to be "publicly available" within the specific context in which it was posted, the data scraping, processing, and use of personal information violates "contextual integrity," a core privacy principle. There's simply no express or implied reasonable expectation or permission for using personal data in this manner.[9] The ADM technology regulations should protect the ***contextual privacy rights***[10] of all California residents and ensure that all types of ADM technology are held accountable for their potential impacts on privacy rights, which require fairness and transparency in the processing of personal information, including using personal data to train LLMs.

Conclusion: ADM technology use raises risks to data privacy, as well as harmful bias concerns from limited or discriminatory data that can reinforce social inequities. ADM technology and processes ignore important intangible human factors that go into real-life decision-making — the ethical, moral, and other human considerations that appropriately influence decisions in the real world. ADM technology should not be allowed to erode privacy, fairness, and human agency in the name of greater efficiency. The regulations must define ADM technology broadly and ensure minimal transparency and accountability, requiring covered businesses to conduct risk assessments before deployment of ADM technology to ensure accuracy, fairness, and human oversight. As ADM profiling technology becomes more complex, human oversight is crucial to ensure privacy, safety, fairness, accountability and respect for human autonomy and agency. Thank you for your attention to this critical issue. I look forward to seeing the adoption of meaningful ADM technology regulations to protect the privacy and well-being of Californians.

Respectfully submitted,

[redacted]

David Wendell Phillips
Larkspur, California

[redacted]

---

[9] In add t on to the ack of perm ss on, LLMs produce mater a factua errors that can be harmfu to persona pr vacy and reputat ona ntegr ty and produce outputs that are b ased. See e.g., Lu za Jarovsky, "*ChatGPT And Large Language Models Are A Privacy Ticking Bomb*," The Pr vacy Wh sperer, Feb 1, 2023.

[10] See K rsten Mart n and He en N ssenbaum, "*Privacy Interests in Public Records: An Empirical Investigation*", 31 Harvard Law Techno ogy Journa , 111, Last rev sed: 11 Ju 2017. "...the respondents judgments n our stud es were h gh y sens t ve to other contextua parameters such as the rec p ents of the nformat on, the terms under wh ch the nformat on had been shared, and the uses to wh ch t had been put. See a so, K rsten Mart n & He en N ssenbaum, "*Measuring Privacy: an Empirical Test Using Context to Expose Confounding Variables"* 18 COLUM. SCI. & TECH. L. REV. 176, 214–15 (2017).

From: Dave O'Toole [redacted]
Sent: Monday, March 27, 2023 12:44 PM
To: Regulations
Subject: PR 02-2023

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Mr. Sabo:

Thank you for the opportunity to provide preliminary comment on the proposed rulemaking for cybersecurity audits, risk assessments, and automated decisionmaking. My name is Dave O'Toole and I am interested in the important work of the California Privacy Protection Agency and the implementation of the California Privacy Rights Act and California Consumer Privacy Act. I am also a public finance executive with two decades of experience in California state government operations and oversight, mainly in the areas of finance, audits, and business regulation.

I am submitting these comments to convey my support for the CPPA's mission and offer considerations for the agency as it initiates rules for regulating affected businesses and protecting consumers. While my comments describe best practices and processes for this proposed rulemaking in general, I am also able to provide regulatory and statutory language to facilitate implementation, if needed.

CYBERSECURITY AUDITS

With the understanding that the underlying purpose of the annual cybersecurity audits is to determine the risks to consumers through businesses' processing of consumers' personal information, including behavioral and preference data, I encourage the CPPA to first adopt a well-established and understood cybersecurity standard that is regularly updated for current threats. As Mr. Chris Hoofnagle testified in your May 2022 pre-rulemaking stakeholder session, standards like those promulgated by the National Institute of Standards and Technology (NIST) or Control Objectives for Information Technologies (COBIT) are widely-respected norms that will reduce the initial adaptation burden for many businesses.

I would also encourage the CPPA to design and adopt an end-to-end audit scope for consumers' personal information risk. A regulated business may have the best cybersecurity program in the world with no consumer risk whatsoever, but if they sell or exchange consumer data with a third party, the consumers' personal

information is only as safe as the cybersecurity program of that third party. Effective audits that meet CPRA standards must include third-party entities in their scope.

Cybersecurity audits must also be scoped to identify and assess the risks of both structured and unstructured data. Structured datasets are what's typically disclosed or deleted when a customer makes a change request. Unstructured datasets are "raw" data that a business has not yet organized for monetization. When a customer asks that their personal data be reported or deleted, businesses in possession of such data will typically report their structured data, concluding that because the any other data is unstructured, it's not pertinent to the request. That unstructured data can then be harvested later, after the consumer has made their deletion or change request. Businesses that are determined to possess unstructured datasets should be required to either delete the dataset or submit it to a third-party processor to have it structured to make personal information identifiable.

In developing audit standards, I recommend the CPPA establish a standard metric to assess the risks to personal information loss or misuse. Specifically, the CPPA should consider incorporating a measure that can be easily translated, reported publicly, and compared to other regulated entities. The state's model for regulating financial institutions is a starting place for crafting consumer risk assessment regulations. At the Department of Business Oversight (now known as the Department of Financial Protection and Innovation) where I served as Chief Deputy, "CAMELS" ratings (measures of capital, assets, management, equity, liquidity, and sensitivity) were used to assess risk to businesses and consumers. Notwithstanding the complexity of banking examinations, the 1 to 5 CAMELS scoring system is easily understood, portable, and readily comparable across the banking industry. A source to begin to develop a cybersecurity scoring metric is the examination manuals crafted by the Federal Financial Institutions Examination Council, which provide the privacy portions of the Graham-Leach Bliley Act.

The CPPA may further want to consider a licensing program to ensure businesses that choose to operate a personal information business line must demonstrate compliance with the statewide standards. Licensing is also an effective tool to generate income to reduce the department's reliance on the annual budgeting process.

Additionally, I would encourage the CPPA to craft a cybersecurity audit program that follows these audit best practice principles.

- ***Operations Review.*** Auditees should possess and practice clear and unambiguous processes for how they protect consumers' personal information, and the auditors should be able to follow those procedures to the same stated process outcome.
- ***Test***. Privacy audits should follow parameters for testing practices and protocols to ensure they match what the auditee has reported. Cybersecurity audits should include regular, unannounced "penetration" testing to verify actual results match stated practices.
- ***Fines and penalties***. Audits should have a meaningful consequence component, set a level to compel correction (e.g., GDPR penalty of two percent of prior year net revenues).
- ***Audit on site***. Whenever possible, auditors have greater success when operating on site of the auditee, where listening and informal conversations facilitate understanding of the firm and open new avenues for investigation. Where a firm has a physical presence in California the auditor should be on site.
- ***Deterrent Effect***. Without disclosing material weaknesses or trade secrets, cybersecurity audit results should be communicated clearly to the general public and auditee's industry, so the lessons can be learned and auditees better prepared for their next audit.
- ***Audit Review Office.*** Business auditees should be afforded a CPPA ombudsman office, where disputes can be filed and impartially reviewed for revisions to audit findings.

- ***Subject Expertise.*** The CPPA will likely face a skeptical technology sector businesses who question the qualifications of government auditors to examine their cybersecurity processes. Hiring and compensation must be sufficient to recruit talented individuals who are both familiar with the work of the auditees and government auditing practices.

RISK ASSESSMENTS

Risk assessments from businesses will be critical to identifying and crafting an appropriate scope for cybersecurity auditees. The potential harms of not securely maintaining personal data, including behavioral and preference data, and allowing that data to be monetized without consumer awareness and consent, is contrary to the central assumptions of consumer privacy embedded in the CCPA and CPRA. To that end, I recommend the CPPA include these risk assessment principles in their rulemaking process.

Limit "Trade Secrets" Exception. Under the cover of trade secrets and copyright law, many large California-based technology corporations have shielded their customer data algorithms from divulgement and public understanding. The social and economic cost of concealed algorithmic makeup to consumers and society is now clear: it became rationale and reason for the success of the CPRA and CCPA. The CPPA should address the substantial obstacle to effective oversight by the "trade secret" defense, and seek to limit the definition of trade secrets. For example, the CPPA should consider rejecting any exceptions for algorithmic technology that was developed with U.S. and California government support, including public universities. Products originally established with the public resources of the California educational system should be publicly available so that they can be utilized in peer-to-peer innovation marketplaces, not sequestered by venture capitalist-backed business.

Clear Report Parameters. To manage the risk assessment workload, the CPPA should establish through rulemaking base content, format, template and size requirements to shape risk assessments and facilitate CPPA's analysis. The variability of reports and lack of institutional capacity to process risk assessments has been a challenge to European regulators under the GDPR, and slowed their ability to carry out their mission.

Well-Defined Processes. In providing their risk assessments, regulated businesses should clearly disclose their practices for processing consumers' personal information, demonstrating that their data collection and use practices meet the plain language "reasonably necessary and proportionate" standard under the CCPA. Critically, personal information must be interpreted and defined as it is practiced by businesses themselves, namely every piece of personal information tied to an individual consumer, including behavioral and preference data. Risk assessments that don't report "actual and potential value" will fall short of CPRA statutes.

AUTOMATED DECISIONMAKING

Addressing algorithmic discrimination and identifying how that is manifested in automated decisionmaking will be a unique challenge for the CPPA. As Professor Safiya Noble wrote in *Algorithms of Oppression* (2018) and testified before the CPPA Board of Directors in May 2022, if the right to be forgotten is to be extended to all personal data, that data must first be identified and accounted for. Many technology companies have well-fortified copyright defenses to prevent such accounting, and the CPPA should prepare for tough regulatory and statutory roadblocks to reach that. As a starting point, the CPPA may wish to consider a position that no consumer datasets are shielded from privacy audits and all should be subject to a legal presumption of transparency.

Inevitably, if the CPPA is to meet its charge to regulate specified automated decisionmaking technologies it will be necessary to audit the algorithms themselves. Ms. Cathy O'Neil, author of "Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy," offers a model to identify algorithms that are implicitly or explicitly corrupted by discrimination and bias.

1. ***Opacity***. Algorithms that can't be seen and evaluated by a range of perspectives inevitably reflect the biases of founders and favor target customers, typically without the awareness of consumers-at-large.
2. ***Scale***. Algorithms with limited use or subject to ample alternatives are often not harmful to consumers. However, as size grows and alternatives diminish, the risk to consumer privacy grows as well.
3. ***Design***. Algorithms that purport to save consumers money or solve social problems sometimes disadvantage consumers who are oblivious to their existence or impact. For example, the discrete collection of personal driving practice information allows insurers to cream skim the "safest" drivers into low-cost insurance pools, while driving up insurance costs for drivers with less stellar data records, an outcome contrary to the central premise of private insurance.

These three criteria may be starting point for the CPPA to develop privacy regulations that apply to business sectors of all sizes and functions, helping the CCPA fully and fairly assess the impact of automated decisionmaking.

Thank you for considering these remarks. I am available to answer questions and add details to my comments provided. I wish the CPPA great success in moving ahead with its rulemaking and implementation process.

Very respectfully,

Dave O'Toole

From:	Benway, Kathleen [redacted]
Sent:	Monday, March 27, 2023 1:15 PM
To:	Regulations
Cc:	Avonne Bell; Felz, Daniel; Oh, Hyun Jai
Subject:	PR 02-2023 - Comment from CTIA -The Wireless Association
Attachments:	CTIA - Comment on Preliminary Rulemaking (3.27.2023) FINAL.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

To the California Privacy Protection Agency,

In response to the Agency's Invitation for Preliminary Comments date February 10, 2023, please find attached the comments of **CTIA – The Wireless Association**. Please feel free to contact me directly if you have any issues accessing the attached document.

Kind regards,

Kathleen Benway
Partner
Alston & Bird LLP
950 F Street, NW, Washington, DC 20004
[redacted] O I [redacted] C
[redacted]

Before the
California Privacy Protection Agency

In the Matter of California Privacy Rights Act of 2020 Rulemaking Process	)))))))	Invitation for Preliminary Comments on Proposed Rulemaking

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Avonne Bell
Director, Connected Life

Jake Lestock
Director, State Legislative Affairs

CTIA
1400 16th St. NW, Suite 600
Washington, DC 20036

(202) 736-3200
www.ctia.org

March 27, 2023

TABLE OF CONTENTS

Before the
California Privacy Protection Agency

In the Matter of	)	
	)	
California Privacy Rights Act of 2020	)	Invitation for Preliminary
Rulemaking Process	)	Comments on Proposed Rulemaking
	)	
	)	

INTRODUCTION

CTIA[1] appreciates the opportunity to provide these comments in response to the California Privacy Protection Agency's (the "Agency's") invitation for preliminary comments on proposed rulemaking under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA").[2] CTIA commends the Agency's efforts to closely evaluate the potential impact of rulemaking regarding cybersecurity audits, risk assessments and automated decision making.

On November 8, 2021, CTIA submitted preliminary comments to the Agency on these topics ("CTIA's November 2021 Comment"). This filing supplements and updates CTIA's November 2021 Comment to more directly respond to the questions the Agency has posed in its present invitation for preliminary comments.

[1] CTIA – The Wireless Association® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] In keeping with the terminology used by the Agency in prior rulemaking, CTIA uses the acronym "CCPA" to collectively refer to the California Consumer Privacy act of 2018, as amended by the California Privacy Rights Act of 2020, and as supplemented by regulations issued under these enactments.

I. Cybersecurity Audits – Civil Code § 1798.185(a)(15)(A)

The CCPA authorizes the Agency to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' … security" to perform annual cybersecurity audits.[3]

In response to the cybersecurity audit questions posed by the Agency, CTIA addresses the following main points, each discussed in further detail below:

- Cybersecurity audits should be obligatory only when, as established by the CCPA, the need for such audits is objectively reasonable – *i.e.*, when the ordinary course of processing results in enumerated, consequential security risks. The Agency's regulations should then allow businesses to audit their cybersecurity programs comprehensively using reasonable frameworks, scope, and audit processes, which are provided by existing security audit frameworks.
- When businesses act under a widely-accepted, industry-standard security audit framework, the Agency should not require that such businesses demonstrate the reasonableness or other compliance characteristics of the framework.
- CTIA encourages the Agency to recognize that industry-standard cybersecurity frameworks meet CCPA standards for thoroughness and independence, as these frameworks are maintained and validated by third-party expert organizations or agencies.

[3] Civ. Code § 1798.185(a)(15)(A).

A. Questions I.1 and I.2: Laws and Best Practices for Cybersecurity Audits, Assessments, or Evaluations[4]

Question I.1. What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits? For the laws identified:

- ***a. To what degree are these laws' cybersecurity audit requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?***
- ***b. What processes have businesses or organizations implemented to comply with these laws that could also assist with their compliance with CCPA's cybersecurity audit requirements?***
- ***c. What gaps or weaknesses exist in these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?***
- ***d. What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?***
- ***e. Would you recommend that the Agency consider the cybersecurity audit models created by these laws when drafting its regulations? Why, or why not?***

Question I.2. In addition to any legally required cybersecurity audits identified in response to question 1, what other cybersecurity audits, assessments, or evaluations that are currently performed, or best practices, should the Agency consider in its regulations for CCPA's cybersecurity audits pursuant to Civil Code § 1798.185(a)(15)(A)? For the cybersecurity audits, assessments, evaluations, or best practices identified:

- ***a. To what degree are these cybersecurity audits, assessments, evaluations, or best practices aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?***
- ***b. What processes have businesses or organizations implemented to complete or comply with these cybersecurity audits, assessments, evaluations, or best practices that could also assist with compliance with CCPA's cybersecurity audit requirements?***
- ***c. What gaps or weaknesses exist in these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?***
- ***d. What gaps or weaknesses exist in businesses or organizations' completion of or compliance processes with these cybersecurity audits, assessments, evaluations, or best practices? What is the impact of these gaps or weaknesses on consumers?***
- ***e. Would you recommend that the Agency consider these cybersecurity audit models, assessments, evaluations, or best practices when drafting its regulations? Why, or why not? If so, how?***

[4] CTIA provides the following comment as generally responsive to the Agency's Questions I.1 and I.2, including their subparts.

A number of "laws that currently apply to businesses" and industry standards have relevance to cybersecurity audits under Section 1798.185(a)(15) – starting with the CCPA itself. As the Agency considers regulations relating to cybersecurity audits, it should seek to align those regulations with existing statutory requirements and industry standards relating to security procedures and practices under the CCPA. Notably, in Section 1798.100(e) of the CCPA, California legislators and voters established that businesses' "security procedures and practices" must be "reasonable" and "appropriate" to the nature of the personal information. Accordingly, Section 1798.185(a)(15)(A)'s rulemaking grant to define the required "scope of the audit" and "a process to ensure that audits are thorough and independent" should be read in light of CCPA's overarching reasonableness-based approach.

In addition, cybersecurity audits should only be obligatory when the burden and expense of an audit is objectively reasonable and necessary, *i.e.*, when enumerated, consequential security risks arise in the ordinary course from processing. If such a risk is present, the Agency's rulemaking should allow businesses to evaluate relevant cybersecurity practices using reasonable (a) frameworks, (b) scope, and (c) processes to conduct audits. CTIA addresses each of these aspects in turn, below:

1. Cybersecurity audits should be triggered exclusively by impactful security risks.

To facilitate reasonable and appropriate auditing obligations, the Agency should define "significant risk" narrowly and require businesses to conduct a cybersecurity audit only when engaging in specific, enumerated activities that present a cybersecurity risk.

Under the CCPA's overarching reasonableness-based approach, the Agency's rulemaking should focus on processing activities that have significant, consequential effects on cybersecurity that impact consumers. Security audits should be required only when engaging in enumerated

activities that present identified material cybersecurity risks. If the definition of "significant risk" is too broad, it will trigger a high volume of cybersecurity audits, even in situations where little to no risk to consumers exists. Quantitatively more audits, covering fewer consequential risks, does not meaningfully improve cybersecurity protection, but rather detracts from it by diverting needed resources away from activities that actually raise impactful risks. A broad, un-enumerated definition of "significant risk" may thus negatively impact consumer protection.

Moreover, the obligation to conduct cybersecurity audits should only be triggered by significant "security" risks and not by "pure privacy" risks. Cybersecurity risks are inherently different from privacy risks. Businesses identify, classify, and remediate cybersecurity risks under different frameworks than they apply to privacy risks. The CCPA and other state privacy laws already recognize this distinction.[5] For example, the CCPA states that the "factors to be considered in determining when processing may result in significant risk to the ***security*** of personal information shall include the size and complexity of the business and the nature and scope of processing activities."[6] In comparison, the CCPA envisions that risk assessments will evaluate risks to "the ***privacy of the consumer***."[7] Therefore, a pure privacy risk should not trigger an obligation to conduct a cybersecurity audit.

2. Reasonable audit frameworks should be permitted.

When a significant security risk makes a cybersecurity audit reasonable to conduct, CTIA encourages the Agency to permit businesses to use existing, widely-accepted cybersecurity frameworks as a safe harbor to CCPA audit requirements, such as those of the International

[5] *See* Civ. Code § 1798.185(a)(15); Colo. Rev. Stat. §§ 6-1-1308(5), 6-1-1309; Conn. Act 22-15, §§ 6(a)(3), 8(a); Va. Code §§ 59.1-578(A)(3), 59.1-580(A).

[6] Civ. Code § 1798.185(a)(15)(A) (emphasis added).

[7] Civ. Code § 1798.185(a)(15)(B) (emphasis added).

Organization for Standardization ("ISO") 27000 series certification,[8] National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF"),[9] Payment Card Industry Data Security Standard ("PCI DSS"),[10] Cybersecurity Maturity Model Certification ("CMMC"),[11] Capability Maturity Model Integration ("CMMI"),[12] and System and Organization Controls ("SOC") standards.[13]

Permitting existing industry-standard audit frameworks would align with the CCPA's stated goals of facilitating "reasonable" and "appropriate" security. Entire industries already rely on, and businesses regularly conduct, audits pursuant to such frameworks, which embody expertise in cybersecurity and are routinely updated to address emerging risks and accepted controls. Further, these standards may already be mandatory for some businesses in certain industries. For example, PCI standards are routinely mandated by contract for companies that process cardholder data. Requiring diverging standards for CCPA cybersecurity audits could impair businesses' ability to meet industry security standards or contractually-imposed security standards.

Other U.S. states have already enacted statutory safe harbors for businesses whose security

[8] *E.g.*, ISO, ISO/IEC 27001:2022 (2022).

[9] NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[10] *E.g.*, PCI, DATA SECURITY STANDARD: REQUIREMENTS AND TESTING PROCEDURES, VERSION 4.0 (2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf.

[11] DEP'T OF DEF., CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) MODEL OVERVIEW (2021), https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf; NIST, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf; NIST, ENHANCED SECURITY REQUIREMENTS FOR PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.

[12] CMMI Inst., *CMMI*, https://cmmiinstitute.com/cmmi.

[13] *E.g.*, Am. Inst. Certified Pub. Accts., *SOC 2® - SOC for Service Organizations: Trust Services Criteria*, https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.

programs reflect these existing cybersecurity frameworks.[14] Similarly, NIST's risk management standards, including the NIST CSF, were designed to enable federal government agencies, many of which process more extensive and sensitive data than many businesses subject to the CCPA, to comply with their statutory information security obligations.[15] CTIA encourages the Agency to consider similar recognition of these frameworks in the context of CCPA cybersecurity audits. Accordingly, ISO, NIST, SOC, CMMC, CMMI, or similar standards should be considered "reasonable" and "appropriate" frameworks under which to conduct CCPA cybersecurity audits.

Permitting audit frameworks such as ISO, NIST, SOC, CMMC, CMMI, and others also helps address the Agency's concerns about "gaps and weaknesses" in "cybersecurity audits, assessments, evaluations, or best practices." These frameworks are continuously updated to *avoid* gaps or weaknesses in the protection they offer. As new technologies – as well as associated risks – arise, these cybersecurity frameworks are a flexible mechanism to swiftly introduce accepted controls and best practices. The CCPA itself contemplates that the "law should adjust to technological changes"[16] and requires businesses to take into account available technology[17] – and these frameworks are built to accomplish just that. Compared to these flexible and continually evolving cybersecurity frameworks, audit frameworks that are "hard-coded" into regulations may rapidly become outdated and obsolete, since they would need to be regularly (and sometimes very quickly) updated through new rulemaking. CTIA submits that the Agency should therefore favor

[14] *See, e.g.*, Ohio Rev. Code § 1354.03(A)(1) (establishing safe harbor for cybersecurity programs that comply with NIST, Federal Risk and Authorization Management Program (FedRAMP), Center for Internet Security (CIS), or ISO standards); Utah Code §§ 78B-4-701 to 706 (same).

[15] *See, e.g.*, NIST, *NIST Risk Management Framework: Federal Information Security Modernization Act (FISMA) Background*, NIST.GOV (last updated Feb. 23, 2023), https://csrc nist.gov/Projects/risk-management/fisma-background.

[16] *See* California Privacy Rights Act of 2020 Ballot Initiative, § 3(C)(4).

[17] Civ. Code § 1798.185(a)(7).

the existing, widely-accepted frameworks that can continuously account for an evolving risk environment.

Lastly, businesses should be able to memorialize audit results using report formats based on the above widely-accepted cybersecurity frameworks. The Agency would create unnecessary procedural burden if it were to create a California-specific format for cybersecurity audit reports. Instead, the above frameworks provide broadly-followed report formats that are readily understood, and which the Agency's rulemaking should not displace.

3. Audits should be reasonable in scope.

In keeping with the reasonableness approach established by the CCPA, the Agency should allow a single cybersecurity audit that comprehensively assesses the business's security program to cover all "significant risks" giving rise to CCPA audit requirements. The Agency should not require separate audits for each specific "significant risk," as this would be overly burdensome and not aligned with existing best practices under industry-standard cybersecurity frameworks.

The common practice under ISO, NIST, SOC, or similar standards is to audit an organization's security program as a whole. This approach assesses whether the business's security program conforms to the control objectives of the applicable audit framework. Such an assessment, conducted comprehensively at the programmatic level, enables security audits to evaluate and validate whether the audited organization has implemented cybersecurity measures throughout its organization that are appropriate to the risks of its personal information processing.

Accordingly, even if one or more discrete "significant risks" initially trigger a business's obligation to conduct a CCPA cybersecurity audit, CTIA submits that the Agency should not require businesses to conduct separate cybersecurity audits for *each* specific activity that may involve a significant security risk. Instead, a single comprehensive audit of the business's

cybersecurity program, conducted under a recognized audit framework, should be considered sufficient to satisfy CCPA audit obligations. CTIA notes the CCPA itself does not appear to permit the Agency to mandate separate, risk-specific audits; it only empowers the Agency to issue regulations requiring businesses to "[p]erform ***a*** cybersecurity audit on an annual basis."[18] The Agency would thus exceed its rulemaking authority if it requires multiple risk-specific cybersecurity audits.

Moreover, as a practical matter, security risks will often be intertwined with one another, so auditing and addressing individual risks in isolation would prove not only burdensome, but also impractical. Allowing a single comprehensive audit to address an organization's cybersecurity program is consistent with the CCPA's rulemaking grant, as well as with the approaches outlined above under broadly-accepted security frameworks.

4. Businesses should be permitted to employ a reasonable audit process.

The Agency should permit businesses to use reasonable audit processes and leverage appropriately-structured internal audit processes to conduct CCPA cybersecurity audits. External cybersecurity audits should be permitted, but not required, to satisfy CCPA cybersecurity audit requirements.

Internal audits, when properly structured, constitute a reasonable approach to satisfying the CCPA's audit requirements. Many businesses have already implemented internal cybersecurity auditing processes, particularly through their own information security or audit functions. As long as audit functions are reasonably designed to be independent, the Agency should permit companies' internal auditing processes to satisfy CCPA cybersecurity auditing requirements. This approach substantially lowers the burden for small- to medium-size businesses, and is more

[18] Civ. Code § 1798.185(a)(15)(A) (emphasis added).

consistent with the intended nature of CCPA cybersecurity audits as preventive – but not punitive – consumer-protection measures.

Notably, other California statutes already allow businesses to conduct statutory audits utilizing their internal resources provided that the businesses maintain appropriate internal structures around the audit function. For instance, the California Insurance Code permits internal audits, stating that "[t]o ensure that an internal auditor remains objective, the internal audit function shall be organizationally independent," and that the "internal audit function shall not defer ultimate judgment on audit matters to others."[19]

Other recent statutory and regulatory cybersecurity frameworks with auditing obligations also permit internal auditing of security programs. For example, the Federal Trade Commission's recently-updated Safeguards Rule for financial institutions under its jurisdiction requires in-scope institutions to evaluate their information security programs, but does not require external audits.[20] Similarly, the National Association of Insurance Commissioners' ("NAIC") Insurance Data Security Model Law requires insurers to "monitor, evaluate and adjust, as appropriate, [their] Information Security Program" – but it also does not require external auditing.[21] These indicate internal auditing is already seen as reasonable and appropriate for financial services and insurance companies, which in turn suggests the Agency should view internally-conducted audits as broadly

[19] Ins. Code § 900.3(a), (c).

[20] *See* 16 C.F.R. § 314.4(g), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314 ("In order to develop, implement, and maintain your information security program, you shall [] [e]valuate and adjust your information security program in light of the results of the testing and monitoring …; any material changes to your operations or business arrangements; the results of risk assessments performed under … this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.").

[21] NAIC, INSURANCE DATA SECURITY MODEL LAW at § 4(G) (2017), https://content.naic.org/sites/default/files/inline-files/MDL-668.pdf.

sufficient for businesses under the Agency's CCPA jurisdiction. The Agency should, therefore, permit businesses to leverage their existing internal procedures to satisfy CCPA requirements.

To be clear, CTIA is suggesting that the Agency should permit third-party auditing to satisfy CCPA auditing requirements—but should not require it. If a business already engages an external auditor to conduct cybersecurity audits, such third-party audits should be accepted as satisfying CCPA audit requirements. But the Agency should not force businesses to engage third parties to conduct cybersecurity audits. Requiring third party audits would go well beyond the "reasonable" and "appropriate" approach to cybersecurity that the CCPA envisions. Due to its burdensome expense and disruption, mandatory external auditing is more akin to a punitive measure than a preventive measure, and thus, is inconsistent with the objectives of CCPA Section 1798.185(a)(15)(A). A blanket requirement for third-party auditors is particularly hindering for small- to medium-sized enterprises, and may disproportionately impact smaller businesses that provide essential services but do not generate high margins. Lastly, it is unnecessary to mandate external audits as the Agency's current draft rulemaking seeks to empower the Agency itself to "audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA."[22]

B. Question I.3: Demonstrating that Cybersecurity Audits Comply with the CCPA

<u>Question I.3</u>. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted cybersecurity audits that the business completed to comply with the laws identified in question 1, or if the Agency accepted any of the other cybersecurity audits, assessments, or evaluations identified in question 2? How would businesses demonstrate to the Agency that such cybersecurity audits, assessments, or evaluations comply with CCPA's cybersecurity audit requirements?

[22] Draft Cal. Code Regs. § 7304(a) (last updated Feb. 3, 2023).

As stated above, CTIA submits that the CCPA's primary "cybersecurity audit requirement[]" is that audits are reasonable in terms of framework, scope, and process. If a business audits itself under one of the widely-accepted frameworks outlined above – such as ISO, SOC, or NIST – it would seem excessive to require that businesses also "demonstrate" the reasonableness or other compliance characteristics of the framework. These frameworks are maintained by independent organizations (or agencies) with extensive cybersecurity expertise, and are subject to regular updates consistent with the ever-changing risk environments. Indeed, the Office of the California Attorney General has previously suggested that businesses reference widely-recognized cybersecurity frameworks, such as the NIST CSF, as part of cybersecurity best practices.[23]

II. Risk Assessments – Civil Code § 1798.185(a)(15)(B)

The CCPA authorizes the Agency to issue regulations requiring businesses to submit "risk assessments" for processing activities that present significant risk to consumers' privacy.[24] In response to the questions posed in the Agency's invitation for preliminary comments, CTIA addresses the following main points, each discussed in further detail below:

- The definition of "significant risk" should align with the triggers already present in other U.S. state privacy statutes for data protection assessments. The mandatory content of risk assessments should align with the CCPA's rulemaking grant as well as other U.S. state privacy statutes and best practices.
- Businesses should only be required to submit a summary risk assessment to the Agency every two to three years, and the Agency should implement appropriate

[23] *See, e.g.*, KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T JUSTICE, CYBERSECURITY IN THE GOLDEN STATE (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/2014_cybersecurity_guide.pdf.

[24] Civ. Code § 1798.185(a)(15)(B).

safeguards to protect these submitted summary assessments and the information they contain.

- The Agency should engage in a formal administrative action pursuant to CCPA Section 1798.199.45 to access the complete content of risk assessments.

A. Questions II.1 and II.3: Laws or Other Requirements that Currently Require Risk Assessments[25]

Question II.1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments? For the laws or other requirements identified:

a. ***To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?***
b. ***What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA's risk-assessments requirements (e.g., product reviews)?***
c. ***What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?***
d. ***What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?***
e. ***Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?***

Question II.3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):

a. ***What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?***
b. ***What other models or factors should the Agency consider? Why? How?***
c. ***Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?***
d. ***What processing, if any, does not present significant risk to consumers' privacy or security? Why?***

[25] CTIA provides the following comment as generally responsive to the Agency's Questions II.1 and II.3, including their subparts.

CTIA supports the requirement to conduct risk assessments as a pro-privacy tool. Indeed, CTIA's members are already performing robust and meaningful data protection assessments to assess processing risks and benefits, and to protect the privacy of their customers. CTIA thus encourages the Agency to draft regulations that align CCPA risk assessment requirements with existing best practices and current statutory standards in state privacy laws. This approach would best embody the CCPA's statutory goals of enabling organizations to "identify and weigh" the risks and benefits of data processing, while advancing meaningful consumer protection and enabling interoperability of assessments across jurisdictions. Below, CTIA addresses each of these in turn:

1. The "significant risk" that triggers CCPA risk-assessment obligations should be consistent with existing state statutory standards and best practices.

The Agency should define the "significant risk" that triggers CCPA risk-assessment obligations as occurring only when businesses engage in specific, enumerated activities that present a heightened privacy risk to consumers. This would ensure consistency with existing state statutory standards and best practices, thus aligning with the CCPA's goals for risk assessments and other U.S. state privacy laws.

First and foremost, the CCPA's stated statutory goal is for risk assessments to "identify[] and weigh[] the benefits resulting from the processing … against the potential risks to the rights of the consumer …, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing."[26] This goal is best met by focusing the definition of "significant risk" – which triggers assessment obligations – on enumerated processing activities that present specific risks of substantial and identified harm to

[26] Civ. Code § 1798.185(a)(15)(B).

consumers. This would enable focused assessments that meaningfully increase consumer privacy, while also facilitating the Agency's oversight function.

This impact-focused approach to "significant risk" can be achieved by aligning the CCPA regulations with other U.S. state privacy laws. The Colorado Privacy Act (the "CPA"), Connecticut Data Privacy Act (the "CTDPA"), and Virginia Consumer Data Protection Act (the "VCDPA") limit the triggers for "data protection assessments" (DPAs) to statutorily enumerated activities, such as (a) processing for targeted advertising, (b) personal information sale, (c) profiling that presents a reasonably foreseeable risk of enumerated substantial injuries to consumers, and (d) processing of sensitive data.[27]

Requiring risk assessments beyond these enumerated activities would run afoul of the CCPA's statutory goal of addressing higher-risk activities where "risks to privacy [may] outweigh the benefits resulting from processing,"[28] compelling companies to divert resources to conduct risk assessments even when no impactful risk is present. As an example of a potentially overbroad risk-assessment obligation that would not meaningfully advance consumer privacy, CTIA urges the Agency not to require risk assessments merely for "large-scale" processing – or merely based on a "large number" of impacted consumers. Numerous companies, including small businesses, collect and manage large numbers of email addresses, but merely having a large number of email addresses on file does not itself create an impactful risk to consumers. An overly broad definition of "significant risk" would potentially require risk assessments even for such low-impact activities – requiring a wide swath of businesses to conduct numerous, likely formulaic, risk assessments about activities that do not present impactful risks to consumers. This will not increase consumer

[27] Colo. Rev. Stat. § 6-1-1309; Conn. Act 22-15, § 8(a); Va. Code § 59.1-580(A).

[28] Civ. Code § 1798.185(a)(15)(B).

privacy protection.

2. The mandatory content of risk assessments should enable a thoughtful weighing of risk and benefits, and not require a check-the-box exercise.

The CCPA's stated statutory goals for risk assessments are best fulfilled by aligning the mandatory content for risk assessments with existing statutory requirements for data protection assessments under other U.S. state privacy laws. In striking similarity to the CCPA, other U.S. state privacy statutes currently enacted require data protection assessments to "identify and weigh the benefits that may flow … from the processing … against the potential risks to the rights of the consumer …, as mitigated by safeguards that the controller can employ to reduce the risks."[29] At their core, both the CCPA and other U.S. state privacy laws agree that risk assessments should conduct a meaningful analysis of (a) the benefits of a processing activity, against (b) the risks of that activity, as mitigated by safeguards implemented by the business. This can be achieved by risk assessments that identify the processing activity, describe its intended use cases, and then weigh and balance the relevant risks – as mitigated by the business. Such an approach encourages businesses to focus on the substance of risks that processing may create, as opposed to conducting the check-the-box exercises that can arise when further factors are mandated for consideration in every assessment, regardless of relevance.

CTIA thus encourages the Agency to follow the CCPA's statutory focus on "identify[ing] weigh[ing] the benefits resulting from the processing … against the potential risks to the rights of the consumer,"[30] and align the content requirements for CCPA risk assessments with the content required under U.S. state privacy laws. This outcome aligns with the goals of the CCPA, advances consumer protection, and promotes interoperability.

[29] *E.g.*, Colo. Rev. Stat. § 6-1-1309(3).

[30] Civ. Code § 1798.185(a)(15)(B).

3. The Agency should permit risk assessments to evaluate entire processing activities generally.

CTIA encourages the Agency to permit risk assessments to evaluate entire processing activities generally, without requiring individualized risk assessments for each system or application that may be part of a broader processing activity. The CPA, CTDPA, and VCDPA all permit a "single data protection assessment" to "address a comparable set of processing operations that include similar activities."[31] This is a pragmatic approach that enables businesses to conduct more meaningful risk assessments, addressing related processing activities based on the commonality of risk they present. In contrast, requiring risk assessments at the level of individual systems or application needlessly multiplies the quantity of risk assessments, without actually addressing any additional risk.

4. The risks that trigger a risk assessment should be separate and distinct from the risks that trigger a cybersecurity audit.

Lastly, the risks that trigger a risk assessment should be separate and distinct from the risks that trigger a cybersecurity audit. Only a significant ***privacy*** risk should require a risk assessment. In contrast, only a significant ***cybersecurity*** risk should require a cybersecurity audit. Businesses' processes for privacy risks assessments are generally separate from their processes for cybersecurity audit. Indeed, generally, privacy risks are organizationally managed by entirely separate functions than cybersecurity risks. To use the Agency's terminology from Question II.3.c, CTIA urges the Agency to have one set of "models or factors" for risk assessments, and a separate set of "models or factors" for cybersecurity audits. Any other approach risks major disruptions for businesses, confusion among appropriate assessment and auditing factors, and unnecessarily making good-faith compliance burdensome and difficult.

[31] Colo. Rev. Stat. § 6-1-1309(5); Conn. Act 22-15, § 8(d); Va. Code § 59.1-580(D).

B. Question II.4: Minimum Content of Risk Assessments

<u>Question II.4</u>. What minimum content should be required in businesses' risk assessments? In addition:

- ***a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?***
- ***b. What, if any, additional content should be included in risk assessments for processing that involves automated decisionmaking, including profiling? Why?***

As stated above, CTIA supports aligning the mandatory content of risk assessments with the statutory text of the CPA, CTDPA, and VCDPA. Requiring additional mandatory content for certain types of processing activities, such as automated decisionmaking, would be counterproductive to the CCPA's stated goal of risk assessments, *i.e.*, a frank analysis that "identif[ies] and weigh[s] the benefits resulting from the processing … against the potential risks to the rights of the consumer." Additional mandatory items to be included in risk assessments can be overly prescriptive, burdensome, and not interoperable with standards across U.S. states. A lengthy and prescriptive list of additional risk assessment content risks working against the goals of risk assessments. Risk assessments can quickly become check-the-box exercises instead of thorough, meaningful analyses of impactful risks. The content mandated by the statutory text of the CPA, CTDPA, and VCDPA is sufficient to analyze processing activities – including automated decisionmaking – and to build privacy protections for them.

C. Question II.5: Accepting Assessments Completed under GDPR or CPA

<u>Question II.5</u>. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?

Please see CTIA's comment in response to Questions II.1 and II.3 above. CTIA supports interoperability of risk assessments among jurisdictions. In this vein, CTIA encourages the Agency

to align the requirements for risk assessments with the applicable statutory requirements under the CPA, CTDPA, and VCDPA.

D. Question II.6: Format of Risk Assessments

Question II.6. In what format should businesses submit risk assessments to the Agency? In particular:

- ***a. If businesses were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business):***
  - ***i What should these summaries include?***
  - ***ii In what format should they be submitted?***
  - ***iii How often should they be submitted?***
- ***b. How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements (e.g., summaries signed under penalty of perjury)?***

CTIA believes businesses' ability to engage in frank, open, and meaningful analysis of their processing activities is critical to the effective protection of consumers' privacy rights. To facilitate such analysis, businesses should only be required to submit a summary risk assessment to the Agency. The Agency should also implement adequate safeguards to protect such summary assessments and their contents. When there is a need to access a full risk assessment, the Agency should engage in a formal administrative process. CTIA discusses these primary points in more detail below:

1. Businesses should only be required to submit a summary risk assessment to the Agency, instead of submitting every risk assessment conducted by the businesses.

CTIA agrees with the Agency's suggestion in its Question II.6 that businesses should not be required to submit every separate risk assessment the business has conducted to the Agency. Instead, businesses should submit a summary of the risk assessments they have conducted over a specified period of time (and as outlined below, CTIA suggests a two- to three-year period).

Submitting a single summary of risk assessments, instead of every single risk assessment, better aligns with the CCPA's statutory text. The CCPA empowers the Agency's regulations to require businesses to "[s]ubmit … on a regular basis ***a*** risk assessment with respect to their processing of personal information."[32] This language indicates the CCPA envisions organizations making a single submission to the Agency, containing a summary generally addressing in-scope processing activities. By its express language, the CCPA's text does not contemplate businesses submitting every risk assessment they conduct.

This approach is consistent with the goal of enabling meaningful oversight by the Agency, while protecting against the disclosure of proprietary information or trade secrets. It also allows organizations to engage in thoughtful assessments with full and open discussions, including with legal counsel; whereas a requirement to over-produce all risk assessments will chill the ability for organizations to engage in meaningful open dialogue and analysis. When the Agency believes more information is necessary, the Agency can seek to employ its investigative powers under the CCPA, as discussed in Section II.D.3. below.

CTIA also suggests that summary risk assessments should be submitted to the Agency every two to three years. A two- to three-year submission cadence strikes an appropriate balance while enabling effective oversight by the Agency.

2. The Agency should implement appropriate safeguards to protect summary risk assessments and the information they contain.

CTIA trusts that the Agency will implement safeguards appropriate to protect any personal information, or any confidential or proprietary information, contained in or otherwise obtained in connection with risk assessment submissions. Safeguards could include widely-accepted measures

[32] Civ. Code § 1798.185(a)(15)(B) (emphasis added).

such as retention periods reasonable in light of the security risks associated with storage of risk assessments, as well as access controls that reflect the internal functional divisions within the Agency.

Additionally, as compelled disclosures to the Agency, it would be appropriate for risk assessments to be exempted from Freedom of Information Act (FOIA) requests under California law, and for the CCPA rules to specify that nothing in or provided in connection with a risk assessment results in a waiver of any evidentiary or other privilege available to a submitting party under applicable law.

3. Accessing full risk assessments should require formal administrative action pursuant to CCPA Section 1798.199.45.

Allowing the Agency to access risk assessments, without any reasonable parameters in place for their access or use, may disincentivize businesses from using these pro-privacy tools. Businesses may be hesitant to put meaningful content in their risk assessments, including any in-depth analysis of risks. Accordingly, CTIA submits that the Agency's regulations should require formal administrative action pursuant to CCPA Section 1798.199.45 in order to obtain full copies of risk assessments.

This approach aligns with privacy statutes enacted in other states. Connecticut and Virginia recognize the importance of procedural protections for the confidentiality of data protection assessments. Accordingly, each requires their respective attorney general to open an investigation and propound a civil investigative demand in order to obtain full risk assessments.[33] The Agency's regulations should consider a similar approach, and require formal administrative action to obtain full risk assessments.

[33] Conn. Act 22-15, § 8(c); Va. Code § 59.1-580(C).

III. Automated Decisionmaking – Civil Code § 1798.185(a)(16)

The CCPA empowers the Agency to issue regulations governing consumers' "access and opt-out rights with respect to businesses' use of automated decisionmaking technology."[34] As described below, CTIA submits that automated decisionmaking ("ADM") technology has been broadly beneficial to consumers and society, and that any forthcoming rulemaking should continue to encourage beneficial ADM uses. CTIA then responds to the Agency's ADM questions by submitting that (a) the CCPA's delegation of rulemaking authority to create ADM rights is insufficient, and would result in unconstitutional rulemaking; and (b) if the Agency nonetheless drafts ADM regulations, it should align its rulemaking with the standards already established by other U.S. state privacy laws and impose consistent obligations across all industries.

A. Question III.4: How Business Use ADM Technologies, Including ADM's Positive Impact

Question III.4. How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.

Because CTIA believes the positive aspects of ADM provide a helpful backdrop for discussing how ADM rulemaking should be structured, CTIA first responds to the Agency's Question III.4 prior to addressing the Agency's further ADM questions. CTIA submits that ADM has had many positive impacts for consumers. These positive impacts are worth highlighting, and CTIA encourages the Agency to consider them when engaging in upcoming rulemaking. The CCPA regulations should not chill the many existing beneficial uses of ADM, or discourage businesses from developing future ADM-driven innovations that are beneficial to consumers or society.

[34] Civ. Code § 1798.185(a)(16).

ADM has enabled new technologies and products such as mobile payments and online financial services, and these developments have had broadly positive outcomes for consumers. For instance, consumers can now purchase practically any product they want from their mobile phones, thanks in significant part to fraud-prevention technology that runs on automated decision engines. Consumers can also apply for and receive a broad range of financial products and services fully online, without needing to go through the traditionally burdensome process of physically going to a bank and negotiating with bank staff or loan officers. These developments happened in substantial part because the processes of online payments and financial services could utilize ADM.

Similarly, ADM technology is helpful in providing "unseen" protection to consumers. It helps telecommunications companies prevent robocalls. It can also power much of the security architecture on important IT infrastructure such as antivirus and intrusion-detection technology. Again, these ADM technologies have led to broadly positive developments for society as a whole, as well as for consumers.

Ultimately, the goal of automated-decisionmaking technology is to eliminate potential biases and inconsistencies often present in human decisions. Human decisions can be subjective and inconsistent, and customers may receive different outcomes – and entirely different experiences – simply by calling a different person. In contrast, proper use of ADM can improve outcomes by making beneficial experiences more consistent across consumers, while lowering associated costs for consumers, businesses, and society. The Agency's regulations should be driven by these goals, and should avoid an overbroad reach that would chill the use of beneficial ADM that does not implicate legally or otherwise consequential decisions.

B. Questions III.1, III.2, and III.3: Laws, Frameworks, and Best Practices Concerning Access and Opt-Out Rights for ADM[35]

Question III.1. ***What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?***

Question III.2. ***What other requirements, frameworks, and/or best practices that address access and/or opt-out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?***

Question III.3. ***With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:***

- ***a. How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?***
- ***b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?***
- ***c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decisionmaking technology requirements?***
- ***d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?***
- ***e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?***
- ***f. Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, how?***

First, CTIA submits that the CCPA's grant for ADM rulemaking does not confer authority to create ADM-related access and opt-out rights, and that such rights created by the Agency would therefore be unconstitutional. Second, if the Agency nonetheless proceeds with ADM rulemaking,

[35] CTIA provides the following comment as generally responsive to the Agency's Questions III.1 – III.3, including their subparts.

CTIA requests that the Agency align with ADM rights approaches that have been enacted by statute in other U.S. states. CTIA discusses these points in more detail below:

1. Agency rulemaking creating an access and opt-out right for automated decisionmaking would be unconstitutional.

Prior to addressing the substance of the Agency's questions, CTIA reiterates its position initially submitted to the Agency in CTIA's November 2021 Comment, that Agency rulemaking creating ADM access and opt-out rights on the basis of the CCPA's present rulemaking grant would be unconstitutional. The CCPA purports to grant the Agency authority to enact and create ADM-related access and opt-out rights through the following single sentence:

> *[The Agency shall adopt] regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.*[36]

Relying on this grant to creating ADM access and opt-out rights would be an unconstitutional delegation of authority. The CCPA itself does not create ADM rights, but rather obliquely references them in the single sentence cited above, then hands the entire fundamental policy issue of ADM rights to the Agency and tasks the Agency with establishing and developing ADM rights out of whole cloth. Under California precedent, rulemaking on this basis would be unconstitutional: "[A]n unconstitutional delegation of authority occurs when a legislative body (1) leaves the resolution of fundamental policy issues to others or (2) fails to provide adequate direction for the implementation of that policy."[37]

[36] Civ. Code § 1798.185(a)(16).

[37] *Gerawan Farming, Inc. v. Agricultural Labor Relations Bd.*, 405 P.3d 1087, 1100 (Ca. Sup. Ct. 2017) (citing *Carson Mobilehome Park Owners' Assn. v. City of Carson*, 672 P.2d 1297, 1299 (Ca. Sup. Ct. 1983)).

The issue can be clearly seen by contrasting the CCPA's approach to ADM rights with its approach to other consumer rights. As one example of how the CCPA handles other rights: for the verifiable consumer rights (Know, Delete, and Correct), the CCPA in each case (a) expressly establishes the substantive right (e.g., "*[a] consumer* ***shall have the right*** *to request that a business delete [] personal information*"[38]); (b) sets forth requirements for enabling consumers to exercise the right;[39] and (c) expressly enumerates exceptions to the right.[40] Only *after* having taken care of these fundamental policy issues does the CCPA delegate authority to the Agency to issue further regulations.[41] The CCPA's approach to Know, Deletion, and Correction rights shows what it looks like when the California legislature and voters resolve the fundamental policy issues associated with consumer privacy rights, then constitutionally delegate authority to the Agency to supplement these policy determinations with rulemaking.

This stands in stark contrast to how the CCPA addresses ADM access and opt-out rights. The CCPA's statutory text does not expressly create substantive ADM rights; it does not provide requirements for exercising ADM rights; and it does provide any exceptions to ADM rights. Instead, as shown above, the CCPA merely contains the single sentence – cited above – that instructs the Agency to adopt "regulations governing access and opt-out rights with respect to businesses' use of [ADM] technology."[42] Thus, in contrast to other CCPA rights, neither the California legislature nor California voters have done the work of making the fundamental policy

[38] Civ. Code § 1798.105(a); *see also id.* at §§ 1798.106(a) (Right to Correct), 1798.110(a), 1798.115(a) (Right to Know).

[39] *See, e.g.*, § 1798.130 (setting forth Notice, Disclosure, Correction, and Deletion Requirements).

[40] *See, e.g.*, Civ. Code § 1798.105(d) ("A business … shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for [eight expressly enumerated exceptions to the Right to Delete].").

[41] *See* Civ. Code § 1798.185(a)(7)-(9).

[42] Civ. Code § 1798.185(a)(16).

determinations that ADM rights can raise. Instead, the CCPA merely references the fundamental policy issue of ADM rights, then hands it to the Agency *in toto* so the Agency can make the substantive policy determinations that – for other CCPA rights – have been resolved by the legislature and voters within the CCPA's statutory text. As CTIA initially argued in CTIA's November 2021 Comment, this results in the legislature and voters "leav[ing] a fundamental policy issue to others." It thus would be unconstitutional for the Agency to now create ADM rights under the CCPA's present rulemaking grant, even if the CCPA purports to grant the Agency the power to do so.

Further, other California authorities are already engaged in parallel efforts to regulate ADM. Their approaches underscore the unconstitutionality that would result from ADM rulemaking based on the CCPA's single-sentence grant cited above. The Civil Rights Department has proposed modifications to its Employment Regulations that generally extend existing anti-discrimination rules so they also cover "automated-decision systems" used in employment.[43] Additionally, the California legislature is currently considering Assembly Bill ("AB") 331, which would regulate "automated decision tools" that are used for "consequential decisions."[44] Either of these frameworks would stand on firmer constitutional footing than ADM rulemaking issued under the CCPA. The Agency should consider deferring potentially unconstitutional ADM rulemaking as these proposals proceed – particularly in regards to AB 331, which aims to create a comprehensive ADM legislative framework.

---

[43] *See* CIV. RIGHTS COUNCIL, PROPOSED MODIFICATIONS TO EMPLOYMENT REGULATIONS REGARDING AUTOMATED-DECISION SYSTEMS (July 28, 2022), https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2022/07/Attachment-G-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf.

[44] *See* Assembly Bill (AB) 331 (as amended in Assembly Mar. 16, 2023), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB331.

If the Agency proceeds with ADM rulemaking, the Agency's rules should account for the parallel ADM rulemaking and legislation within California described above. ADM rulemaking under the CCPA should not create overlapping, conflicting, or confusing requirements or enforcement authorities. Neither consumers, business, nor the Agency would be served by inconsistent ADM rules.

2. If the Agency moves forward with ADM rulemaking, the Agency should align the CCPA regulations with standards of other U.S. state privacy laws.

If the Agency moves forward with access and opt-out rulemaking for ADM, CTIA encourages the Agency to align the regulations with the standards for ADM rights already established by other U.S. state privacy laws. To ensure consistency with these existing standards, CCPA access and opt-out rights for ADM should apply only when automated decisions: (a) are based on profiling, (b) are based on solely automated decisions, and (c) result in enumerated legal or similarly significant effects concerning consumers. Only when all three of these conditions are met should access and opt-out rights be triggered.

(a) Profiling. "Profiling" is a defined term under the CCPA;[45] therefore; tying access and opt-out rights to "profiling"-powered automated decisions creates a level of certainty as to the scope of such a right. This also has a policy justification: automated decisions based on profiling are more likely to have privacy impacts on consumers. Without a "profiling" limitation, the scope of consumer ADM rights will be boundless without any meaningful benefits to consumer privacy protection. For instance, without such a limitation, any

[45] Civ. Code § 1798.140(z) (defining "profiling" as "any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements").

decision based on software-encoded rules could trigger opt-out rights, even if there are no meaningful impacts on consumer privacy. CTIA also notes that all other existing U.S. state privacy laws have limited opt-out rights to automated decisions that are based on profiling.[46]

(b) Solely or Fully Automated Decisions. Next, CCPA access and opt-out rights should only be triggered by "solely" or "fully" automated decisions – not any decision that incorporates an automated component. This is the plain meaning of the word "automated" as used in the CCPA's statutory text. The CCPA's statutory text grants power to regulate technology that results in "automated decisionmaking," providing textual evidence that only "automated" decisions – *i.e.*, purely machine-made decisions – are in-scope for access and opt-out rights.

If ADM rights were to apply to *partially* automated decisions – or to ADM-*assisted* human decisions – each of which already have human involvement built into them, access and opt-out rights become overbroad and lose their policy justification. ADM rights are meant to insert a layer of human oversight into processes that would otherwise remain completely algorithmic. They were not intended to grant new rights over decisions where humans are already involved; otherwise they go beyond the CCPA's intent of regulating "automated" decisionmaking technology. Moreover, if consumers can opt-out of decisions that are partially, but not fully automated, it is unclear how companies should respond to such opt-out. It would appear that companies may need to either not make the decision at all (which does not benefit the consumer), or offer an "algorithm-free" or "solely manual" process for opted-out consumers – and this itself may reintroduce human unfairness and bias.

[46] Colo. Rev. Stat. § 6-1-1306(1)(a)(I)(C); Conn. Act 22-15, § 4(a)(5)(C); Va. Code § 59.1-577(A)(5)(iii).

(c) Enumerated Legal or Similarly Significant Effects. Lastly, ADM access and opt-out rights should only be triggered by automated decisions that result in legal or similarly significant effects concerning consumers. The mere fact that an algorithm makes a decision does not, in itself, cause potential harm to or even impact consumers. ADM should instead only trigger consumer rights when an algorithm produces legal or similarly significant impacts on a consumer (without human involvement as noted above). Accordingly, the Agency should align with the CPA,[47] CTDPA,[48] and VCDPA[49] and enumerate a list of specific decisions that have a legal or similarly significant effect that triggers ADM rights. Specifically, "legal or similarly significant effects" should be limited to decisions, made by the business, that provide or deny financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water, to the consumer. Creating ADM rights without this limitation would impose an unnecessary burden on businesses and disincentivize the advancement of decisioning technology, without actually furthering consumer privacy interests.

C. Question III.8: Access and Opt-Out Rights for ADM Should Not Vary by Industry

Question III.8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?

[47] Colo. Rev. Stat. § 6-1-1303(10).

[48] Conn. Act 22-15, § 1(12).

[49] Va. Code § 59.1-575.

Access and opt-out rights relating to ADM should not vary depending upon industry. ADM rights seek to mitigate the risk of consumers being subject to fully automated, legally consequential decisions without an opportunity for human review. Therefore, the regulations' focus should be on the type of consequences automated decisions will have, and the industry using the technology is not relevant to that analysis.

ADM regulations that are inconsistent across industries risk picking "winners" and "losers," with certain industries receiving preferential treatment while consumers interacting with those industries potentially receive less protection. In contrast, applying the same ADM rules regardless of industry can help avoid competitive distortions and gaps in regulatory protections. CTIA also notes that under all other U.S. state privacy laws that regulate ADM (Virginia, Colorado, and Connecticut), ADM requirements are consistent and do not distinguish among industries.

D. Question III.9: Information to Be Included in ADM Access Requests

Question III.9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer? In addition:

- ***a. What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?***
- ***b. How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?***

CTIA submits that the Agency should align the CCPA's access requirements with ADM transparency already required in other jurisdictions, mindful of the fact that – under the CCPA – consumers can already request the specific pieces of personal information businesses have collected about them.

CTIA agrees that consumers should have a meaningful understanding of ADM technologies that have consequential impacts on them. The CCPA's rulemaking grant for ADM access rights envisions providing consumers with "meaningful information about the logic involved" and "description of the likely outcome."[50] This is a sensible scope for information to be provided in the context of ADM rights. Thanks to consumers' Right to Know, consumers can already request the "specific pieces" of personal information a business may hold about them.[51] Therefore, the "ADM Access" right should be viewed as a supplement to, not a duplication of, consumers' existing Right to Know.

The CCPA's goal for the ADM Access right is therefore to give consumers meaningful information about purely automated decisions, as well as potential outcomes the consumer may receive, so that the consumer can decide whether to proceed. This aligns the CCPA's ADM Access right with ADM transparency rules already in force in other jurisdictions. For example, the GDPR requires a business that employs regulated ADM to provide concise and meaningful information about the logic involved and the likely consequences of automated decisions used.[52] Requiring businesses to disclose any further additional information will increase the burden on businesses and potentially require overly detailed technical explanations, creating consumer confusion. It also risks requiring businesses to divulge trade secrets.

Moreover, the Agency should empower businesses to 'respond to ADM Access requests in advance' by including meaningful information about ADM used, the logic involved, and likely outcomes in their privacy policies. This approach is consistent with the CCPA's general focus on notice. It would also help protect consumers because, instead of needing to undertake affirmative

[50] Civ. Code § 1798.185(a)(16).

[51] Civ. Code § 1798.110(a)(5).

[52] *See, e.g.*, Arts. 13(2)(f), 14(2)(g), 22(1), (4) GDPR.

efforts to submit an access request, consumers could receive required information about ADM simply by reading the business's privacy policy.

CONCLUSION

CTIA appreciates the Agency's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan
Vice President, State Legislative Affairs

Avonne Bell
Director, Connected Life

Jake Lestock
Director, State Legislative Affairs

CTIA

1400 16th St. NW, Suite 600
Washington, DC 20036

(202) 736-3200

March 27, 2023

From: MacGregor, Melissa [redacted]
Sent: Monday, March 27, 2023 1:18 PM
To: Regulations
Cc: Chamberlain, Kim
Subject: PR 02-2023
Attachments: SIFMA California AI Request March 27 2023 .pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Hello,
Please see the attached letter responding to PR 02-2023 - INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING.

Thank you.

Melissa MacGregor
Deputy General Counsel & Corporate Secretary
SIFMA
1099 New York Ave., Suite 600
Washington, DC 20001
O: [redacted]
M: [redacted]

sifma

Invested in America

March 27, 2023

VIA E-Mail to regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR 02-2023 - INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING

Dear California Privacy Protection Agency,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to provide feedback on the California Privacy Protection Agency ("CPPA") Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking dated February 10, 2023.[2] SIFMA members take cybersecurity and data protection seriously as it is a key component of client trust and confidence. In addition, SIFMA members are subject to a wide array of federal, state, and international laws and regulations governing cybersecurity and data protection. There are also significant requirements in place that would govern SIFMA members' use of artificial intelligence ("AI") that should also be considered in any CPPA rulemaking or guidance.

---

1 SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate on legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA"). For more information, visit http://www.sifma.org.

2 California Privacy Protection Agency, *Invitation for Preliminary Comments on Proposed Rulemaking Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking* (February 10, 2023) (available at https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf).

A. The CPPA rules governing cybersecurity risk and AI should take into account existing laws and regulations.

Most critically, the CPPA should take into consideration existing and future federal and state requirements and ensure that any rules promulgated closely align and provide sufficient flexibility to achieve compliance without unnecessary additional burdens on covered entities. To that end, any assessments or audits that companies perform as subjects of federal or state cybersecurity and artificial intelligence laws, regulations, or frameworks should also satisfy any related CPPA audit and assessment requirements.

Specifically, SIFMA members or their affiliates are already subject to, or will be subject to the following cybersecurity requirements:

- The SEC has proposed cybersecurity risk management rules that would require broker-dealers, investment advisers, funds, and other entities to periodically assess and draft documentation of cybersecurity risks.[3] The proposed rules also provide factors that must be considered when conducting risk assessments. Additionally, existing rules and recent SEC enforcement actions indicate that firms should take a risk-based approach in effectively managing cyber risks, which is the approach already taken by many financial institutions.

- FINRA explains in its Cybersecurity Report that broker-dealer firms should conduct a cybersecurity risk assessment or risk-based audit to determine risks in developing cybersecurity programs.[4]

- GDPR requires companies that engage consumers in the United Kingdom or European Union to conduct a Data Protection Impact Assessment where the processing data is likely to result in a high risk of harm to the rights and freedoms of natural persons who reside in those jurisdictions.[5]

---

[3] *See* Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34-97142 (March 15, 2023); Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, Release No. 34-94197 (Feb. 9, 2022).

[4] *See* FINRA Rules Related to Cybersecurity, available at https://www.finra.org/rules-guidance/key-topics/cybersecurity#rules.

[5] *See* Article 35, EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679.

- The New York Department of Financial Services ("NYDFS") Cybersecurity Regulation requires a periodic cybersecurity risk assessment. [6]

Similarly, when considering rules governing AI, the CPPA should consider the extensive risk management frameworks that financial institutions already have in place, including frameworks that address oversight and assessment of AI and automated decisionmaking more broadly within financial institutions, of which privacy considerations are one aspect when personal information is involved. In particular, the CPPA should consider whether such requirements would already be addressed or are currently being considered by financial services regulators.

The CPPA should take the following into consideration when proposing additional regulations pertaining to AI:

- California's Department of Insurance released Bulletin 2022-5 which discussed obligations on insurance company obligations to ensure there is not unfair discrimination as a result of the use of artificial intelligence/Big Data analytics.[7]

- NIST AI Risk Management Framework is intended to help build trustworthiness in AI design and development.[8]

- FINRA published a report on AI in the financial services industry finding that firms were taking a cautious but useful approach to using AI in various aspects of the business but did not cite any significant regulatory concerns.[9]

- The Office of the Comptroller of the Currency ("OCC") released supervisory expectations for using AI last year.[10]

---

[6] *See* 23 NYCRR 500.9.

[7] *See* Bulletin 2022-5, California Department of Insurance (June 30, 2022), available at https://www.insurance.ca.gov/0250-insurers/0300-insurers/0200-bulletins/bulletin-notices-commiss-opinion/upload/BULLETIN-2022-5-Allegations-of-Racial-Bias-and-Unfair-Discrimination-in-Marketing-Rating-Underwriting-and-Claims-Practices-by-the-Insurance-Industry.pdf.

[8] *See* NIST AI Risk Management Framework (January 2023), available at https://www.nist.gov/itl/ai-risk-management-framework.

[9] *See* FINRA Report, Use of Artificial Intelligence (AI) in the Securities Industry (June 10, 2020), available at https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry ("FINRA AI Report").

[10] *See* OCC News Release 2022-52, Deputy Comptroller Testifies on Artificial Intelligence (May 13, 2022), available at https://occ.gov/news-issuances/news-releases/2022/nr-occ-2022-52.html.

B. Cybersecurity audits and risk assessments should be risk-based, independent, non-public, and track existing requirements adopted in other jurisdictions.

The California Privacy Rights Act ("CPRA") requires covered entities to conduct both annual cybersecurity audits and "regular" risk assessments. Audits must be performed by the covered entity, but the entity must establish the scope of the audit and also ensure the audit is independent. Risk assessments must be submitted to the CPPA and must disclose whether the covered entity's processing includes sensitive personal information. If the processing does include sensitive personal information, the business must identify any risks and benefits of processing such information with a goal of minimizing such processing if the risks outweigh the benefits to the consumer.

SIFMA appreciates the importance of periodic cybersecurity audits and risk assessments as they are an efficient way for companies to review their policies and find areas of weakness and risk without exposing the firm to additional risk. As demonstrated by the list of existing requirements above, financial institutions already undergo significant risk assessments and audits for various purposes. As such, any implementing regulations should reenforce that both the audit and the risk assessment are risk-based requirements. Further, covered entities should be expressly permitted to use third-party assessments, such as SOC 2 Type 2, to meet the CPRA criteria.

Annual audits should be risk-based to take into account the business activities, size, and other factors that may impact cyber risk. As such, covered entities should not be required to review every aspect of their cybersecurity programs every year if there is not a sufficient risk-based reason to perform such a review. In addition, firms could use resources to take deeper dives on certain issues as necessary without wasting resources on reviewing issues that are low risk. Any cybersecurity audit should be "independent," but such a requirement should also expressly permit internal auditors or an affiliate to perform the audit if they meet the independence standard. Most large companies have robust internal audit capabilities which can achieve the same results as any external auditor.

Further, audits and risk assessments should not be required to be made public. Public disclosure of such audits or risk assessments puts companies and the cyber ecosystem as a whole at significant risk as such documents can provide a roadmap for bad actors.

C. Regulation of automated decisionmaking and artificial intelligence should be principles-based and consider the extensive risk management processes that financial institutions already have in place.

The growing use and capabilities of automated decisionmaking and artificial intelligence (together, "AI") have understandably captured the attention of the public and regulators in a broad range of sectors. It makes sense for financial services regulators to increase their understanding and the public's understanding of how AI is used, evidence

related to perceived risks, and how actual risks are being addressed. Close and ongoing discussions and exchanges of information between regulators and industry are especially important. For all these reasons, the CPPA's request for feedback is an important step in a valuable process.

The financial services sector does, however, have unique and important differences, when compared to other major industries, in its treatment of AI-related risks and capabilities. Established financial institutions already have sophisticated systems in place for overseeing a broad variety of risks, including risks posed by using AI in various contexts. Financial service providers have devised and implemented these risk management frameworks with extensive input from federal financial services regulators, at both the policy and implementation levels.

Senior managers and boards of financial institutions devote considerable resources to ensuring the adequacy, flexibility, and adaptability of those systems and processes to identify, quantify, and mitigate risks of various types. The resulting risk management systems typically involve both focused accountability and cross-function and cross-divisional processes. Firms measure the resulting effectiveness of these processes with a range of established and evolving tools. As different types of asset, personnel, macroeconomic, and process risks emerge and are addressed, institutions test, refine, and expand the capabilities of their risk management processes.

At the same time, financial institutions' uses of AI capabilities are not new, and their consideration and management of risks related to those uses are well developed. Financial institutions have used automated methods of processing customer information, monitoring and protecting against fraud, assessing financial performance and risk, evaluating credit risk, assessing value at risk, and discharging many other functions.[11] In recent years, the "artificial" capabilities associated with these processes have grown more sophisticated. Likewise, financial institutions have undertaken an equally long and continuous process of identifying, monitoring, and mitigating risks associated with using those capabilities.

Further, as we recommended above for cybersecurity audits and risk assessment, the CPPA should consider any assessments of AI used to satisfy other federal or state requirements should also satisfy regulations promulgated under CPRA.

* * *

[11] *See* FINRA AI Report.

SIFMA appreciates the opportunity to provide feedback on the CPPA's proposals and would be pleased to discuss these comments in greater detail. If you have any questions or would like to schedule a meeting, please contact me at [redacted].

Sincerely,

[redacted]

Melissa MacGregor
Managing Director, Deputy General Counsel & Corporate Secretary

From: Zoelle Egner [redacted]
Sent: Monday, March 27, 2023 1:25 PM
To: Regulations
Subject: PR 02-2023
Attachments: CPPA Automated Decision-making Comment.pdf

To whom it may concern:

Please find attached a comment letter addressing automated decision-making, submitted on behalf of Tracy Chou, CEO and founder of Block Party. We appreciate the opportunity to share our perspective on this important issue.

Best regards,
Zoelle

Zoelle Egner
Head of Marketing and Growth
Block Party
Read our latest article: Coming to Terms with the Messy Spectrum of Online Speech

Block Party Studio Company
admin@blockpartyapp.com
www.blockpartyapp.com

March 27, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd
Sacramento, CA 95834
regulations@cppa.ca.gov

RE: PR-02-2023: Preliminary Comments on Proposed Rulemaking – Automated Decision-making

Dear California Privacy Protection Agency Board Members,

Block Party appreciates the opportunity to comment on the proposed rulemaking concerning the regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology." As founder and CEO of Block Party, my experience and expertise is around online safety, social media platforms and building an environment for consumers to have more control over their online experience and data. I write to offer comments and recommendations around § 7063 Authorized Agents and relatedly 7026(j). Block Party supports the Regulation, but recommends that further rulemaking occur to allow the rights clarified in the Regulation to be meaningful.

Regulation 7026(j) Opt-out with Authorized Agents

As an authorized agent to many social media platform users, I can attest to the importance of offering users both the ability to opt-out of automated decision-making technology and to meaningfully access their data so that users can reduce the sometimes corrosive impact of automated decision-making technologies. I believe it is important to enable authorized agents to submit and act on behalf of consumers especially in regards to opt-out preferences as stated in Regulation 7026 (j):

(j) A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.

The regulation recognizes that authorized agents provide a critical service for users. As Board Member Alastair Mactaggart said during a public comment period around the proposed regulations on August 23, 2022 in a letter stating "thus in plain English reading of 1798.135(e) is that a consumer may authorize…another person (person as in a company, corporation, application, nonprofit, etc., including obviously any application or tool provided by such entity) to opt-out for the consumer, i.e. on the consumers behalf."

Meaningful User Rights & Alternatives

In many instances, automated decision-making prevents consumers from meaningfully exercising their rights to opt-out in a fair and equitable manner. However, if consumers are merely granted the right to opt-out of automated decision-making algorithms, many features of a social media platform may no longer work for consumers. For example, a consumer may be interested in opting-out of the utilization of their data by automated decision-making algorithms to determine what content appears in their feed on social media. Currently, there is no option for a consumer to exercise this right; the only option available to consumers is to leave/deactivate the account on the social media platform. And if the only meaningful way to opt-out is not to use the platform at all, the user effectively has no automated decision making rights.

To allow users to meaningfully exercise their rights on the platform, social media platforms must offer consumers a path to an equivalent alternative for their online experience if they opt-out. So, consumers should have an equivalent alternative methodology to select a feed for consumers not interested in allowing their data to be used through automated decision-making algorithms to have access to social media. Platforms have failed to meet this obligation, and they may never choose to do so.

Third Party Tools & User Control/Decision-making

There is another lens to evaluate this problem. Third party developers who serve as authorized agents have the capacity to offer tools that allow users to make the decisions themselves. Through their agents' technology, users have the ability to retain control of both their feeds and their data. If users are unwilling to provide their data to opaque automated decision-making

algorithms, leveraging an authorized agent would offer users the power and control to set their own preferences, parameters and data use. Users should be able to decide for themselves what algorithms and automated decision-making they would like over their own online experience. Either third party-developed tools or alternatives to automated decisioning on social media would offer users a meaningful choice and experience regardless of opting in or out and would not punish users for exercising their rights.

Issues with Automated Decision-making on Social Media

Children

Automated decision-making algorithms have been the cause for many issues on social media platforms. Children are being served inappropriate content that fuels body image, self-harm and other negative perceptions. Currently, users or their guardians are unable to opt-out of the automated decision-making technology and algorithms that automatically show consumers content without their knowledge or input. A simple opt-out of the algorithm is not the answer here. Instead, parents and guardians should have the ability to set guardrails for what content their children see, by selecting the controlling algorithms to monitor that only appropriate content is being shown.

Abuse & Harassment

Additionally, many consumers endure online harassment, abuse, trolling, and unwanted and inappropriate content due to automated decision-making algorithms that currently control the consumer experience. In this circumstance again, users' only choice at the moment is to endure the poor choices of automated decision-making or to leave the platform entirely.

Under CCPA, consumers have the right to understand the manner in which a business uses algorithms to serve a consumer based on data collected from the consumer. These access rights can only be meaningful, however, if platforms allow a way to enable users and their authorized agents to make privacy and safety decisions, **and** provide alternative options to users so that they have meaningful ways to enjoy these platforms even if they elect to opt-out of automated decision-making algorithms. As Alastair Mactaggart pointed out back in 2020, "CCPA has spawned a privacy industry, because the law requires companies to accept an intermediary on your behalf, an authorized agent. That was always my goal, to make sure we would have businesses you could go to and say 'Handle this for me.'"[1]

Equivalent Options for Opting Out

---

[1] https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/new-privacy-laws-generate-business-opportunities-compliance-headaches

While the current rulemaking allows for the use of authorized agents to opt-out of authorized decision-making technology, it does not require that users who opt-out to have a meaningful equivalent option. Such a meaningful equivalent option could be provided by a platform, itself, or an authorized agent could offer equivalent services. For an authorized agent to do so, however, platforms must have clear regulatory guidance to allow third-party agents access to offer users an equivalent experience.

Further Rulemaking Recommendation

I recommend further rulemaking that addresses the consumers' right to enable authorized agents that can act on their behalf for the consumers' overall online experience and data. To do so, social media platforms should be required to offer free access to their public Application Programming Interfaces (APIs) to users and their authorized agents to create and control their own experiences in ways that suit them best. Because the platforms will never be able to create an online experience that works for every consumer, opening up the ecosystem to outside developers who have written authorization to act as authorized agents will create more experiences to cater to specific needs and audiences.

Such a rulemaking is possible without requiring the social media platforms to reveal any of their trade secrets or proprietary technology. I would like to strongly encourage the California Privacy Protection Agency to consider rulemaking on consumer control of the social media experience through the requirement that social media platforms offer open APIs. Open APIs enable new tools to better manage the algorithms and automated decision-making. At Block Party, we believe that consumers deserve a choice and should be able to control their online experience for their own safety and protection.

We appreciate the opportunity to share our comments and we welcome any questions the Board may have.

Sincerely,

Tracy Chou
CEO and Founder
Block Party

From: Reem Suleiman [redacted]
Sent: Monday, March 27, 2023 1:29 PM
To: Regulations
Subject: PR 02-2023: Mozilla's Preliminary Comments to CPPA
Attachments: Mozilla CPPA Preliminary comments_3-27-23_RSJH.pdf

Good afternoon,

Attached is Mozilla's response to the CPPA's request for preliminary comments on cybersecurity, risk assessments, and automated decision making. Please reach out if you have any additional questions.

Thank you for the opportunity,
-Reem

--
Reem Suleiman (she/her)
US Advocacy Lead
Mozilla Foundation

MOZILLA'S RESPONSE TO THE CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA) INVITATION FOR PRELIMINARY COMMENTS ON "CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING"

March 27, 2023

Table of Contents

I. MOZILLA'S VISION FOR A SECURE INTERNET

Mozilla is a global community working together to build a better internet. As a mission-driven organization, we are dedicated to promoting openness, innovation, security, and accessibility online. We are constantly investing in the security of our products, the internet, and its underlying infrastructure. We are also deeply vested in furthering our mission of trustworthy AI, which we lay out in our white paper "Creating Trustworthy AI,"[1] to advance transparency and accountability in the use of automated systems.

Owned by a not-for-profit foundation, a foundational principle of Mozilla's guiding Manifesto[2] demands that individual privacy and security online must not be treated as optional. Mozilla also prioritizes privacy and security in our public interest advocacy, calling for comprehensive privacy legislation, greater transparency, and robust enforcement of data privacy law and regulations around the globe – including

[1] Ricks, B and Surman, M. "Creating Trustworthy AI." Mozilla. December 2020. https://assets.mofoprod.net/network/documents/Mozilla-Trustworthy_AI.pdf
[2] Mozilla Manifesto. https://www.mozilla.org/en-US/about/manifesto/

California's Consumer Privacy Rights Act (CPRA).[3] Mozilla is the creator of Firefox, an open-source browser that millions of people use as their window to the web, as well as a suite of privacy and security-enhancing products and features such as our VPN[4] (Virtual Private Network), which helps people create a secure, private connection to the internet; DNS over HTTPs - or DoH[5] - the protocol that encrypts domain name look-ups and closes one of the last great security vulnerabilities in the internet; and the end-to-end encrypted Firefox Sync[6] service, which protects all your synced data so Mozilla can't read it.

In addition, Mozilla developed a set of minimum security standards we think all connected products should meet – at the very least. Think of it as a "you must be this tall to ride" set of standards. These include five basic things: the product must use encryption; the company must provide automatic security updates; if a product uses a password, it must require a strong password; the company must have a way to manage security vulnerabilities found in their products; and the company must have an accessible privacy policy. Our minimum security standards are used in our *Privacy Not Included*[7] consumer guide, which comes with **Privacy Not Included* warning labels on products we think consumers should think twice about before buying. If we can't confirm a product meets our Minimum Security Standards, it automatically earned the **Privacy Not Included* label, which we feel should be the minimum threshold for products entering the market.

Mozilla welcomes the CPPA's efforts to examine cybersecurity audits, risk assessments, and automated decisionmaking as they develop and propose regulations that implement amendments to the California Consumer Privacy Act (CCPA). While cybersecurity

---

[3] Mozilla. "Four key takeaways to CPRA, California's latest privacy law." Mozilla Open Policy & Advocacy Blog.
November 20, 2020.
https://blog.mozilla.org/netpolicy/2020/11/20/here-are-four-key-takeaways-to-cpra-californias-latest-privacy-law/
[4] Mozilla VPN, at https://www.mozilla.org/en-US/products/vpn/more/what-is-a-vpn/
[5] Patrick McManus, "Improving DNS Privacy in Firefox," Firefox Nightly News (June 1, 2018), at https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/
[6] Firefox Sync, at https://www.mozilla.org/en-US/firefox/sync/
[7] https://foundation.mozilla.org/en/privacynotincluded/about/

audits and risk assessments pose timely and important questions, today we will focus on the questions related to automated decisionmaking systems (ADMS). We are happy to have follow up conversations on all topics addressed in the agency's invitation for preliminary comments or topics found within the CCPA, such as data protection, consumer privacy, and curbing dark patterns (or deceptive design practices).

II. MOZILLA'S THINKING ON AUTOMATED DECISIONMAKING

Enabling more access to information regarding ADMS and providing people with more control over when they are affected by automated decision-making is critical. It is a necessary precondition for allowing people to contest automated decisions that cause harm. Our 'Trustworthy AI' strategy highlights the underlying importance of balancing 'agency' and 'accountability' with automated systems. While 'accountability' relates to the responsibilities and remedies that are necessary when AI systems fail (e.g. in making discriminatory decisions or abusing peoples' data), ensuring 'agency' means that people using or impacted by these systems have the ability to understand and control consequential functions. Therefore, from our vantage point, it is important that the CPPA provides for robust mechanisms that give consumers transparency and control. In response to question 9, disclosure and access to this data should provide consumers the answers to questions like: Are ADMS used for certain decisions? How do they make such decisions? What information do these systems rely on? And how exactly are they deployed? For access to be meaningful, consumers need easy-to-understand descriptions. However (in response to question 7), more detailed and technical information must be available for experts, researchers, and others looking to understand these systems and their potential or existing harms, such as discrimination or profiling.

Inspiration for what access may look like can be found (in response to question 1), for example, in EU law as well as in several proposals currently moving through the EU's legislative process. For instance, Article 22 of the General Data Protection Regulation

(GDPR) provides data subjects, with some exceptions, with the right “not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” However, this still leaves significant ambiguity when it comes to the question of what constitutes a decision solely based on automated processing or what qualifies as affecting a person to a similar degree as a decision producing legal effects. This has also led to Article 22 being of limited utility for data subjects. The CPPA can learn from this experience and tackle some of these ambiguities. Similarly, Recital 71 of the GDPR — which is not legally binding but meant to aid interpretation of the regulation — purports that data subjects should be able to obtain an explanation and contest automated decisions.

The EU’s recently enacted Digital Services Act (DSA), on the other hand, stipulates in Article 37 that users of very large online platforms and search engines (including major social media and content sharing platforms) should be able to opt out of receiving algorithmic recommendations based on profiling within the sense of the GDPR. It also prescribes, in Article 28, that online platforms need to provide information about their recommender systems, especially about the main parameters used in these systems, in their terms and conditions. With regard to online platforms, this is distinct from the GDPR’s intent to provide explanations to users on a case-by-case basis in that it provides general information to all users ex ante.

The most comprehensive proposal in the EU in this regard comes in the draft Platform Work Directive, which is currently being negotiated. Article 6 of the initial proposal platform worker directive would prescribe that detailed information needs to be provided about ADMS used for algorithmic management of workers. At the same time, Article 8 would give platform workers a right to human review of significant automated decisions, like termination decisions. This is an important concept that should be applied to any high stakes decisions in which an ADMS is deployed.

Finally, the EU’s proposed AI Act would include an additional transparency mandate toward affected people. In Article 52, amongst other things, it would prescribe that “AI systems intended to interact with natural persons“ would need to be designed in such a

way that people interacting with these systems are informed that this is, in fact, the case.

Such approaches to providing access to information as well as choice for individuals can prove helpful in that they both create awareness of the fact that people are subjected to automated decisions as well as how, and provide them with more agency over their experiences. However, it is also important to highlight that in many cases this will not be enough to effectively prevent or mitigate harm. In fact, rarely will it address the underlying causes of harms like discrimination through ADMS.

Moreover, there are limitations to approaches that provide transparency only in individual cases and not by default. For example, it puts the onus on individuals to protect themselves instead of incentivizing companies to proactively prevent and mitigate harms. Further, transparency and opt-out mechanisms are likely to benefit those the most who have the necessary digital literacy to critically assess the information provided by companies as well as the choices available to them. To truly address the root causes of algorithmic harms, further action is needed — for example through documentation requirements, audits of ADMS, human oversight, and robust complaint and redress mechanisms.

III. CONCLUSION

We are grateful for the opportunity to engage again[8] with the California Privacy Protection Agency, and we are happy to be a resource on this important topic as well as other areas of mutual interest. If we can provide any additional information that would be helpful, please do not hesitate to contact us. We look forward to continued engagement with the Agency.

[8] Mozilla Comments to CCPA Consultation https://blog.mozilla.org/netpolicy/files/2021/11/Mozillas-Comments-to-CCPA-Consultation-November-2021-6.pdf

Contact for Additional Information

Jenn Taylor Hodges, Director of US Public Policy and Government Relations, Mozilla Corporation - [redacted]

Reem Suleiman, US Advocacy Lead, Mozilla Foundation - [redacted]

From: Traci Lee [redacted]
Sent: Monday, March 27, 2023 2:27 PM
To: Regulations
Cc: Jeff Reed; Stephen Williams
Subject: PR 02-2023 - Proofpoint, Zscaler, and Okta Comments on Proposed Rulemaking
Attachments: CCPA_Comments_(cybersecurity_audits, _risk_assessments_and_automatic_decision-making)_-_3.27.23_-_FIN.pdf

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [redacted]

Dear Mr. Sabo,

On behalf of cybersecurity companies Proofpoint, Zscaler, and Okta, I have attached our joint submission relating to the Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decision-making. We thank the California Privacy Protection Agency for your consideration and for the opportunity to respond.

Please reach out with any questions.

Regards,
Traci Lee
--
Traci Lee
Director, US State and Local Government Affairs
[redacted]

[redacted]

March 27, 2023

California Privacy Protection Agency
ATTN: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

Re: PR 02-2023
INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING
CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISION-MAKING

Dear Mr. Sabo,

As global leaders in combating cybersecurity threats, safeguarding data, and enhancing public and private organizations' privacy and security postures, we – Proofpoint, Zscaler, and Okta – an informal coalition of cybersecurity companies, appreciate the opportunity to respond to the California Privacy Protection Agency (the "Agency") Invitation for Preliminary Comments on Proposed Rulemaking for the California Consumer Privacy Act of 2018 , as amended by the California Privacy Rights Act of 2020 (the "CCPA").

Proofpoint

Proofpoint is a cybersecurity company specializing in helping organizations protect against advanced cybersecurity threats and compliance risks such as identity theft, phishing, ransomware and business email compromise. As part of its cybersecurity and compliance services, Proofpoint provides and uses a global intelligence platform that gives businesses the critical visibility they need to maintain the security of their email, Cloud applications, and other IT systems, and to respond to threats against the business and its employees.

For example, with respect to email borne cybersecurity threats, the Proofpoint service detects and filters harmful content included in email messages from reaching our customers' employees (including California consumers) by helping to detect fraudulent activity and potential threats to the business systems used by those employees. Another example of Proofpoint's services are the Proofpoint security training programs that empower our customers with highly effective cybersecurity training tools in order to train their employees (including California consumers) so they know how to protect themselves (and their systems) from malicious attacks such as identity theft and impersonation. As a leading enterprise security service provider of anti-fraud and threat detection products and services, we are on the cutting edge of helping organizations protect against advanced cybersecurity threats and compliance risks, and thereby protecting the privacy of California residents and the security of their personal information.

Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange is the company's cloud-native platform that protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location.

Headquartered in San Jose, California, Zscaler was founded in 2007 with a mission to make the cloud a safe place to do business and a more enjoyable experience for enterprise users. Zscaler's purpose-built security platform puts a company's defenses and controls where the connections occur—the internet—so that every connection is fast and secure, no matter how or where users connect or where their applications and workloads reside.

Distributed across more than 150 data centers globally, Zscaler's SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. It powers all four categories of Zscaler services, including Zscaler Internet Access, which secures connections to the internet and SaaS applications and protects against cyberthreats; Zscaler Private Access, which provides zero trust access to internal

applications in the cloud and data center without a VPN; Zscaler Cloud Protection, which secures workloads using microsegmentation and by identifying cloud misconfigurations; and Zscaler Digital Experience, which provides visibility into the complete path between user and app to pinpoint performance issues.

Okta

Okta is a publicly-traded (NASDAQ: OKTA), identity and access management company offering software-as-a-service to businesses, governments, non-profit entities, and other organizations across the United States and around the world. Founded in 2009 and headquartered in San Francisco, California, Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables the company's customers to securely connect people to technology, anywhere, anytime and from any device.

Okta's customers use our services to work with some of their mission-critical, sensitive data, including the names, email addresses, and mobile phone numbers of their users. Accordingly, acting with integrity and transparency, so that we earn and maintain our customers' trust, is critically important to all of us at Okta. To that end, Okta maintains privacy protections across its suite of services, as detailed in our third-party audit reports and standards certifications.

Our collective companies Proofpoint, Zscaler, and Okta provide tools and solutions to customers in both the private and public sectors to help ensure that their systems are kept safe and secure, so that critical data can remain private and protected. Strong cybersecurity is essential for consumer privacy protection, and it is critical to ensure cybersecurity activities are permitted to make proportionate use of personal information to manage security risks and incidents. To that end, Proofpoint, Zscaler, and Okta support the Agency's efforts to protect Californians' consumer privacy and offer comments on the proposed rulemaking regarding cyber security audits, risk assessments, and automated decision-making.

Proofpoint, Zscaler, and Okta are herein collectively referred to as "the Companies."

I. Cybersecurity Audits

The CCPA directs the Agency to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security to perform annual cybersecurity audits, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent."

A. The cybersecurity audit requirement should be interoperable with the existing robust ecosystem of evolving cybersecurity standards and audit practices.

Various state and federal laws and regulations require businesses to conduct cybersecurity audits, assessments, and similar reviews. These include sectoral laws such as the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act, as well as obligations in more than half the states for certain businesses to maintain a comprehensive written information security plan, one component of which is to conduct risk assessments.[1] Against this backdrop, customers of cloud services expect vendors to meet and demonstrate compliance with increasingly elevated standards for cybersecurity by providing independent, third party audit or assessment reports, separate and apart from any legal requirements. This constellation of existing requirements and enterprise customer expectations provides an important and flexible foundation for cybersecurity audit and assessment practices in the cybersecurity industry.

Particularly in view of industry's ability to innovate and evolve rapidly to meet the increasingly complex and ever-changing cybersecurity landscape, the Companies urge that any new audit requirements align

[1] *See, e.g.*, 201 Mass. Code Regs. § 17.03(2), N.Y. Gen. Bus. Law § 899-BB, and Or. Rev. Stat § 646A.622

with established standards and practices.[2] To the fullest extent possible, therefore, the Companies recommend that any audit be conducted and measured against existing generally accepted standards, such as NIST, SOC 2, or ISO. Both the NIST Framework for Improving Critical Infrastructure Cybersecurity and ISO 27001 certifications, for example, are highly recognized standards for communicating desired cybersecurity objectives to internal and external business stakeholders, and supporting the integration of security controls from a multitude of frameworks to achieve those objectives. Such frameworks include the Zero Trust security model, and various well-established security controls (e.g., identity and access management and multi-factor authentication).

Establishing new and separate standards that do not align with the widely accepted standards already in place will yield inconsistent cybersecurity practices and outcomes. Among other things, unharmonized standards will, (1) complicate security training, (2) negatively impact the use of shared resources and services, (3) hinder collaboration between organizations and agencies, and (4) lead to confusion with respect to emerging security controls and updates to best practices. In addition, any overly prescriptive standards or requirements would quickly become outdated and lead to box-checking instead of thoughtful initiatives that actually reduce cybersecurity risk. Given the especially lucrative nature of stolen enterprise and government information and the heavily resourced and nimble ecosystem of bad actors who are constantly evolving their attack vectors, such an approach would also inadvertently hamstring an organization's ability to protect itself.

B. Invasive audits pose risks to businesses in the security space.

The Companies applaud the Agency's commitment to developing regulations that account for the needs of businesses to help prevent and detect security incidents and protect against malicious, deceptive, fraudulent or illegal activity. To that end, the Companies encourage the Agency to consider appropriate boundaries regarding the information that businesses in the security space must provide in any new audit.

Overly invasive audits would undermine and damage the very measures that security companies and their customers implement to provide effective cybersecurity. They would compel the disclosure of information concerning their threat protection and identification practices, including the intricacies of a security vendor's backend systems, sources of personal information, and technology used for processing, which could be detrimental to the security of the services such security vendors provide and consumers rely upon. Moreover, the compelled disclosure of how a security company's internal systems connect and operate would require the Companies to make known their intellectual property and confidential cybersecurity practices, thereby affording threat actors (including criminal organizations and nation state intelligence agencies) powerful new resources for bypassing security measures and evading detection. Such information is critical to both the value and success of the security services that the Companies and other security vendors provide to customers, as well as the maintenance of overall consumer security standards across the broader Internet.

In accordance with the CCPA's stated intention that new regulations should not require businesses to disclose trade secrets in response to consumer requests,[3] the Agency should confirm that any new cybersecurity audit requirements would similarly not oblige businesses to disclose trade secrets and security controls in place (especially, when such disclosures could diminish a company's security posture). In addition, in line with the CCPA's carve-out for trade secret information in a business's submission of a risk assessment,[4] the Companies urge the Agency to include a similar carve-out under 1798.185(a)(15)(A) with respect to audits, or to clarify that such carve out applies to both subsections (A) and (B) of 1798.185(a)(15). While it seems clear that the Agency's intent matches the above, clarifying language would remove any sense of ambiguity.

Importantly, the regulations should go one step further to clarify that a cybersecurity business is not required to make disclosures that are reasonably likely to compromise its security posture and fraud detection and prevention efforts, or otherwise compromise the privacy or security of its consumers, regardless of whether such information constitutes a trade secret of the business. Providing businesses

[2] Indeed, the Agency has long acknowledged the need for ensuring that new regulatory requirements are compatible with requirements in other jurisdictions. See, e.g., California Civil Code § 1798.185(d); California Civil Code § 1798.199.40(i), California Civil Code § 30.

[3] Cal. Civ. Code § 1798.185(a)(3).

[4] Cal. Civ. Code § 1798.185(a)(15)(B).

[redacted]

with the flexibility to refrain from disclosing information that could impair the protection of California consumers from malicious cyber threats would be entirely consistent with the CCPA.

II. Risk Assessments

Pursuant to the CCPA, businesses that process personal information that presents a significant risk to consumers' privacy or security must submit risk assessments to the Agency on a regular basis.

A. To determine when a risk assessment is required, the Agency's regulations should implement a balancing test that considers the consumer benefits and the risks given the nature of the processing activities.

Various comprehensive privacy laws and regulations around the world, including the United States (U.S.), require risk assessments for certain processing activities, most notably the European Union's General Data Protection Regulation (GDPR) and other U.S. state privacy laws (*e.g.*, the Colorado Privacy Act). While these requirements vary in scope and detail, they generally resemble CCPA's requirement by establishing an assessment obligation for processing activities that are deemed high-risk, and in some cases requiring the submission of such assessment to a regulatory authority. Within this context, the key question is what types of processing activities trigger the assessment requirement in the first place by qualifying as high-risk.

While the Companies recognize the importance of privacy risk assessments for protecting consumers and understand the intent behind the CCPA's risk assessment requirements, we also regard strong cybersecurity as essential to protecting consumers and deem various tools that analyze personal information as vital to that aim. The Companies therefore recommend that any regulations regarding risk assessment should take these benefits into account by focusing not only on the nature of the underlying processing activities but also their aim of protecting consumers and any relevant business purposes, such as improving overall security across a website and the Internet. Consideration of such factors would be altogether consistent with the CCPA's requirement for risk assessments (which implies that consumer benefit is a valid consideration in assessing processing activities), as well as its list of business purposes (which includes "[h]elping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes").[5]

B. The CCPA's risk assessment requirements should remain flexible.

The fundamental question of a risk assessment is how effectively a compliance program addresses the privacy and security risks associated with processing personal information. Flexible frameworks are ideal for this type of evaluation. Businesses should have the flexibility to assess their relative risk and best determine how to protect consumer data, as such protection may include limiting the information disclosed to third parties or made public. The Agency should avoid overly broad rules that fail to take into consideration the different risks particular industries face and the active intelligence gathering conducted by threat actors to further their abilities to counteract or evade security measures that are made readily known to them.

C. Requiring the submission of risk assessments on a "regular basis" will be costly, burdensome, and ultimately ineffective.

While the Companies understand the Agency's intent behind requiring submissions of risk assessments, the Agency should reconsider the effectiveness of requiring businesses to submit routinely recurring risk assessments to the Agency absent a compelling reason. Risk assessments conducted and filed "on a regular basis" may become resource-intensive and burdensome for both the Agency and businesses. Internally, a business should conduct periodic assessments, but such assessments should not be required to be submitted to the Agency unless (1) the Agency has a specific need to investigate a particular business's measures in place, or (2) the residual risks of processing remain high after the business has conducted an assessment.

[5] Cal. Civ. Code § 1798.140(e).

Under the Colorado Privacy Act ("CPA"), the Virginia Consumer Data Protection Act ("VCDPA"), and the Connecticut Data Privacy Act ("CTDPA"), for example, the Attorney General may request the disclosure of a data protection assessment; however, there is no requirement that such assessments be provided to the Attorney General on a regular basis.[6] Preparing and submitting such assessments on a regular basis can take resources away from valuable compliance efforts and yield little benefit to consumers when the Agency does not have concrete indications of wrongdoing by a business. Further, the CPA makes clear that data protection impact assessments submitted by businesses under the law are confidential and exempt from public inspection and copying under the Colorado Open Records Act.[7] The law also emphasizes that "disclosure of a data protection assessment under the law does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment."[8] Accordingly, the Companies urge the Agency to include similar language to ensure the protection of the contents of risk assessments where such risk assessments have been prepared by businesses that provide security services.

Similarly, the GDPR requires controllers to conduct data protection impact assessments ("DPIA") for high-risk processing activities,[9] but only a subset of those assessments must be submitted to a regulatory authority. The underlying intent of the DPIA is not to mandate administrative tracking, but rather a tool to ensure that businesses consider the risks associated with their processing activities to adequately protect personal data and meet compliance requirements.

To maintain consistency with other established regulatory requirements, the Agency could require businesses to conduct a risk assessment, such as a DPIA, for those high-risk processing activities. The Agency could then require a business to document and maintain the assessment on file, which may be provided by the business to the Agency upon request in connection with an investigation or consumer inquiry. This methodology is consistent with the spirit and intent of the CCPA.

III. Automated Decision-making

Pursuant to the CCPA, the Agency is directed to "issue regulations governing access and opt-out rights with respect to businesses' use of automated decision making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."[10]

A. Carve outs must be provided where automatic decision-making technology is used for security purposes, such as fraud prevention and threat intelligence.

The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to defend against adversaries. With the advancement of artificial intelligence models, it would be a mistake to assume that threat actors are not using this technology to harm consumers. Restricting the ability of cybersecurity companies to use such technologies would prevent cybersecurity companies from protecting California consumers. The Companies urge the Agency to avoid expanding CCPA's existing access and opt-out rights in a way that would create an express right to opt-out of automated decision-making technology, particularly where such use of the technology is only for purposes of preventing and detecting security incidents and/or protecting against malicious, deceptive, fraudulent or illegal activity. The Companies further encourage the Agency to exclude these technologies from any requirements to divulge information about the logic of their underlying decision-making,[11] which could reveal sensitive security-related details and trade secrets.

A rule that permits consumers to opt out of the use of such technology with respect to their personal information— when such technology is used for the purposes of maintaining the security of such information— is at odds with the goals of the CCPA, which requires businesses to implement reasonable

[6] See Colo. Rev. Stat. § 6-1-1309(4); VA. Code § 59.1-580(C); Public Act 22-15 § 8(c).
[7] Colo. Rev. Stat. § 6-1-1309(4).
[8] Colo. Rev. Stat. § 6-1-1309(4).
[9] See Article 35, General Data Protection Regulation
[10] Cal. Civ. Code § 1798.185(a)(16).
[11] See Cal. Civ. Code § 1798.180(16).

[redacted]

security procedures and practices to protect personal information.[12] Such opt-out permission would limit a cybersecurity provider's ability to utilize the threats identified through the processing of consumer data on behalf of their customers to evolve security systems and controls necessary to detect and prevent against security incidents that compromise the availability, authenticity, integrity, and confidentiality of such information. This scenario increases the risks of unauthorized access, acquisition, or exfiltration—ultimately limiting consumers' ability to achieve control over their data in the manner intended by the rulemaking.

More to the point, consumers benefit both directly and indirectly from measures aimed at detecting security incidents and protecting against unauthorized activity; their own personal information is subject to improved security, and the enterprises with which they interact are themselves better able to protect personal information that consumers disclose as part of everyday business. These security risks are multiplicative, in the sense that fraudsters use compromised consumer accounts and information to escalate unauthorized activity more broadly. If consumers are permitted to opt out of such processing, a security service provider's ability to provide its services in a meaningful way will be dramatically limited to the detriment of this entire ecosystem and may force cybersecurity companies to stop providing its services to those who do opt out.

Further, requiring security vendors to disclose details of their use of automatic decision-making tools in connection with a consumer's access request would be devastating to the effectiveness of the services they provide. A security vendor's disclosure of detailed information regarding how its technologies make decisions (i.e., their internal logic, and the likely outcome of the process with respect to a consumer) would result in the exposure of trade secrets, proprietary information, or violations of intellectual property rights that are essential to the business and the protection of California consumers. Disclosing such information also presents a cybersecurity risk, as threat actors can identify vulnerabilities and exploit them, thus putting companies and their users at significant risk.

Allowing service providers to reasonably use consumer data for security and anti-fraud purposes subject to existing CCPA requirements would not only help to enhance consumer privacy, but also permit business' cybersecurity programs to stay ahead of cyber criminals who are constantly evolving and finding new vulnerabilities to exploit. Furthermore, as service providers, the Companies process consumer personal information on behalf of businesses for the purpose of helping to ensure the security and integrity of their systems. Like other security service providers, we continuously strive to build upon and improve our services to better protect customers and consumers alike, and the use of automated decision-making technology is key to our success.

B. Artificial intelligence drives innovation and is key to supporting the spirit of the CCPA.

For businesses to be able to help support the Agency's goal of increasing consumer data protections, they must be able to utilize security service providers that can develop and improve their services in a meaningful and effective way— particularly in response to accelerating technological advances and ever-evolving cyber threats. Many businesses outsource some degree of their security operations to service providers who specialize in detecting and preventing cyber-attacks. Allowing security service providers to fully utilize automatic decision-making technology to strengthen their services is critical to advancing the Agency's objective.

Patterns and models generated through such automated decision-making technology are used to improve the detection and prevention of fraudulent activity. Without such technology, service providers in the security space would not be able to keep pace with modern, rapidly evolving cybersecurity risks posed by cybersecurity threat actors.

While the Companies understand the risks inherent to automatic decision-making technology, the Companies strongly encourage the Agency to consider the significant benefits that such technology provides when security service providers can leverage the technology to prevent and detect fraudulent activity. The Agency should weigh such benefits against the risks of limiting business uses of the technology.

[12] Cal. Civ. Code § 1798.100(e).

[redacted]

IV. Conclusion

Securing the privacy of individuals' data and making our technology and innovations available to our customers to enable them to improve their business are core drivers for each of our companies. The Companies believe that by incorporating into the draft regulations tailored limitations that contemplate how different industries are, the Agency has an opportunity to ensure that businesses can continue to adequately protect themselves, their customers, and consumers from cyber threats.

Proofpoint, Zscaler, and Okta thank you for your time and consideration. We welcome further discussion regarding the issues raised above.

[redacted]

Jeff Reed

VP & AGC

Proofpoint, Inc.

[redacted]

Torrie Nute

VP, AGC

Zscaler

[redacted]

Tim McIntyre

VP & AGC, Privacy & Product

Okta