epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER,
CENTER FOR DIGITAL DEMOCRACY, AND CONSUMER FEDERATION OF AMERICA

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

On Proposed Rulemaking re Cybersecurity Audits, Risk Assessments,
and Automated Decisionmaking

PR 02-2023

March 27, 2023

The Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America submit these comments in response to the California Privacy Protection Agency (CPPA)'s February 2023 invitation for public input concerning the agency's development of further regulations under the California Consumer Privacy Act of 2018 (CCPA) as amended by the California Privacy Rights Act of 2020 (CPRA).

As we have conveyed in previous comments, we firmly support the CPPA's efforts to establish robust protections for Californians against harmful commercial data practices. As the agency formulates regulations concerning cybersecurity audits, risk assessments, and automated decisionmaking, we renew our call to "protect consumers' rights" and "strengthen[] consumer privacy" at every opportunity, consistent with the expressed will of California voters.[1] In particular, we urge the Agency to take account of the full spectrum of harms that can result from personal data processing and the use of automated decisionmaking systems (ADS); establish strong cybersecurity

[1] California Privacy Rights Act of 2020 §§ 3, 3(C)(1).

audit standards that draw on the strongest commonalities between existing frameworks; require businesses to routinely conduct robust risk assessments and to submit both unredacted and summarized versions to the CPPA; and ensure that consumers enjoy robust and effective ADS disclosures and opt-out rights.

I. Our organizations

The Electronic Privacy Information Center[2] is a public interest research center established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has previously provided comments on the CCPA[3] and published a detailed analysis of the CPRA before its approval by California voters.[4]

The Center for Digital Democracy[5] is a public interest advocacy, research, and education organization with a mission to ensure that digital technologies serve and strengthen democratic values, and safeguard privacy, civil, and human rights.

The Consumer Federation of America,[6] an association of nonprofit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education, promotes policies that protect consumers from unwanted and inappropriate use of their personal information.

---

[2] https://epic.org/.
[3] Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Nov. 8, 2021), https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf [hereinafter EPIC et al. 2021 CCPA Comments]; Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf.
[4] EPIC, *California's Proposition 24* (2020), https://epic.org/californias-proposition-24/.
[5] https://www.democraticmedia.org.
[6] https://consumerfed.org/.

II. Harms and use cases

The Agency asks several questions about the application and harms of personal data processing and automated decisionmaking technology. Before turning to our discussion of how the Agency should regulate harmful data practices, we address those questions here. In particular, we set out (a) the privacy, autonomy, physical, discrimination, data security, and other harms caused by the processing of personal information; (b) examples of how automated decisionmaking technology is already used in commercial settings; and (c) examples of consumer experiences with automated decisionmaking technology.

a. Harms from the processing of personal information

Responsive to question II.2

Consumers are persistently tracked online through the sweeping collection, processing, and use of their personal information.[7] This personal data fuels online commerce and can be used in ways that consumers expect and welcome. But when these commercial surveillance systems enable online firms to build detailed profiles of consumers, often including sensitive personal characteristics, consumers are exposed to "ever-increasing risks of data breaches, data misuse, manipulation, and discrimination."[8] Even with the most effective notice and transparency

[7] Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 7 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM- comments-Nov2022.pdf [hereinafter EPIC FTC Comments on Commercial Surveillance]; *see also* FTC Office of Tech., *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, Fed. Trade Comm'n (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking; *Factsheet: Surveillance Advertising: How Does the Tracking Work?*, Consumer Fed. of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how- tracking-works/.

[8] *Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of Caitriona Fitzgerald), https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security/; *see also* Consumer Fin. Prot. Bureau, *CFPB Issues Advisory to Protect Privacy When Companies Compile Personal Data* (Jul. 7, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-advisory-to-protect-privacy-when-companies-compile-personal-data/ ("Americans are now subject to round-the-clock surveillance by large commercial firms seeking to monetize their personal data.").

requirements, consumers cannot meaningfully consent or protect themselves from complex commercial surveillance practices.[9]

Commercial systems that track individuals and process personal information can inflict a wide range of harms. Privacy scholars Danielle Citron and Daniel Solove have cataloged numerous harms resulting from the large-scale processing of personal information, including autonomy, physical, discrimination, and data security harms.[10] The scale and scope of these harms is "especially acute for marginalized communities, where they foster discrimination and inequities in employment, government services, healthcare, education, and other life necessities."[11] For example, physical harms facilitated by privacy violations—like stalking and assault—can pose a disproportionate risk to victims of domestic violence.

Other privacy harms include economic harms (e.g., a heightened risk of identity theft that would result in financial loss), reputational harms, relationship harms, and psychological harms (e.g., emotional distress from threats or harassment online). Psychological harm can result from a fear of exposure or misuse of sensitive data including medical records or intimate images.[12]

The violation of autonomy is another type of privacy harm. While autonomy harms can flow from the overcollection personal data processing itself, other mechanisms like manipulation, dark

[9] EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 153 ("We have moved beyond the notion that notice and consent alone can legitimize commercial surveillance practices when those practices are too complex and numerous for even the most sophisticated consumer to understand."); Mary Madden, Data & Society, *Privacy, Security, and Digital Inequality* (Sept. 27, 2017), https://datasociety.net/wp-content/uploads/2017/09/DataAndSociety_PrivacySecurityandDigitalInequality.pdf ("52% of those in the lowest-earning households say that not knowing what personal information is being collected about them or how it is being used makes them "very concerned," compared with 37% of those in the highest-income households.").
[10] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 830–59 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[11] *Id*. at 7.
[12] Danielle K. Citron, *Sexual Privacy*, 128 Yale L. J. 1870, 1874–81 (2019), https://www.yalelawjournal.org/pdf/Citron_q8ew5jjf.pdf.

patterns, or violations of contextual integrity can result a loss of autonomy online.[13] For example, platform design can result in thwarted expectations when consumers are nudged to purchase certain items, divulge information, or exposed to profiling and targeted advertising from an unexpected secondary use of their data.[14] Consumers do not have control over data collected without their knowledge or downstream uses of the data they knowingly provided to online companies. "The loss of control poses special concerns for sensitive data about individual consumers' finances, health, intimate relationships, and precise location."[15]

Commercial surveillance can also lead to discrimination harms.[16] Troves of personal data fuel systems that target and profile consumers by dividing and scoring consumers based on their characteristics, demographics, and behaviors.[17] Through mechanisms like targeted advertising, consumers are sorted in ways that "reflect and entrench systemic biases."[18] Targeted advertising can reinforce discrimination against marginalized groups and deprive those individuals of equal access to information about various economic opportunities including housing, employment, and education.[19] For example, before changing their ad targeting system after a settlement with the Department of Justice, Meta "allowed discrimination in the targeting and delivery of ads for housing, credit service, and job openings based on sex, race, and age."[20] Other examples include retail websites charging

[13] EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 33.
[14] *Id*. at 44–45.
[15] EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 46.
[16] *Id*. at 112–13.
[17] *Id*. at 48.
[18] *Id*.
[19] Aaron Rieke and Corrine Yu, *Discrimination's Digital Frontier*, The Atlantic (Apr. 15, 2019), https://www.theatlantic.com/ideas/archive/2019/04/facebook-targeted-marketing-perpetuates-discrimination/587059/.
[20] *Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of David Brody), https://docs.house.gov/meetings/IF/IF17/20220614/114880/HHRG-117-IF17-Wstate-BrodyD-20220614.pdf.

different prices based on user demographics[21] and consumer financial discrimination through payday loan ad targeting.[22]

The collection and processing of personal information can also result in harmful data security violations.[23] The accumulation of data, whether "from the consumer directly, scraped from public sources, and purchased from data brokers, creates serious security risks."[24] Specific categories of data collection and processing can heighten the security risks associated with an eventual breach, sale, or downstream use. A data breach or incident revealing sensitive information like health data, data collected from children or teenagers, or financial information can exacerbate the harm from exposure. For example, unauthorized secondary use of location data can reveal historical or real-time location, "exposing an individual to stalking and other physical threats, as well as doxing."[25] Location data can illustrate sensitive information like visiting an abortion clinic, substance abuse support meeting, or place of worship.[26] Additionally, because location data is "available for purchase for a nominal fee,"[27] or accessible through hacking and security breaches, bad actors can purchase data to stalk, harass, or pose other threats to the wellbeing of individuals.

---

[21] Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, Wall St. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
[22] Aaron Rieke and Logan Koepke, *Led Astray: Online Lead Generation and Payday Loans*, Upturn (2015), https://www.upturn.org/reports/2015/led-astray/.
[23] EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through A Section 5 Unfairness Rulemaking* 7 (Jan. 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf [hereinafter *Data Minimization White Paper*].
[24] *Id*. at 29.
[25] EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 50.
[26] *See* Assoc. Press, *Priest Outed via Grindr App Highlights Rampant Data Tracking*, NBC News (July 22, 2021), https://www.nbcnews.com/tech/security/priest-outed-grindr-app-highlights-rampant- data-tracking-rcna1493; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Corin Faife, *ICE Uses Data Brokers to Bypass Surveillance Restrictions, Report Finds*, The Verge (May 10, 2022), https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers- georgetown-law;
[27] EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 50.

b. Uses of automated decisionmaking technologies

Responsive to question III.4

The commercial use of automated decisionmaking systems (ADS) is rapidly growing.[28] From computer vision to recommendation systems, generative AI, and facial recognition, a vast array of ADS has been developed and deployed by companies just in the last several years.[29] Many of these systems are used in operations, supply chain management, risk assessment, marketing, and strategy.[30] This includes systems for automating product feature optimization, risk modeling, and customer service analytics.[31] But companies also use automated systems to screen and score individuals and to make significant decisions that impact their health, welfare, and access to housing, employment, education, public benefits, and credit.

Despite the well-documented inaccuracy, discrimination, and opacity problems that characterize these systems (see below), automated decisionmaking technology has spread to a wide range of industries and applications, including:

- *Employment screening.* ADS has been used in all aspects of the job application process, including resume screening, interviews, and hiring determinations.[32] For example, HireVue uses ADS to evaluate job applicants based on biometric data collected in automated interviews.[33]

[28] McKinsey & Co., *The State of AI in 2022* (Dec. 6, 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review (Annual State of AI survey of 1,500 companies, adoption of AI has doubled since 2017).
[29] *Id*.
[30] *Id*.
[31] *Id*.
[32] *See, e.g.*, Sheridan Wall & Hilke Schellmann, *LinkedIn's job-matching AI was biased. The company's solution? More AI*, MIT Tech. Rev. (June 23, 2021), https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias- ziprecruiter-monster-artificial-intelligence/.
[33] *See* EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 76 ("HireVue—just one competitor in the employment screening field—has over 700 corporate customers[.]"); Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/documents/in-re-hirevue/.

- *Facial recognition.* The commercial use of facial recognition technology has proliferated in stores, stadiums, arenas, and other public accommodations across the country.[34]
- *Health screening.* ADS has been used to make predictive determinations about patient outcomes and direct courses of treatment.[35]
- *Education.* PowerSchool claims to hold data on over 75% of K-12 students in North America and provides schools with tools to generate predictions about graduation rates, SAT scores, and other outcomes.[36]
- *Targeted advertising.* "[A]s AI-powered advertising grows more pervasive and sophisticated, it is doing so without guardrails."[37]
- *Housing.* Landlords and property management groups use tenant screening algorithms,[38] and Airbnb has used automated risk assessment tools to rate potential guests.[39]

---

[34] *See, e.g.*, Georgia Gee, *Here Are the Stadiums That Are Keeping Track of Your Face*, Slate (Mar. 14, 2023), https://slate.com/technology/2023/03/madison-square-garden-facial-recognition-stadiums-list.html; Sara Morrison, *The World's Scariest Facial Recognition Company is Now Linked to Everybody From ICE to Macy's*, Vox (Feb. 28, 2020), https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach.
[35] *See, e.g.*, Donna M. Christiensen et al., *Medical Algorithms are Failing Communities of Color,* HealthAffairs (Sept. 9, 2021) https://www.healthaffairs.org/do/10.1377/forefront.20210903.976632/ ("From consultation programming for glaucoma to automated intake processes in primary care to scoring systems that evaluate newborn' health conditions, patients regularly encounter these technologies and algorithms whether they know it or not."); Andrew Wong et al., *External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients*, 181(8) JAMA Intern Med. 1065 (June 2021), https://pubmed.ncbi.nlm.nih.gov/34152373/; Tom Simonite, *How an algorithm blocked kidney transplants to Black patients*, WIRED (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/; Casey Ross & Bob Herman, *Denied by AI: How Medicare Advantage plans use algorithms to cut off care for seniors in need*, Stat (Mar. 13, 2023); https://www.statnews.com/2023/03/13/medicare-advantage-plans-denial-artificial-intelligence/.
[36] *See, e.g.*, Todd Feathers, *This Private Equity Firm Is Amassing Companies That Collect Data on America's Children*, The Markup (June 11, 2022), https://themarkup.org/machine-learning/2022/01/11/this- private-equity-firm-is-amassing-companies-that-collect-data-on-americas-children; Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, The Markup (Mar. 2, 2021), https://themarkup.org/machine-learning/2021/03/02/major-universities- are-using-race-as-a-high-impact-predictor-of-student-success.); Daan Kolkman, *"F**k the algorithm?" What the world can learn from the UK's A-level grading fiasco, London Sch. Econ. Impact Blog* (Aug. 26, 2020), https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can- learn-from-the-uks-a-level-grading-fiasco/ (grading algorithms).
[37] *See, e.g.*, Harriet Kingbay, *AI and Advertising A consumer perspective* 7 (2020) https://www.harrietkingaby.com/_files/ugd/435e8c_3f6555abb25641be8b764f5093f1dd4f.pdf.
[38] *See, e.g.*, Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Ctr. for Democracy & Tech. (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/.
[39] *See* Mark Blunden, *Booker beware: Airbnb can scan your online life to see if you're a suitable guest*, Evening Standard (Jan. 3, 2020), https://www.standard.co.uk/tech/airbnb-software-scan-online-life- suitable-guest-a4325551.html.

- *Access to credit.* Algorithms are routinely used to dictate creditworthiness and credit limits.[40]
- *Insurance.* Health insurance companies analyze personal data to determine reimbursement decisions and risk scores.[41]

c. Consumers' experiences with automated decisionmaking

Responsive to question II.5

Whether they know it or not, consumers already have extensive experience with automated decisionmaking technologies, including many algorithms that are harmful, invasive, discriminatory, and unfair. Consumers are often unaware when they are subject to an automated decision or whether that determination is adverse, as many of these systems are opaque and hidden from view.

A recent Cisco study highlighted the discrepancy between consumers' and vendors' expectations concerning ADS:

> It can be difficult for consumers to understand the algorithms and automated decisions that may impact them directly, such as when qualifying for a loan or getting a job interview. Ninety-six percent (96%) of organizations in our survey believe they have processes already in place to meet the responsible and ethical standards that customers expect, which is up from 87% last year. Yet, the majority of consumers don't see it that way. As reported in the Cisco 2022 Consumer Privacy Survey, 60% of consumers are concerned about how organizations apply and use [artificial intelligence (AI)] today, and 65% already have lost trust in organizations over their AI practices.[42]

Recent surveys by the Pew Research Center echo these sentiments. A 2022 study found that a larger share of Americans are "more concerned than excited" than are "more excited than concerned" by the increased use of AI in daily life.[43] The same study found that consumer concerns

[40] *See, e.g.*, Genevieve Smith & Ishita Rustagi, *When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity*, Stan. Soc. Innovation Rev. (Mar. 31, 2021), https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity.
[41] *See, e.g.*, EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 90.
[42] *Cisco 2023 Data Privacy Benchmark Study*, Cisco 15 (2023), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf.
[43] Lee Rainie, Cary Funk, Monica Anderson, & Alec Tyson, *How Americans Think About Artificial Intelligence*, Pew Res. Ctr. (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/how-americans-think-about-artificial-intelligence/ .

include potential loss of jobs, privacy considerations, worries that AI's ascent might surpass human skills, a loss of human connection, misuse, and overreliance.[44] A 2023 survey explored public views on AI in health and medicine and found similar concerns, finding that "there's significant discomfort among Americans with the idea of AI being used in their own health care."[45] In the survey, 60% of U.S. adults expressed that they would feel uncomfortable if their own health care provider relied on AI for things like diagnosing disease or recommending treatments, and 57% said this use of AI would make the patient-provider relationship worse.[46] More Americans (37%) are concerned that this type of AI would make the security of patients' records worse compared to the 22% who believed it would improve security.[47] The report cited a major factor in these views: "[a] majority of the public is unconvinced that the use of AI in health and medicine would improve health outcomes."[48]

Consumers have experienced numerous documented harms as a result of the use of commercial automated decisionmaking systems (as well as many harms that cannot be conclusively proven due to the opacity of the systems at play). For example:

- *Hiring and employment.* Workers pushed back against being "hired or fired by algorithm," expressing concerning that it could lead to widespread discrimination and unfair treatment.[49] HireVue, a pre-employment screening company, halted its use of facial recognition after criticism that it was unfair and unlawful (though the company continues to use voice analysis).[50]

---

[44] *Id.*
[45] Alec Tyson, Giancarlo Pasquini, Alison Spencer, & Cary Funk, *60% of Americans Would Be Uncomfortable with Provider Relying on AI in Their Own Health Care*, Pew Res. Ctr. (Feb. 22, 2023), https://www.pewresearch.org/science/2023/02/22/60-of-americans-would-be-uncomfortable-with-provider-relying-on-ai-in-their-own-health-care/.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *AI at work: Staff 'hired and fired by algorithm'*, BBC News (Mar. 25, 2021), https://www.bbc.com/news/technology-56515827.
[50] EPIC, *Facing FTC Complaint From EPIC, Halts Use of Facial Recognition* (Jan. 12, 2021), https://epic.org/hirevue-facing-ftc-complaint-from-epic-halts-use-of-facial-recognition/.

- *Criminal justice.* In 2016, ProPublica reported that an algorithm which purported to predict the likelihood of a person committing a future crime was biased against Black individuals.[51] Facial recognition software misidentified an innocent Baltimore man as a match for a suspect in a crime captured by CCTV, and he remained in jails for days due to the algorithmic error.[52] A Detroit man was wrongfully arrested after facial recognition misidentified him in January 2020.[53] A New Jersey man was arrested after a facial recognition system misidentified him as a "high-profile" match and considered pleading to a crime he did not commit after spending 10 days in jail.[54] Another Detroit man was wrongfully identified by facial recognition software, arrested in front of his children, and detained for 30 hours.[55]

- *Education.* Students in the UK protested after the government proposed using an algorithm to determine their higher education scores during the COVID-19 pandemic.[56] Students pushed back against harmful and invasive use of remote proctoring AI that purported to determine whether students were cheating during schoolwork.[57]

- *Housing.* Tenants in a rent-stabilized apartment complex in Brooklyn fought back against their landlord's proposal to subject them to facial recognition for building access.[58] EPIC warned the Federal Trade Commission (FTC) that AirBnB's use of an algorithm to determine a renter's "trustworthiness" was likely unfair and posed a high risk of disparate and unfair impact.[59]

---

[51] Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[52] Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED (Feb. 28, 2023), https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.
[53] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.
[54] *Id.*
[55] *Id.*
[56] Ammara, *"F*ck the Algorithm"; a Rallying Cry For the Future*, Medium (Aug. 17, 2020), https://medium.com/digital-diplomacy/fuck-the-algorithm-the-rallying-cry-of-our-youth-dd2677e190c.
[57] Todd Feathers, *Schools are Abandoning Invasive Proctoring Software after Student Backlash*, Vice (Feb. 26, 2021), https://www.vice.com/en/article/7k9ag4/schools-are-abandoning-invasive-proctoring-software-after-student-backlash; *see* EPIC, *In re Online Test Proctoring Companies* (2020), https://epic.org/documents/in-re-online-test-proctoring-companies/.
[58] Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html; Erin Durkin, *New York tenants fight as landlords embrace facial recognition cameras*, The Guardian (May 30, 2019), https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex.
[59] Letter from EPIC to the Fed. Trade Comm'n, *In re Airbnb* (Aug. 18, 2022), https://epic.org/wp-content/uploads/2022/08/EPIC-In-re-Airbnb-supplemental-FTC-letter-1.pdf.

- *Taxes.* The IRS was forced to backpedal from its plan to use ID.me—a commercial verification tool that relies in part on facial recognition—as the exclusive means of confirming the identity of taxpayers seeking certain tax records.[60]
- *Public Events and Venues.* The entertainment company which owns Madison Square Garden faced public backlash after the venue used facial recognition technology to identify and remove an attorney who worked at a law firm litigating against the company.[61]

d. Prevalence of algorithmic discrimination

Responsive to question III.6

It is difficult to precisely quantify the prevalence of algorithmic discrimination because individuals rarely know when they have experienced an adverse algorithmic decision, what factors went into such a decision, or whether the decision was influenced by a protected characteristic or proxy for a protected characteristic. Still, there is abundant evidence[62] that such discrimination does occur. To take just a few examples:

- A recent study showed that an algorithm used to determine eligibility and prioritization for kidney transplants unfairly prevented Black patients from receiving transplants.[63]

[60] Rachel Metz, *After face-recognition backlash, ID.me says government agencies will get more verification options*, CNN (Feb. 9, 2022), https://www.cnn.com/2022/02/08/tech/idme-facial-recognition-bypass/index.html.
[61] Kashmir Hill and Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. Times (Dec. 22, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.
[62] *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[63] Tom Simonite, *How an algorithm blocked kidney transplants to Black patients*, WIRED (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/ ("One third of Black patients, more than 700 people, would have been placed into a more severe category of kidney disease if their kidney function had been estimated using the same formula as for white patients. . . . In 64 cases, patients' recalculated scores would have qualified them for a kidney transplant wait list. None had been referred or evaluated for transplant, suggesting that doctors did not question the race-based recommendations."); *see also* EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 69.

- Amazon stopped using a resume-reading algorithm after it discovered that the system taught itself that male candidates were preferable based on the patterns and information that the models were trained on.[64]
- Automated tenant screening reports have wrongfully excluded applicants for housing.[65]

For more examples of discriminatory automated decisionmaking technologies, we refer the Agency to EPIC's recent comments to the Federal Trade Commission on commercial surveillance.[66]

The White House, federal agencies, multiple states,[67] and the District of Columbia[68] have recognized the importance of protections against discriminatory automated decisionmaking technology. The White House's Office of Science and Technology Policy issued an executive order to address the problem of algorithmic discrimination and equity in AI, explaining that "[a]lgorithmic discrimination occurs when automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law."[69] In 2021, the Equal Employment Opportunity Commission launched an initiative to ensure that AI, machine learning, and other emerging technologies comply with federal civil rights laws.[70]

---

[64] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias against Women*, Reuters (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
[65] Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters*, Mark Up (May 28, 2020), https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters.
[66] EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 67–151.
[67] *See* Pollyanna Sanderson, Sara Jordan, & Stacey Gray, *Automated Decision-Making Systems: Considerations for State Policymakers*, Future Privacy F. (May 12, 2021), https://fpf.org/blog/automated-decision-making-systems-considerations-for-state-policymakers/.
[68] Stop Discrimination by Algorithms Act of 2021, D.C. Council, B24-0558, 24th Council (D.C. 2021-2022), https://legiscan.com/DC/bill/B24-0558/2021.
[69] Office of Sci. and Tech. Pol'y, *Algorithmic Discrimination Protections*, White House (Oct. 2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/.
[70] *Artificial Intelligence and Algorithmic Fairness Initiative*, Equal Emp. Opportunity Comm'n (2021), https://www.eeoc.gov/ai.

The Federal Trade Commission has published guidance warning of the "risks, such as the potential for unfair or discriminatory outcomes or the perpetuation of existing socioeconomic disparities" from the use of AI technology.[71] Recognizing that discrimination is common in automated decisionmaking systems, regulators and legislators have begun taking action to address the problem. We encourage the CPPA to do so as well.

III. Cybersecurity audits

The Agency asks what laws currently require cybersecurity audits, to what extent these laws' requirements align with those of Civil Code § 1798.185(a)(15)(A), and what gaps or weaknesses there may be in these regimes. The Agency also asks about other related evaluations that are currently performed, again asking about alignment with § 1798.185(a)(15)(A) and any gaps or weaknesses in these models. The Agency's rules will ultimately determine the scope of these audits and the recommended process and oversight mechanisms necessary to ensure that they are thorough and independent.

We make recommendations below for ways that the Agency can establish strong audit standards while respecting the potential for a harmonizing cross-compliance process. In short: there are significant commonalities among data security standards in existing regulatory and voluntary frameworks. Rather than endorse a single existing model, we urge the Agency to establish its own audit rubric based on the strongest common factors among existing standards. We note that the Center for Internet Security's Critical Security Controls for Effective Cyber Defense (CIS Controls)

[71] Andrew Smith, Dir., FTC Bureau of Consumer Prot., *Using Artificial Intelligence and Algorithms*, Fed. Trade Comm'n Business Blog (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

is the standard most likely to be in wide adoption by companies doing business in California,[72] and we recommend that the Agency develop an audit rubric that builds upon the same principles.

a. Why annual cybersecurity audits matter

Consumers rely on the entities that collect their personal data to take the necessary steps to protect that data. These entities are in control of how much personal data they collect, how long they retain it, how (and whether) they dispose of it, and what safeguards they implement to prevent unauthorized access throughout the data lifecycle. There are cost-effective and well-established methods for reducing the likelihood of breaches and for mitigating the harm of unauthorized access when it does occur. Poor data security practices increase the likelihood and severity of breaches, which in turn increase the risk of identity theft and other downstream harms to consumers. Governing Magazine recently reported that California led the nation in data breaches in the five-year period 2017-2021, with more than 325,000 victims collectively losing more than 3.7 billion dollars (representing more than 18% of losses nationwide).[73]

Downstream consumer harms resulting from data breaches can include identity theft and other forms of account compromise. The Federal Trade Commission (FTC) reported high levels of benefits fraud in 2020 and 2021, in addition to credit fraud increasing from 27% of identity theft

[72] See Kamala D. Harris, Attorney General, *California Data Breach Report* 30 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ("Recommendation 1: The 20 controls in the Center for Internet Security's Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet."). The most recent version of these controls were published two years ago. See Ctr. Internet Sec., *CIS Critical Security Controls Version 8* (May 2021), https://www.cisecurity.org/controls/v8.

[73] Kevin Smith, *California Had the Most Data Breaches in the Last Five Years*, Governing (July 26, 2022), https://www.governing.com/security/california-had-the-most-data-breaches-in-the-last-five-years (citing to Forbes Advisor report).

reports in 2020 and 2021 to 40% of reports in 2022.[74] In 2021, the Department of Justice found that 68% of victims of identity theft suffered $1 or more in direct financial losses with their most recent incident of identity theft[75] and estimated that this fraud cost the U.S. economy more than $15 billion.[76] For example, in late 2020, websites used to generate auto insurance quotes were exploited to obtain personal data later used to submit fraudulent claims for pandemic and unemployment benefits.[77]

The impacts of identity theft can be far-reaching, discovered only after downstream harms have occurred (e.g., through a collections notice for a bill the consumer neither incurred nor knew of), and difficult to remedy after the fact. A Government Accountability Office report indicated that past victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[78] Yet these harms do not appear on the victim's bank statement or credit report and can be nearly impossible to control where a Social Security Number (SSN) is used (by virtue of the role the SSN plays as a government and private-sector identifier).[79]

---

[74] FTC, *Consumer Sentinel Network: Data Book 2022* at 9 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf (calculating percentage by taking fraction of number of reports by theft type out of total identity theft reports); FTC, *Consumer Sentinel Network: Data Book 2021* at 9 (2021), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (same methodology); FTC, *Consumer Sentinel Network: Data Book 2020* at 9 (2020), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf (same methodology).

[75] Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2018* at 9 (Apr. 2020), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

[76] See *id.* at 1 ($15.1 billion in total financial losses due to identity theft where the victim lost $1 or more). This was also true in the DOJ's two prior reports. *See* Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2016* at 1 (Jan. 2019), https://bjs.ojp.gov/content/pub/pdf/vit16.pdf ($17.5 billion); Bureau of Just. Stat., Dep't of Just., *Victims of Identity Theft, 2014* at 7 (Sept. 2015), https://bjs.ojp.gov/content/pub/pdf/vit14.pdf ($15.4 billion).

[77] Industry Letter Re: Cyber Fraud Alert to N.Y. State Dep't of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

[78] U.S. Gov't Accountability Office, GAO-14-34, *Agency Responses to Breaches of Personally Identifiable Information Need to be More Consistent* 11 (2013), http://www.gao.gov/assets/660/659572.pdf.

[79] Br. of Amicus Curiae EPIC at 14, *Storm v. Paytime, Inc.*, No. 15-3690 (3d Cir. Apr. 18, 2016), https://epic.org/documents/storm-v-paytime-inc/.

To make matters worse, a stolen SSN, unlike a stolen credit card, cannot be effectively cancelled or replaced.[80]

Although it is difficult to remedy the harms of identity theft after the fact, preventing the underlying breach is neither difficult nor expensive. The California Attorney General's Office concluded that many of the hundreds of breaches it studied could have been prevented, or detected and corrected more rapidly, by implementation of its recommended data security controls.[81] More broadly, the Department of Homeland Security has estimated that 85% of data breaches were preventable,[82] and more recently the Internet Society has estimated 95% of breaches could have been prevented.[83] The FTC has often noted that reasonable security measures are relatively low-cost.[84] Security technologist and fellow at Harvard Kennedy School Bruce Schneier recently observed in the New York Times:

> In all of these cases, the victimized organizations could have very likely protected our data better, but the reality is that the market does not reward healthy security. Often customers aren't even able to abandon companies with poor security practices, as many of them build "digital moats" to lock their users in. Customers don't abandon companies with poor security practices. Hits to the stock prices quickly recover. It's a

[80] *Id.* at 13.
[81] *See* Harris, *supra* note 72, at 32.
[82] Dep't of Homeland Sec. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016), https://www.us-cert.gov/ncas/alerts/TA15-119A.
[83] Internet Society's Online Trust Alliance, *2018 Cyber Incident & Breach Trends Report* 3 (July 9, 2019), https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf.
[84] *See, e.g.*, Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 11(a), 11(i)(i) (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter [hereinafter *CafePress*]; Complaint, *In re SkyMed International, Inc.*, FTC File No. 1923140 at ¶ 23 (Jan. 26, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923140-skymed-international-inc-matter [hereinafter *SkyMed*]; Complaint, *In re InfoTrax Systems, L.C.*, FTC File No. 1623130 at ¶ 11 (Dec. 30, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3130-infotrax-systems-lc [hereinafter *InfoTrax*]; Complaint, *In re LightYear Dealer Technologies, LLC*, FTC File No. 1723051 at ¶ 22 (Sept. 6, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3051-lightyear-dealer-technologies-llc-matter [hereinafter *LightYear*]; Complaint, *FTC v. Equifax, Inc.*, No. 1:2019-cv-03297 at ¶¶ 23(A)(iv), 24 (N.D. Ga. Jul. 22, 2019), https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3203-equifax-inc [hereinafter *Equifax*]; Complaint, *FTC v. Ruby Life Inc. d/b/a AshleyMadison.com*, No. 1:16-cv-02438 at ¶ 42 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3284-ashley-madison [hereinafter *AshleyMadison*]; Complaint, *In re Lenovo, Inc.*, FTC File No. 1523134 at ¶ 25 (Jan. 2, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3134-lenovo-inc [hereinafter *Lenovo*].

> classic market failure of a powerful few taking advantage of the many, and that failure is one that only representation through regulation can fix.[85]

The burden represented by annual audits pales in comparison to the burdens consumers suffer from unauthorized access to their data. As such, the costs of harm to consumers and to the American economy (e.g., due to fraud facilitated by identity theft) that result from data breaches would be better internalized as preventative data security costs incurred by the entities best positioned to prevent the harm from occurring in the first place.

Cybersecurity audits can identify deficient practices and help companies to shore up vulnerabilities before a breach occurs, mitigating the damage or perhaps preventing it entirely. However, it is important to note that it remains the company's responsibility to maintain best practices in between annual audits.[86] If the audit process amounts to a standalone annual exercise in compliance, it is unlikely to meaningfully improve data security. The Agency has recognized this through its emphasis on the thoroughness and independence of audits and through its questions interrogating the weaknesses and gaps in existing data security assessment models. The Agency is not seeking to mandate completion of a box-checking chore; it has been tasked with identifying a methodology that can best address a core deficiency that persistently hurts trust in businesses and that could continue to leave consumers vulnerable. Although it is unfortunate that deficient data security has been such a needlessly persistent problem, the Agency can benefit from the lessons learned over the last decade to ensure that its audit requirements entail more than box-checking and blind approvals, but rather establish a new and robust standard for businesses entrusted with consumer data.

---

[85] Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, N.Y. Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html.

[86] In the context of credit card payments and data security, for example, Verizon consistently reports that 44% or more of organizations fail to maintain PCI-DSS compliance in between annual compliance validations (most recently more than 56% failed to maintain compliance). *See* Verizon, *2022 Payment Security Report* 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf.

b. Scope of audits

Responsive to questions I.1, 2, and 5

The implicit goal of § 1798.185(a)(15)(A) is to mitigate risks to the privacy and security of consumers' personal information by establishing factors that will reduce that risk and by compelling businesses to address those factors through an annual audit process. Accordingly, the CPPA's audit requirements should identify the right factors for an audit to consider and ensure that the audit process is thorough and independent. There are several provisions common among current data security laws and frameworks which should inform the scope of the annual audit required under § 1798.185(a)(15)(A). These include access controls, secure password practices, user authentication, segmentation of systems, traffic monitoring, ongoing security reviews, data mapping, data minimization, staying current on known vulnerabilities, employee training, overseeing service providers and product integrations, and requiring additional security precautions where appropriate (e.g., remote access and storing and/or transmitting sensitive information).

These provisions are not exhaustive of all issues that could create or exacerbate system vulnerabilities,[87] but each of them should apply to companies at a level commensurate with the scope and scale of the type and volume of data they collect.[88] Just as heightened measures should be required for riskier processing or processing of more sensitive types of data, less stringent measures may be required for companies collecting smaller amounts of data or types of data that inflict less severe harms if breached (e.g., state of residence as opposed to Social Security Number). This "risk-based approach" to data security is already in place in the banking industry,[89] and has been enacted

[87] Device mapping and encryption, for example, were not addressed above.
[88] William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1179 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf (noting that across multiple data security frameworks "the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian").
[89] *See, e.g.*, David W. Perkins, *Tailoring Bank Regulations: Differences in Bank Size, Activities, and Capital Levels* (Dec. 21, 2017), https://digital.library.unt.edu/ark:/67531/metadc1094396/.

as data security policy at the state level.[90] It is likely that a cottage industry will emerge to assist companies with a data security regime that grows as the company's data collection and processing grows (or as those data practices become riskier). We have provided additional detail about how these issues are handled in current laws and frameworks in Appendix 1.

A number of current federal laws impose data security obligations, including the Health Insurance Portability and Accountability Act (HIPAA),[91] Children's Online Privacy Protection Act (COPPA),[92] Gramm-Leach-Bliley Act (GLBA) (specifically the Safeguards Rule),[93] and Federal Credit Report Act (FCRA).[94] Several states other than California also have data security laws, including Massachusetts,[95] New York,[96] and Oregon.[97] Existing frameworks include those proposed by the Financial Industry Regulatory Authority (FINRA),[98] National Institute of Standards and

[90] *See, e.g.*, 201 Mass. Code Regs. 17.03(1) (2010), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download (requiring a security program include "administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information").
[91] 45 C.F.R. pt. 160; 45 C.F.R. pt. 164.
[92] 16 C.F.R. pt. 312; 16 C.F.R. §§ 312.3(e), 312.8.
[93] 16 C.F.R. pt. 314.
[94] 16 C.F.R. pt. 682.
[95] 201 Mass. Code Regs. 17.00 (2010).
[96] N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2022) (NYDFS regs); N.Y. Gen. Bus. Law, § 899-bb (2020) (SHIELD Act data security provisions).
[97] Or. Rev. Stat. tit. 50, § 646A.622 (2021).
[98] *See, e.g.*, FINRA, *Report on Cybersecurity Practices* (Feb. 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf [hereinafter *FINRA 2015*]; FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf [hereinafter *FINRA 2022*].

Technology (NIST),[99] Cyber and Infrastructure Security Agency (CISA),[100] and Federal Financial Institutions Examination Council (FFIEC),[101] as well as industry standards such as the Payment Card Industry Data Security Standards (PCI-DSS).[102]

Notably in 2016, then-Attorney General of California Kamala Harris set the expectation that businesses would conform their data security practices to the requirements of the Center for Internet Security (CIS) framework, stating that "[t]he set of 20 [CIS] Controls constitutes a minimum level of security—a floor—that any organization that collects or maintains personal information should meet."[103] The 2016 CIS framework outlined explicitly parallel recommendations from NIST, International Organization for Standardization (ISO), HIPAA, FFIEC, and PCI-DSS frameworks. The FTC has also identified deficient data security practices in a number of its Section 5 enforcement actions over the last 10 years.[104] Cyber risk insurance guidance continues to play an important role in shaping data security practices and to indicate what priorities have been

[99] NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version* 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter *NIST 1.1*]; NIST, *Getting Started with the NIST Cybersecurity Framework: A Quickstart Guide* (Updated Apr. 19, 2022), https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide [hereinafter *NIST Quickstart*] (providing a helpful high-level overview).

[100] CISA, *Cross-Sector Cybersecurity Performance Goals* (2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf [hereinafter *CISA Goals*]. Currently CISA has only offered guidelines, but new breach reporting rules promulgated under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) may be mandatory.

[101] *See, e.g.*, FFIEC*, FFIEC Cybersecurity Assessment Tool: Inherent Risk Profile*, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Inherent_Risk_Profile.pdf.

[102] *See, e.g.*, *Requirements and Testing Procedures Version 4.0*, PCI Security Standards Council (Mar. 2022), https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf.

[103] *See* Harris, supra note 72, at 31 ("The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable."); *id.* at Appendix B. Note the numbering on these controls have been updated since the 2016 Data Breach Report—most recently in CIS Critical Security Controls Version 8 (May 2021), which is the version numbering we cite to in Appendix 1.

[104] *See, e.g.*, First Am. Complaint, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), https://www.ftc.gov/legal-library/browse/cases-proceedings/1023142-x120032-wyndham-worldwide-corporation [hereinafter *Wyndham*]; *CafePress*; *SkyMed*; *InfoTrax*; *LightYear*; *Equifax*; *AshleyMadison*; *Lenovo*; Complaint, *FTC v. D-Link Corp.*, No. 3:17-CV-00039-JD (N.D. Cal. Mar. 20, 2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/132-3157-x170030-d-link [hereinafter *D-Link*].

emphasized by businesses with explicit incentives to mitigate the risks of breaches. For example, several cyber insurance companies ask prospective insured about firewalls, password strength, multi-factor authentication, and patching known vulnerabilities in their own risk assessment questionnaires.[105] Other laws and frameworks (e.g. GLBA) can fall short in a number of ways, including by assuming that a consumer who has not opted out of processing is aware of and accepts the risks of that processing, by allowing data sharing without concern for data security, and by having limited applicability, e.g. only governs health care providers, only protects current customers, etc.

Based on CIS controls, FTC actions, cyber insurance priorities, and other laws and frameworks, the audits required by § 1798.185(a)(15)(A) should include at a minimum:

- data mapping;
- data minimization;
- access controls;
- secure password practices;
- user authentication;
- segmentation of systems;
- traffic monitoring;
- ongoing security reviews;
- staying current on known vulnerabilities;
- employee training; and
- overseeing service providers and product integrations.

Additional security precautions may be necessary where appropriate (e.g., remote access or processing sensitive information).

[105] See McGeveran, *supra* note 88, at 1172–73 (citing to Sample cyber insurance applications, IAPP, https://iapp.org/resources/article/sample-cyberinsurance-applications/ (last visited Mar. 17, 2023)) (noting that all three companies inquire about firewalls, password strength, and multifactor authentication in their risk assessment questionnaires).

The Agency should also establish a set of best practices as benchmarks for its required audit categories that incorporates but is not necessarily limited to the list above. It may be helpful to present the recommended practices as basic cybersecurity hygiene for the modern threat environment.

c. Deficiencies in existing authorities

Responsive to question I.1

The Agency specifically asks about gaps or weaknesses in existing data security regimes. Many laws are limited in applicability: HIPAA only applies to health care providers (which may not include period tracker apps),[106] and although GLBA applies clearly to current customers, it is less clear whether its data security-focused Safeguards Rule applies to former customers.[107] Relatedly, several laws allow for disclosure of information to third parties who are not necessarily subject to the same data security requirements as the regulated entity.[108] Two recent breaches of AT&T subscriber data underscore the importance of extending data security requirements to third parties with access to consumer data.[109] Overseeing service providers and product integrations must be included within the scope of the Agency's annual audits if only for this reason.

---

[106] *See, e.g.*, Charles Ornstein, *Federal Patient Privacy Law Does Not Cover Most Period-Tracking Apps*, ProPublica (July 5, 2022), https://www.propublica.org/article/period-app-privacy-hipaa.

[107] *See* Fed. Trade Comm'n, *How to Comply with the Privacy of Consumer Financial Information Rule the Graham-Leach-Bliley Act*, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act (last visited Mar. 27, 2023) (data security rules apply to customers but it is possible for an organization to have consumers who do not maintain a customer relationship; former customers seem to be considered consumers not customers); 16 C.F.R. pt. 314.3 (protecting customer information); 16 C.F.R. pt. 314.2 (defining "customer information", "customer", and "consumer").

[108] As a few examples: FCRA/FACTA and GLBA allow for sharing with affiliates, HIPAA/HITECH allow exceptions for marketing and for collecting payments, GLBA allows exceptions for "necessary services" and allows contracts enforcing confidentiality but does not require contracts enforcing data security.

[109] *See* David Lumb, *AT&T Vendor Data Breach Exposed 9 Million Customer Accounts*, CNET (Mar. 9, 2023), https://www.cnet.com/tech/mobile/at-t-vendor-data-breach-exposed-9-million-customer-accounts/; *see also* Brian Krebs, *It Might Be Our Data, But It's Not Our Breach*, Krebs on Security (Aug. 11, 2022), https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/.

Additionally, GLBA and prescreening under FCRA are premised on an opt-out version of the notice and choice model of consumer consent, with notoriously difficult opt-out mechanisms.[110] The Agency must include data mapping and data minimization within the scope of its annual audits to ensure the company is aware of what data it actually needs and how that data should be protected, rather than permitting companies to rely on outdated methodologies that attempt to shift the burden to consumers.[111]

Some laws do not incorporate established best practices in their data security requirements. For example, the GLBA Safeguards Rule does not explicitly require segmentation of systems,[112] despite the prevalence of that best practice factor in CIS Controls, FTC enforcement actions, and voluntary frameworks developed by expert entities like CISA and NIST.[113]

d. Thoroughness and independence of auditors

Responsive to questions I.1, 2, and 4

Section 1798.185(a)(15)(A) requires audits that are thorough and independent. We understand "thorough" to require actual analysis and not merely a checkbox exercise. We understand "independent" to mean operating without the audited company's influence. As one example, an audit should not merely report the audit subject's response as to whether the organization has a strong

[110] *See, e.g.*, Elizabeth D. De Armond, A Dearth of Remedies, 113 Penn St. L. Rev. 1, 18 (2008) (noting that even a consumer who seeks to opt out may not have their decision respected if the consumer fails to precisely follow opt-out instructions); EPIC, *The Fair Credit Reporting Act (FCRA)*, https://epic.org/fcra/ (2023) (discussing the problems with an opt-out model for prescreening).
[111] *See, e.g.*, Remarks of Comm'r Rebecca Kelly Slaughter, FTC Hearing #12, The FTC's Approach to Consumer Privacy (Apr. 10, 2019), https://www.ftc.gov/system/files/documents/public_statements/1513009/slaughter_remarks_at_ftc_approach_to_consumer_privacy_hearing_4-10-19.pdf; *Data Minimization White Paper*, *supra* note 23, at 5 (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/ ("The current 'notice and choice' regime, in which consumers are expected to read extensive privacy policies and make 'all or nothing' decisions about whether to use an online service or app, makes it impossible for consumers to meaningfully participate in the market while protecting their privacy.").
[112] *FTC Safeguards Rule: What Your Business Needs to Know*, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023).
[113] See Appendix 1.

password policy in place; rather, the auditor should actually attempt to set up access with a weak password to see if the policy has been implemented and works as intended.[114]

Twitter whistleblower Peter "Mudge" Zatko remarked in Congressional testimony last year:

> "[H]ow was Twitter still operating like this? Since there was a 2011 consent decree that was aimed at addressing a fair amount of this? . . . One, there were a lot of evaluations and examinations, which were interview questions. So essentially, the organization was allowed to grade their own homework. Did you make things better? Yes, we did. Okay, check. There wasn't a lot of ground truth. There wasn't a lot of quantified measurements. And a fair amount of the interviews came from companies, auditors that Twitter themselves were able to hire. So I think that's a little bit of a maybe conflict of interest."[115]

Mudge suggested the solution include "accountability, and setting quantitative goals and standards that can be measured and audited independently" in order to "change management structures, and drive change in companies when it's needed such as this."[116]

We urge the Agency to establish quantitative goals and standards, requiring actual investigation and analysis and not merely interviews. We also encourage the Agency to establish processes that reduce the likelihood of a conflict of interest as described in Mudge's testimony. For example, the Agency could certify auditors and randomize which get assigned to which company.

e. Triggers for the audit requirement and cross-compliance

Responsive to questions I.1, 2, and 3

The Agency asks about the benefits and drawbacks for consumers if it accept audits completed by businesses to comply with existing laws and asks how businesses should demonstrate that those audits comply with the CPPA's requirements. Because laws like GLBA have significant gaps and weaknesses—including failing to incorporate best practice factors, failing to capture data

[114] Kevin G. Coleman, *Security Assessment or Security Audit?*, infoTECH Spotlight (Sept. 21, 2009), https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.
[115] Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022) (testimony of Peter Zatko), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower.
[116] *Id.*

security risks at third party entities, and allowing companies to rely on purported consumer consent rather than strengthening inadequate data security practices—the Agency should measure compliance against its own standards. The Agency should therefore not accept audits geared towards other legal frameworks as compliant with the CCPA cybersecurity audit requirement.

However, the Agency could establish supplemental requirements that would allow companies to use existing audits in conjunction with specific supplemental reviews to demonstrate compliance. For example, the GLBA Safeguards Rule does not explicitly require segmentation of systems,[117] so a company seeking to demonstrate compliance with § 1798.185(a)(15)(A) through its GLBA reporting might need to provide supplemental information regarding practices such as internal firewalls. Similarly, the Agency could require companies to supplement their existing reporting to ensure data that will be shared with affiliates or third-party vendors (e.g., for marketing or payment collections purposes) will be appropriately secured. The Agency can get ahead of industry arguments that existing reporting is sufficient by clarifying upfront what supplemental information it will require if companies intend to rely on existing audits.

Additionally, if supplemental information is required, to the extent that the existing audit includes a holistic analysis component, that analysis should be revisited taking into account the supplemental information which was not required in the existing audit. The FFIEC framework for example concludes with an overall inherent risk profile rating, based on multiple factors that framework takes into account, such as number of devices, use of person-to-person payments, and access controls.[118] Factors such as data minimization however are outside its scope. If the Agency decides to accept audits based on the FFIEC framework, it should require an updated inherent risk

[117] *FTC Safeguards Rule: What Your Business Needs to Know*, *supra* note 112.
[118] *See* FFIEC, *FFIEC Cybersecurity Assessment Tools ver. 1.1* at app. A, (May 2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_Appendix_A_May_2017.pdf.

profile rating that reflects all of the key protocols of priority to the Agency, not merely those recommended in the FFIEC model. However, if an FFIEC-based audit already incorporates this "supplemental" information (e.g., data minimization), any revision to the audit would likely be unnecessary.

Audits must also provide detail sufficient to demonstrate that the auditor was thorough. Companies should not be able to merely certify that they have fully addressed the critical areas considered in a cybersecurity audit without actually improving their practices.[119] The Agency should not deem an entity audit process compliant unless that entity clearly establishes that its audit process was sufficiently independent and that it thoroughly reviewed all of the best practice factors identified in the Agency's regulatory framework.

How a business might demonstrate that existing audits comply with the requirements of § 1798.185(a)(15)(A) will likely depend upon what requirements the Agency actually imposes in its audits. Regardless of how the Agency chooses to define the scope of annual cybersecurity audits, we recommend that the Agency require companies to submit any audits intended to satisfy 1798.185(a)(15)(A). This will equip the Agency to analyze trends, propose new supplemental reporting requirements that better reflect the evolving threat landscape, and offer education and trainings for common weaknesses identified from reviewing the submitted audits.[120]

---

[119] *See, e.g.*, R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 Vill. L. Rev. 625, 644 (2004) ("Financial institutions have sent out billions of notices without any change in privacy materializing."). Although the author discussed privacy concerns, the critique of compliance disconnected from reality is applicable to data security as well.

[120] Indeed Profs. Solove and Hartzog argue that "[g]overnment organizations could act proactively to hold companies accountable for bad practices before a breach occurs, rather than waiting for an attack. This strategy would strengthen data security more than the current approach of focusing almost entirely on breached organizations." Daniel J. Solove & Woodrow Hartzog, *Data Vu: Why Breaches Involve the Same Stories Again and Again*, Sci. Am. (July 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4326723.

§ 1798.185(a)(15)(A) requires businesses to perform an annual cybersecurity audit when their processing of consumers' personal information presents significant risk to consumers' privacy or security. It also establishes that the size and complexity of the business and the nature and scope of data processing activities should inform whether that data processing may result in significant security risks, thereby triggering the audit requirement. We urge the Agency to err on the side of inclusion, especially as the Agency's authority to require less frequent or less robust assessments from smaller and simpler organizations is ambiguous. This means that data held by organizations that do not satisfy the "significant risk" threshold could be stored or shared without adequate data security protections. As we have noted in a prior filing,[121] "significant risk" should be understood to mean nontrivial risk rather than exceptional risk. We reiterate here that this interpretation not only aligns with the goals of the CPRA but also aligns with Civil Code § 1798.81.6, which defines "significant risk" as a risk that "*could reasonably result* in a breach of the security of the system . . . of personal information[.]"[122]

We also maintain that Senator Kirsten Gillibrand's Data Protection Act[123] offers a useful compilation of hazardous data processing activities. However, regarding the "nature and scope of data processing" language in § 1798.185(a)(15)(A), again the Agency should consider whether the processing could reasonably result in compromising the privacy or security of consumer data, not merely whether the data is particularly sensitive. For example, while a definition of sensitive information might not include the list of websites for which a consumer maintains a user account, publicizing that list could compromise the consumer's privacy (as it may reveal religious, health, sexual, or other personal information) and expose the consumer to more sophisticated phishing

[121] EPIC et al. 2021 CCPA Comments, *supra* note 3, at 3.
[122] Civ. Code § 1798.81.6(c) (emphasis added).
[123] S. 2134 § 2(11), 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/2134/text.

attacks. Not limiting the audits to sensitive data processing is also consistent with the risk assessment language of the statute, which requires risk assessments even when a business does not process special categories of personal data that qualify as "sensitive."[124]

Factoring in "the size and complexity of the business" should be secondary to the magnitude of the possible harm. An organization that is too undercapitalized to adequately safeguard consumer data should not be permitted to collect it, as that would expose the data to disproportionate risk of unauthorized access.

f. Other important principles

Responsive to questions I.1, 2, and 3

We urge the Agency to prioritize best practice over harmonization, not only because it will result in the best protections for consumers but also because it is likely that subsequent regulations will complicate an approach primarily driven by harmonization. For example, new regulations will likely result from the recent Whitehouse National Cybersecurity Strategy[125] and the FTC's rulemaking on commercial surveillance and data security.[126] In a breach reporting context specifically, new regulations could also include Cyber and Infrastructure Security Agency (CISA)

[124] Civ. Code § 1798.140(ae).
[125] *See FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*, The White House (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.
[126] See Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security.

rules under CIRCIA,[127] an update by the Federal Communications Commission (FCC) to its CPNI rules,[128] and the Securities and Exchange Commission (SEC)'s rulemaking on cyber incidents.[129]

IV. Risk assessments

A risk assessment, also known as a data protection impact assessment or privacy impact assessment, is an analysis of how and why personally identifiable information will be collected, processed, stored, and transferred. The term may also describe an assessment of the privacy and other data-driven risks posed by the use of an algorithm or automated decision-making system. The objective of a risk assessment is to "anticipate[] problems, seeking to prevent, rather than to put out fires."[130] When implemented properly, risk assessments force institutions to carefully evaluate the full spectrum of privacy and data-driven risks of a contemplated processing activity, to identify and implement measures to mitigate those risks, and to determine whether the processing activity can be justified in light of any risks that cannot be fully mitigated. A risk assessment can also provide regulators and the public with vital information about processing activities that may pose a threat to privacy and civil rights.

A risk assessment should not be a simple box-checking exercise or a static, one-off undertaking. Rather, it is "a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should continue until

[127] See *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, Cybersec. & Infrastructure Sec. Agency (2022) https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.
[128] *See FCC Proposes Updated Data Breach Reporting Requirements*, Fed. Commc'ns. Comm'n (Jan. 6, 2023), https://www.fcc.gov/document/fcc-proposes-updated-data-breach-reporting-requirements.
[129] *See SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, Sec. & Exch. Comm'n (Mar. 9, 2022), https://www.sec.gov/news/press-release/2022-39; *SEC Reopens Comment Period for Proposed Cybersecurity Risk Management Rules and Amendments for Registered Investments and Funds*, Sec. & Exch. Comm'n (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-54.
[130] *Privacy Impact Assessment* v (David Wright & Paul de Hert, eds., 2012) (foreword by Gary T. Marx).

and even after the project has been deployed."[131] Or as the Office of Management and Budget warns federal agencies, a risk assessment "is not a time-restricted activity that is limited to a particular milestone or stage of the information system or [personally identifiable information] life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles."[132]

As the Agency develops regulations concerning the scope, frequency, content, and availability of risk assessments under the CCPA, we urge you to bear these hallmarks of effective risk assessments in mind. Specifically, we recommend that the Agency (a) draw on the strongest risk assessment frameworks that have already been developed, including those in the Colorado Privacy Act and the General Data Protection Regulation; (b) adopt a definition of "significant risk" which is both inclusive and flexible enough to account for emerging data-driven risks; (c) direct businesses to include content analogous to what is required under the GDPR and recently-developed Colorado Privacy Act regulations; (d) not allow businesses to rely on risk assessments from another jurisdiction unless the assessments (and any necessary addenda) would independently satisfy CCPA requirements; (e) direct businesses to submit each risk assessment in full to the Agency and to prepare a summarized or redacted version for public consumption; and (f) not extend special treatment to businesses that have less than $25 million in annual gross revenues if they otherwise qualify as a CCPA-covered business based on their processing of personal information.

a. Existing laws and frameworks.

Responsive to questions I.1

Although there are a variety of risk assessment frameworks in use, we highlight five in particular as valuable points of reference for the Agency:

[131] *Id.* at 5–6.
[132] Off. of Mgmt. & Budget, Exec. Off. of the President, *OMB Circular A-130: Managing Information as a Strategic Resource* app. II at 10 (2016).

- Article 35 of the General Data Protection Regulation[133] and implementing guidance;[134]
- The Colorado Privacy Act[135] and implementing regulations;[136]
- The Federal Chief Information Officers Council Algorithmic Impact Assessment tool;[137]
- The Canadian Government's Algorithmic Impact Assessment tool;[138] and
- The E-Government Act of 2002[139] and implementing guidance.[140]

The relevant strengths and gaps of these frameworks are addressed throughout the remainder of this section.

b. Significant risk

Responsive to question II.3

Establishing a strong and effective definition of the term "significant risk" in the CCPA is vital.[141] Under section 1798.185(a)(15), the Agency must issue regulations requiring "businesses whose processing of consumers' personal information presents *significant risk* to consumers' privacy or security" to conduct risk assessments.[142] The CCPA does not define "significant risk," but the Agency should interpret this term broadly to maximize the protection afforded to California residents and to ensure that businesses routinely evaluate the hazards of processing and storing personal information. A "significant risk" must be understood to mean a *material* or *nontrivial* risk rather than an exceptional or unusual one. Establishing too high a threshold for audits and risk

[133] Commission Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119).
[134] Article 29 Data Protection Working Party, *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* at (Oct. 4, 2017), https://ec.europa.eu/newsroom/article29/items/611236.
[135] C.R.S. § 6-1-1309.
[136] 4 CCR 904-3, https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.
[137] *Algorithmic Impact Assessment*, CIO.gov (last visited Mar. 27, 2023), https://www.cio.gov/aia-eia-js/.
[138] *Algorithmic Impact Assessment tool*, Gov't of Canada (Jan. 19, 2023), https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.
[139] E-Government Act, Pub. L. No. 107-347, § 208(b)(2)(B)(ii), 116 Stat. 2899, 2901 (Dec. 17, 2002).
[140] OMB, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10.
[141] Civ. Code § 1798.185(a)(15).
[142] *Id*. (emphasis added).

assessments would unduly limit the businesses from which a careful analysis of privacy and data-driven risks is required, make it easier for businesses to avoid assessment obligations by strategically downplaying the risks of their processing activities, and undermine the express data protection purposes of the CCPA as amended.

Not only is a broad reading of "significant risk" consistent with the aims of the CCPA; it also aligns with the meaning of the term in a related provision of the Civil Code concerning personal data. As noted above, section 1798.81.6 imposes various obligations on credit reporting agencies whose computer systems are "subject to a security vulnerability that poses a *significant risk* . . . to the security of computerized data that contains personal information[.]"[143] The term "significant risk" is defined in the same section as a risk that "*could reasonably result* in a breach of the security of the system . . . of personal information[.]"[144] Carrying this definition forward to the CCPA, the Agency should construe the phrase "presents significant risk to consumers' privacy or security" as referring to data processing that *could reasonably result* in harm to consumers' privacy or civil rights, not merely processing that is likely or certain to cause such harm. This also follows from the categories of information that the CCPA requires businesses to include in a risk assessment. Such assessments must specify "*whether* [their] processing involves sensitive personal information,"[145] which indicates that risk assessments are required even when a business does not process special categories of personal data that qualify as "sensitive."[146]

The Agency asks for views on whether its definition of "significant risk" should follow the approach outlined in the European Data Protection Board (EDPB)'s Guidelines on Data Protection Impact Assessments. Adopting this approach would require businesses to conduct a risk assessment

[143] Civ. Code § 1798.81.6(a) (emphasis added).
[144] Civ. Code § 1798.81.6(c) (emphasis added).
[145] Civ. Code § 1798.185(a)(15)(A) (emphasis added).
[146] Civ. Code § 1798.140(ae).

if a processing activity falls into two (and in some cases, just one) of nine categories: evaluation or scoring, automated-decision making with legal or similar significant effect, systematic monitoring, sensitive data processing, processing on a large scale, matching or combining of datasets, processing of data concerning vulnerable data subjects, processing involving innovative uses or new technologies, and processing that would impede an individual's exercise of rights or access to a service or contract.[147]

We generally support the EDPB's approach, but with two caveats. First, as reflected in the Colorado Privacy Act,[148] we urge the Agency to add two additional processing categories to this list: (1) processing personal data for purposes of behavioral advertising and (2) selling, sharing, or transferring personal data to third parties. Although these categories may overlap in significant part with the categories set out by the EDPB, both forms of processing present sufficiently acute risks to individuals as to warrant separate inclusion.

Second, we urge the Agency to adopt an overarching definition of "significant risk" (consistent with the above discussion) as a backstop to any enumerated risky processing activities. As the EDPB notes of its own nine-criteria list: "There may be 'high risk' processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to [Data Protection Impact Assessments]."[149] Mindful of this possibility, the Agency should clarify that "significant risk" is present whenever a processing activity *could reasonably result* in harm to consumers' privacy or civil rights, and that any enumerated examples of such risky activities are non-exhaustive. This umbrella definition would account for emerging processing activities that may pose heightened risks to individuals not apparent from the current state of

[147] Article 29 Data Protection Working Party, *supra* note 134, at 9–11.
[148] C.R.S. § 6-1-1309(2).
[149] Article 29 Data Protection Working Party, *supra* note 134, at 9.

technology, and it would provide additional guidance for determining whether a processing activity that falls into one or more enumerated categories necessitates the completion of a risk assessment.

c. Content of assessments

Responsive to question II.4

With respect to the minimum content businesses should be required to include in risk assessments, we agree with the Agency's focus on the GDPR and the Colorado Privacy Act. We believe these two frameworks, along with the guidance and regulations that implement them, provide the best template for the Agency to set out the categories of information and analysis that must be included in a business's risk assessment. Further, we highlight specifically the Office of Management & Budget's requirement that federal agencies' impact assessments under the E-Government Act concerning "major information systems" must "reflect more extensive analyses of":

1. the consequences of collection and flow of information,
2. the alternatives to collection and handling as designed,
3. the appropriate measures to mitigate risks identified for each alternative and,
4. the rationale for the final design choice or business process.[150]

We also refer the Agency to EPIC's recent comments to the FTC concerning commercial surveillance. Building on a proposed list of elements suggested by the Commission, EPIC recommended that impact assessments required under a trade rule include:

- The data [companies] use;
- How they collect, retain, disclose, or transfer that data;
- How they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods;
- How they process or use that data to reach a decision;
- Whether they rely on a third-party vendor to make such decisions;
- The impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers;
- Risk mitigation measures to address potential consumer harms[;] …
- The purpose(s) for which the company will collect, process, retain, or make available to third parties each category of personal data;

[150] *Id.* at 34.

- The sources of the personal data the company will collect, process, retain, or make available to third parties;
- Which third parties and service providers, if any, the company will make personal data available to;
- What notice or opportunities for consent will be provided to consumers concerning the company's collection, processing, or retention of their personal data or the making available of such information to third parties;
- The potential harms that might result from such processing, including but not limited to privacy, physical, economic, psychological, autonomy, and discrimination harms;
- The company's asserted need to engage in such collection, processing, retention, or transfer of personal information;
- Any alternatives to such collection, processing, retention, or transfer of personal information seriously considered by the company and the reason(s) why such alternatives were rejected;
- How the asserted benefits resulting from such collection, processing, retention, or transfer to the company, the consumer, other stakeholders, and the public compare to the risks to the consumer; and
- A plain language summary of the assessment that would be comprehensible to a reasonable consumer.[151]

EPIC also recommended that the Commission require companies using automated decision-making systems to make or inform determinations about individuals to disclose, at minimum, the following about each system:

1. A detailed description of the intended purpose and proposed use of the system, including:
    a. What decision(s) the system will make or support;
    b. Whether the system makes final decision(s) itself or whether and how supports decision(s);
    c. The system's intended benefits and research that demonstrates such benefits;
2. A detailed description of the system's capabilities, including capabilities outside of the scope of its intended use and when the system should not be used;
3. An assessment of the relative benefits and costs to the consumer given the system's purpose, capabilities, and probable use cases;
4. The inputs and logic of the system;
5. Data use and generation information, including:
    a. How the data relied on by the system is populated, collected, and processed;
    b. The type(s) data the system is programmed to generate;
    c. Whether the outputs generated by the system are used downstream for any purpose not already articulated;
6. Yearly validation studies and audits of accuracy, bias, and disparate impact; and

[151] EPIC FTC Comments on Commercial Surveillance, *supra* note 7, at 163–64.

7. A detailed use and data management policy.[152]

Finally, the Algorithmic Impact Assessments tools of the U.S. Federal Chief Information Officers Council[153] and the Canadian Government[154] provide a helpful example of the types of information that should appear in a risk assessment of an automated decision-making system. In addition to the content of these tools, the Agency should consider developing a similar web portal for businesses to submit risk assessment summaries as means of simplifying compliance, enforcement, and trend measurement.

d. Cross-compliance

Responsive to question II.5

As we note above with respect to cybersecurity audits, we believe that risk assessments completed in compliance with analogous data protection frameworks of other jurisdictions can serve as the basis for a CCPA-compliant risk assessment, subject to two conditions. First: the risk assessment must be supplemented with any content and analysis required by the CCPA that is not present in the original assessment. The Agency should not permit a substandard risk assessment to fulfill a business's CCPA obligations merely because it satisfies the laws of another jurisdiction. Doing so could encourage a race to the bottom, in which the least rigorous risk assessment rules would become the de facto national standard. Second (as we explain with respect to cybersecurity audits): if supplemental information is required, to the extent that the existing assessment includes a holistic analysis component, that analysis must be revisited, taking into account the supplemental information which was not found in the original assessment. Businesses cannot be permitted simply to drop in additional information and assume that the outcome of an assessment ostensibly based on that information will remain unchanged.

---

[152] EPIC FTC Comments on Commercial Surveillance, *supra* note 77, at 84–85.
[153] Algorithmic Impact Assessment, *supra* note 137.
[154] Algorithmic Impact Assessment tool, *supra* note 138.

As set out below, we believe the best mechanism for businesses to demonstrate that their risk assessments are compliant is for CCPA regulations to require routine submission of such assessments into database maintained by the Agency. Although the Agency may not be in a position to fully review each assessment submitted, even the possibility that an assessment may be randomly selected for a CPPA audit would incentivize strict compliance.

e. Format and frequency

Responsive to questions II.6 and 8

The most effective way to implement the regular submission mandate of section 1798.185(a)(15)(B) is to require businesses to submit to the Agency both (1) a complete written record of each risk assessment mandated by the CCPA, and (2) a plain language summary of each assessment sufficient for both Agency personnel and interested members of the public to understand the nature, scope, purpose, risks, and asserted justification of each covered processing activity. Further, the Agency should require that each risk assessment and summary be submitted 14 days prior the processing activities it covers; updated and resubmitted 14 days prior to any material changes to covered processing activities; and reviewed—and if necessary, updated—no less than once every six months. Finally, the Agency should maintain a public database of summary risk assessments and require businesses to make such documentation directly available to interested individuals.

The Agency asks whether businesses should be required to submit a summary risk assessment to the Agency on a regular basis as an alternative to submitting every risk assessment. The answer is *both*. Summaries would assuredly be valuable for oversight purposes, as they would enable the Agency to readily identify trends, areas of concern, and data processing activities warranting further investigation across the private sector. To this end, the Agency should establish an online portal for businesses to submit summaries in a standardized format, one analogous to the

Algorithmic Impact Assessments tool of the Federal Chief Information Officers Council.[155] These standardized summaries should include sufficient detail—and be written in sufficiently plain language—for the average reader to understand the nature, scope, purpose, risks, and asserted justification of each covered processing activity.

Still, summaries are by their nature incomplete: they omit detail and can obscure (intentionally or not) critical information necessary to understand the full risk profile of business's processing activities. They simply do not tell the full story. For these reasons, the Agency should also direct businesses to submit their full risk assessments to the CPPA at the time they are completed or updated. Just as a business operating in California must file a complete tax return with the Franchise Tax Board (FTB),[156] it must also file a complete risk assessment with the CPPA if it intends to engage in the processing of personal information that poses a significant risk. As with a tax return received by the FTB, the Agency's receipt of a risk assessment would not imply that the Agency endorses the content of that assessment or open a safe harbor to a business for unlawful conduct; it would simply reflect a business's own assertions concerning its processing activities. If the Agency later becomes aware of apparent CCPA violations by a business—whether through an audit of that business's risk assessment or other means—the Agency would remain free to investigate and take appropriate enforcement action.

The fact that resource limitations may prevent the Agency from reviewing every risk assessment upon filing does not diminish the value of having at-will capability to retrieve and audit such assessments through a central, Agency-controlled database. Indeed, the knowledge that each risk assessment will be accessible to the Agency at its discretion will provide a powerful incentive

[155] *See id.*; Algorithmic Impact Assessment, *supra* note 137.
[156] *Doing business in California*, Franchise Tax Bd. (2023), https://www.ftb.ca.gov/file/business/doing-business-in-california.html.

for businesses to scrupulously evaluate, document, and mitigate the risks posed by their processing of personal data. This would reduce the need for the Agency to rely on the attestation of a corporate officer that a business's "summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements." And like the FTB, the CPPA can maintain such a database while protecting confidential business information from being "divulge[d]" or exposed to the public.[157]

With respect to what should be considered "regular" submission, we renew our recommendation that businesses be required to conduct each risk assessment as soon as the business takes material steps toward data processing activities that may pose a significant risk to individuals. To be fully effective, a risk assessment must "begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project."[158] A plausible outcome of a risk assessment should be a decision to abandon or significantly modify a proposed processing activity because it poses an unacceptable risk to individuals—an outcome that is far less likely to occur if a business completes an assessment at the last second. In the interests of establishing clear expectations for businesses and an enforceable standard for the Agency, we recommend that the Agency direct businesses to submit full risk assessments no less than 14 days before engaging in processing activities (or undertaking significant modifications to existing processing activity) that would trigger the assessment requirement.

We also recommend that businesses be required to review—and if necessary, update and resubmit—privacy risk assessments (1) 14 days in advance of any change to a business's data processing activities that might reasonably alter the resulting risks to individuals, and (2) in any event no less than once per six-month period. In most cases, a six-month review requirement would

[157] Cal. Civ. Code § 1798.185(a)(15)(B).
[158] *Privacy Impact Assessment*, *supra* note 130, at 5–7.

not necessitate further documentation from a business, as such updates to an assessment would generally be due to the Agency before material changes are made to a business's processing activities.

Finally, we urge the Agency to (1) establish a publicly accessible and searchable database that includes, at a minimum, the risk assessment summaries submitted by businesses; and (2) require businesses to disclose the same documentation in a conspicuous manner to interested members of the public. In addition to forcing an institution to evaluate and mitigate the harms of data processing, a risk assessment "also serves to inform the public of a data collection or system that poses a threat to privacy."[159] Although the CPRA already requires the agency to "provide a public report summarizing the risk assessments filed with the agency,"[160] we believe it is critical to make more granular information presumptively public and enable interested individuals to learn more about specific products and services that may pose a risk to their privacy. To this end, the Agency should also explore the possibility of requiring presumptive public disclosure of the full underlying risk assessments, subject only to the narrow redactions necessary to protect data security and trade secrets.

f. Companies grossing less than $25 million per year

Responsive to question II.7

The risk assessment compliance requirements for businesses with less than $25 million in annual gross revenues should not differ materially from companies above that threshold. As the CCPA itself reflects, a business grossing less than $25 million a year can pose meaningful risks to the privacy and civil rights of individuals if it "annually buys, sells, or shares the personal information of 100,000 or more consumers or, households" or "[d]erives 50 percent or more of its

[159] EPIC, *Privacy Impact Assessments* (2021), https://epic.org/issues/open-government/privacy-impact-assessments/.
[160] Civ. Code § 1798.199.40(d)

annual revenues from selling or sharing consumers' personal information."[161] Differentiating risk assessment requirements based solely on revenue would fail to account for such risks. Further, businesses can experience rapid growth: a successful app or platform may gross $300,000 one year and $30 million the next. Depending on the required frequency of and triggers for risk assessments, such growth could enable a business to escape meaningful accountability for its processing activities for many months after it has crossed the $25 million line.

To the extent that small businesses may fear added compliance costs from risk assessment requirements, it is important to note that the risk assessments for smaller-scale and lower-risk processing activities will generally be much less burdensome to complete (if they are required at all). But a small business that engages in large-scale, hazardous processing of personal information should not be able to do so without the careful evaluation and mitigation necessitated by a risk assessment. As we explain above: an organization that is too undercapitalized to adequately safeguard consumer data should simply not be permitted to process it.

[161] Civ. Code § 1798.140(d)(1).

V. Automated decisionmaking

The use of opaque, untested, and unproven automated decisionmaking systems has exploded across contexts such as hiring,[162] public benefits,[163] healthcare delivery,[164] insurance,[165] banking,[166] and student proctoring.[167] As set out above, these systems can cause bodily harm, loss of liberty, loss of opportunity, financial harms, dignitary harms, and discrimination harms.[168]

The CCPA as amended gives consumers the opportunity to bridge the gap between knowledge and disclosure. Notably, several aspects of the CCPA overlap with other laws and regulations coming into force, in particular the Colorado Privacy Act. Drawing on Colorado's

---

[162] *See, e.g.*, Dinah Wisenberg Brin, *Employers Embrace Artificial Intelligence for HR*, SHRM (Mar. 22, 2019), https://www.shrm.org/resourcesandtools/hr-topics/global-hr/pages/employers-embrace-artificial-intelligence-for-hr.aspx; Sheridan Wall & Hilke Schellmann, *LinkedIn's Job-Matching AI was Biased. The Company's Solution? More AI.*, MIT Tech. Rev. (Jun. 23, 2021), https://www.technologyreview.com/2021/06/23/1026825/linkedin-ai-bias-%20ziprecruiter-monster-artificial-intelligence; Monica Montesa, *AI Recruiting in 2023: The Definitive Guide*, Phenom (Mar. 14, 2023), https://www.phenom.com/blog/recruiting-ai-guide; QuantumBlack, McKinsey & Co., *The State of AI in 2022—and a Half Decade in Review* (Dec. 6, 2022), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review#/; Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, Wash. Post (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[163] *See, e.g.*, Arnauld Bertrand & Julie McQueen, *Why AI and the Public Sector are a Winning Formula*, Ernst & Young Global Ltd. (Oct. 21, 2020), https://www.ey.com/en_gl/government-public-sector/why-ai-and-the-public-sector-are-a-winning-formula; Grant Fergusson, *Public Benefits, Private Vendors: ow Private Companies Help Run our Welfare Programs*, EPIC (Jan. 26, 2023), https://epic.org/public-benefits-private-vendors-how-private-companies-help-run-our-welfare-programs/.

[164] *See, e.g.*, Liz Kwo, *Contributed: Top 10 Use Cases for AI in Healthcare*, Mobi Health News (Jul. 1, 2021), https://www.mobihealthnews.com/news/contributed-top-10-use-cases-ai-healthcare.

[165] *See, e.g.*, Insurance Europe, *AI in the Insurance Sector* (Nov. 2021), https://www.insuranceeurope.eu/publications/2608/artificial-intelligence-ai-in-the-insurance-sector/.

[166] *See, e.g.*, Eleni Digalaki, *The Impact of Artificial Intelligence in the Banking Sector & How AI is Being Used in 2022*, Bus. Insider (Feb. 2, 2022), https://www.businessinsider.com/ai-in-banking-report.

[167] *See e.g.*, Complaint and Request for Investigation, Injunction, and Other Relief, *In re Online Test Proctoring Companies* (Dec. 9, 2020), https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf.

[168] *See, e.g.*, EPIC FTC Comments on Commercial Surveillance, *supra* note 77; Rebecca Kelly Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 Yale J.L. & Tech 1, 51 (2021); *see also* Citron & Solove, *supra* note 10, at 855; Buolamwini & Gebru, *supra* note 62.

recently adopted regulations and other similar frameworks, we urge the Agency to ensure that consumers enjoy robust access and opt-out rights with respect to ADS.

a. Existing laws and frameworks

i. Current and anticipated laws

Responsive to question III.1

As key points of reference for its rulemaking, we would point the Agency to the Colorado Privacy Act,[169] the New York City Hiring Law,[170] and regulatory controls on predictive policing around the country.[171] Highlights of other relevant state laws include:

- Alabama Act 2022-420, which prohibits state and local law enforcement agencies (LEAs) from using facial recognition technology match results to establish probable cause in a criminal investigation or to make an arrest;
- Illinois Public Act 102-0047, which requires employers that rely solely on AI analysis of video interviews to determine whether an applicant will be selected for an in-person interview to collect and report demographic data about the race and ethnicity of applicants; and
- Vermont Act 132, which requires the Division of Artificial Intelligence to propose a state code of ethics on the use of artificial intelligence in state government, make recommendations to the General Assembly on policies, laws, and regulations of artificial intelligence in state government, and make annual recommendations and reports to the General Assembly on the use of artificial intelligence in state government and requires the Agency of Digital Services to conduct an inventory of automated decision systems developed, employed, or procured by state government.

[169] Colo. Rev. Stat. § 6-1-1301 *et seq.*
[170] N.Y. Local Law 144, Int. No. 1894-A (2021), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9.
[171] *See, e.g.*, Exec. Order No. 14,074, 87 Fed. Reg. 32,945 (2022).

Sectoral regulations are also under development by the Colorado Department of Insurance,[172] the California Civil Rights Council,[173] and the New York City Department of Consumer and Worker Protection[174] among others, and federal rulemakings are in progress at the Federal Trade Commission[175] and the Consumer Financial Protection Bureau.[176]

Notable overseas laws include the General Data Protection Regulation,[177] the European AI Act,[178] China's AI laws,[179] and India's potential AI regulations.[180]

ii. Other frameworks

Responsive to question III.1

There have been over 40 notable frameworks and guidance documents on the use of AI and automated decision-making systems published in recent years.[181] We highlight four in view of their

[172] Governance and Risk Management Framework Requirements for Life Insurance Carriers' Use of External Consumer Data and Information Sources, Algorithms, and Predictive Models, 3 Colo. Code Regs. § 702-4.
[173] Cal. Civ. Rts. Council, Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems, Cal. Code Regs. tit. 2, § 11008 *et seq.* (2022), https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2022/07/Attachment-G-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf.
[174] New York City Dep't of Consumer & Worker Prot., Text of Proposed Rule on Automated Employment Decision Tools (2023), https://rules.cityofnewyork.us/wp-content/uploads/2022/12/DCWP-NOH-AEDTs-1.pdf.
[175] FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).
[176] Consumer Fin. Prot. Bureau, *Consumer Financial Protection Circular 2022-03* (May 26, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.
[177] Commission Regulation (EU) 2016/679, 2016 O.J. (L 119) 1 (EU).
[178] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021).
[179] *See Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022,* Digichina (Jan. 10, 2022), https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.
[180] *See* Simon Sharwood, *India Teases AI Plan to 'Catalyse the Next Generation of the Internet,'* The Register (Mar. 8, 2023), https://www.theregister.com/2023/03/08/digital_india_bill_ai/.
[181] *Cf.* Jessica Fjeld et al., Berkman Klein Center for Internet & Society, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI* (2020), https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf.

comprehensiveness, their support by actors that have substantial influence, their focus on the individuals affected by automated systems, or the prominence of their authors.

A Blueprint for an AI Bill of Rights was released by the White House Office of Science and Technology Policy in January 2023.[182] It sets out five major principles: Safe and Effective Systems; Freedom from Algorithmic Discrimination; Data Privacy; Notice and Explanation; and Human Alternatives, Consideration, and Fallback[183]. The document lays out why these principles are critical, examples of how they are violated, and examples of how they have been implemented. The Blueprint notes that individuals must be protected from abusive data practices and calls for data minimization rules, stating: "You should be protected from violations of privacy through design choices that ensure such protections are included by default, including ensuring that data collection conforms to reasonable expectations and that only data strictly necessary for the specific context is collected."[184]

The AI Risk Management Framework by the National Institute of Standards and Technology ("NIST") was developed pursuant to the National AI Initiative Act.[185] NIST describes the document as a "[voluntary] resource [for] the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems."[186] Divided into four main aspects of AI lifecycles (Govern, Map, Measure, and Manage), the framework includes examples of how companies can adopt a more responsible approach to building and using AI tools. However, as the framework reminds readers, it is entirely nonbinding.

---

[182] White House Office of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights: Making Automaed Systems Work* (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[183] *Id.*
[184] *Id.*
[185] 15 U.S.C. § 9411 *et seq.*; *see also* Nat'l Inst. of Standards & Tech., *NIST AI 100-1: Artificial Intelligence Risk Management Framework* (AI RMF 1.0) (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[186] Nat'l Inst. of Standards & Tech., *supra* note 185.

The OECD AI Principles[19] were adopted in 2019 and endorsed by 42 countries—including the United States and the G20 nations. The OECD AI Principles establish international standards for AI use:

1. Inclusive growth, sustainable development and well-being.
2. Human-centered values and fairness.
3. Transparency and explainability.
4. Robustness, security and safety.
5. Accountability.[21]

The OECD also urges governments to ensure the development of "trustworthy AI" and to focus on "AI-related social, legal and ethical implications and policy issues." Governments are specifically urged to "review and adapt, as appropriate, their policy and regulatory frameworks and assessment mechanisms as they apply to AI systems to encourage innovation and competition for trustworthy AI." The OECD AI Principle on Transparency and Explainability states: "AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art: . . . to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation, or decision." "AI Actors" are defined as those "who play an active role in the AI system lifecycle, including organisations and individuals that deploy or operate AI."

The Universal Guidelines for Artificial Intelligence, a framework for AI governance based on the protection of human rights, were set out at the 2018 Public Voice meeting in Brussels, Belgium.[26] The Universal Guidelines for AI have been endorsed by more than 250 experts and 60 organizations in 40 countries. The UGAI comprise twelve principles:

1. Right to Transparency.
2. Right to Human Determination.
3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.

6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.[187]

Among the key principles, the UGAI states: "All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome" (Right to Transparency); "Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions" (Fairness Obligation); "An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system" (Assessment and Accountability Obligation); "Institutions must ensure the accuracy, reliability, and validity of decisions" (Accuracy, Reliability, and Validity Obligations); and "Institutions must establish data provenance and assure quality and relevance for the data input into algorithms" (Data Quality Obligation).

b. ADS access and opt-out rights

Responsive to question III.7

An opt-out allows users to avoid discrimination and other harmful consequences of an automated decisionmaking system by choosing not to be subject to it in the first place. To make this effective, the CPPA should require controllers to clearly explain the key parameters of each automated decisionmaking system, ensure that opting out of ADS is frictionless for the consumer, and establish strong protections to prevent discrimination based on opt-out status.

[187] The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/.

These safeguards should enable users to grasp the difference between how certain ADS systems work, but it will likely take time for the public to understand the contexts in which automated decisionmaking technology is used and which systems may result in discriminatory outcomes. A recent Pew Research Center study showed that, while only 15% of Americans are more excited than concerned about increased use of AI in daily life, less than a third of Americans surveyed could accurately identify six instances where AI is used in common everyday experiences.[188] These regulations should start to bridge that gap and incentivize businesses to be more responsible with data collection and ADS adoption, as they will be forced to disclose key information about their tools that may steer concerned users toward other products.

c. ADS disclosures

Responsive to question III.9

When developing rules as to how controllers must provide information about the logic of their automated decisionmaking systems, the Agency should be attentive to both the content and the format of disclosures to make them effective.

We urge the Agency to mandate, at minimum, that a business disclose the purpose of an automated decisionmaking system; what decision the tool is making or supporting; the factors the system relies on; a plain-language explanation of the logic of the system;[189] the sources and life cycle of the data processed by the system, including any brokers or other third-party sources; and how the system has been evaluated for accuracy and fairness, including links to any audits, validation studies, or impact assessments.

[188] Brian Kennedy, Alec Tyson, and Emily Saks, *Public Awareness of Artificial Intelligence in Everyday Activities*, Pew Research Center (Feb. 15, 2023), https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/.

[189] For example, in a predictive profiling system or automated decisionmaking system, the explanation should include data sources and how particular inputs affect determinations (e.g., if a criminal arrest in the last three years increases a "risk" classification by two points).

Further, it is critical that the disclosure not be buried only in the business's terms service or other equally hard-to-find location. It must be easily accessible ahead of the consumer's interaction with the system so that opt-out and access rights can be exercised *prior* to an automated decision being rendered.

The Agency should consider publishing model disclosures and display formats for websites and mobile applications—templates that would enable clear and seamless display of ADS information at the consumer's request without (for example) swamping consumers with popups that take over the screen. There is good language to this effect in the Colorado Privacy Act, which requires "A controller [to] provide consumers with a reasonably accessible, clear, and meaningful privacy notice"[190] and provide a "clear, conspicuous method … provided either directly or through a link, in a clear, conspicuous, and readily accessible location *outside the privacy notice*."[191]

VI. Conclusion

We thank the Agency for the opportunity to comment on its further forthcoming CCPA regulations and are eager to continue working with the CPPA to protect the privacy of all Californians.

Respectfully submitted,

Electronic Privacy Information Center
Center for Digital Democracy
Consumer Federation of America

[190] Colo. Rev. Stat. § 6-1-1308(a).
[191] 4 CCR 904-3 at § 4.03(b)(1)(a), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.

APPENDIX 1

New Baseline Expectations for Data Security: Consensus on Cybersecurity Hygiene for the Modern Threat Environment

Recommended Data Security Protocol	Non-Exhaustive List of Citations
Data minimization	• 16 C.F.R. pts. 314.4(c)(6), 682 • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(C)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(C)(i), (iv) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.13 (2022) • CIS Critical Security Controls 3.1, 3.4 • Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(f) (Oct. 24, 2022) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(a) (Oct. 31, 2022) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 34 (Apr. 16, 2018) • PCI-DSS Principal Requirement 3
Data mapping	• N.Y. Comp. Codes R. & Regs. tit. 23, § 500.3 (2022) • CIS Critical Security Controls 3.1, 3.2, 3.7, 3.8 • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 14 (Dec. 30, 2019) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(B) (N.D. Ga. Jul. 22, 2019) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(g) (Feb. 1, 2021) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 24 (Apr. 16, 2018) • FFIEC Cybersecurity Assessment Tools ver. 1.1 5-6, 28-29 (May 2017) • PCI-DSS Principal Requirement 1
Access controls	• 201 Mass. Code Regs. 17.04(1)(d,3), 17.04(2) (2010) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(vii) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.07 (2022) • FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023) (citing to 314.4(c)(1) of Safeguards Rule) • Final Rule, FTC, Standards for Safeguarding Customer Information, 86 Fed. Reg. 70286 (Dec. 9, 2021) (noting that "[s]uch overbroad access could create additional harm in the event of an intruder gaining access to a system by impersonating an employee or service provider")

	• CIS Critical Security Controls 3.3, 4.7, 5.1, 5.4, 5.5, 6.1, 6.2, 6.6, 6.8, 13.5 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(j) (3d Cir. 2015) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(a) (Oct. 31, 2022) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(d) (Dec. 30, 2019) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(D), 23(C) (N.D. Ga. Jul. 22, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(b) (D.D.C. Dec. 14, 2016) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(e) (Sept. 6, 2019) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(c) (Jan. 26, 2021) • Complaint at ¶ 13(c), In re Drizly, LLC, FTC File No. 2023185 (Oct. 24, 2022); • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(b) (Dec. 21, 2021) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(a) (Oct. 26, 2018) • CISA, Cross-Sector Cybersecurity Performance Goals 9 (2022) (control 1.5) • FINRA, Report on Cybersecurity Practices 17-20 (Feb 2015) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 7 (May 2022) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 29, 30 (Apr. 16, 2018) • FFIEC Cybersecurity Assessment Tools ver. 1.1 16-20, 26 (May 2017) • PCI-DSS Principal Requirement 7
Secure password practices	• 201 Mass. Code Regs. 17.04(1)(b),(c) (2010) • CIS Critical Security Controls 5.2 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(e)-(f) (3d Cir. 2015) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(b)(i), (iii), (vi) (D.D.C. Dec. 14, 2016) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(b)-(c) (Oct. 31, 2022) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(D) (N.D. Ga. Jul. 22, 2019) • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 11(c), (f) (Jun. 23, 2022)

	• Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(b),(c) (N.D. Cal. Mar. 20, 2017) • CISA, Cross-Sector Cybersecurity Performance Goals 8, 9, 10 (2022) (controls 1.2, 1.4, 1.6, 1.7) • FFIEC Cybersecurity Assessment Tools ver. 1.1 21 (May 2017) • PCI-DSS Principal Requirement 2
User authentication	• 201 Mass. Code Regs. 17.04(1) (2010) • N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.12 (2022) • FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023) (citing to 314.4(c)(5) of Safeguards Rule) • CIS Critical Security Control 6.3, 6.4, 6.5, 6.6, 12.7 • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 25 (Jun. 23, 2022) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(d) (Feb. 1, 2021) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(e) (Sept. 6, 2019) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(a)(iii), 24 (Oct. 26, 2018) • Complaint, In re Paypal, Inc., FTC File No. 1623102 at ¶ 40(c)(1) (May. 24, 2018) • CISA, Cross-Sector Cybersecurity Performance Goals 8 (2022) (control 1.3) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 30 (Apr. 16, 2018) • PCI-DSS Principal Requirement 8
Segmentation of systems	• CIS Critical Security Control 3.12, 4.4, 12.8 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(a), 28 (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(e) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(C)-(D), 23(B) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(e) (Dec. 30, 2019) • CISA, Cross-Sector Cybersecurity Performance Goals 22 (2022) (control 8.1) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 30 (Apr. 16, 2018)

	• Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4, at 39-40 (March 2022) (Requirement 1) • FFIEC Cybersecurity Assessment Tools ver. 1.1 8,16 (May 2017) • PCI-DSS Principal Requirement 10
Traffic monitoring	• 201 Mass. Code Regs. 17.04(4) (2010) • N.Y. Comp. Codes R. & Regs. Tit. 23, § 500.06 (2022) • 16 C.F.R. pt. 314.4(c)(8) • CIS Critical Security Control 13 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(h)-(i) (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(e) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(F), 23(A)(iii)-(iv), 23(C)(iii) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(f), 17 (Dec. 30, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(d) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 35 (D.D.C. Dec. 14, 2016) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(g) (Oct. 31, 2022) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(f) (Jan. 26, 2021) • CISA, Cross-Sector Cybersecurity Performance Goals 8 (2022) (control 1.1) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 36, 38-39 (Apr. 16, 2018) • FFIEC Cybersecurity Assessment Tools ver. 1.1 16, 25-26 (May 2017) • PCI-DSS Principal Requirement 10
Staying current on known vulnerabilities and ongoing security reviews (e.g. penetration testing)	• 201 Mass. Code Regs. 17.03(2)(h),(i), 17.04(6),(7) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(B)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(B) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.05 (2022) • 16 C.F.R. pts. 314.4(b)(2), 314.4(d), 314.4(g) • FTC Safeguards Rule: What Your Business Needs to Know, FTC, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 17, 2023) (“assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems”)

	• CIS Critical Security Control 7, 13.5, 18 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(d), 29 (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(b) (Feb. 1, 2021) • Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(A), 23(A) (N.D. Ga. Jul. 22, 2019) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(b) (Dec. 30, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 10,11(c)-(d) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(e) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(d) (Jan. 26, 2021) • Complaint, In re Residual Pumpkin Entity, LLC, d/b/a CafePress, FTC File No. 1923209 at ¶ 1(a), (d)-(e), (h) (Jun. 23, 2022) • Complaint, In re Paypal, Inc., FTC File No. 1623102 at ¶ 40(b) (May. 24, 2018) • Complaint, In re Drizly, LLC, FTC File No. 2023185 at ¶ 13(d)-(e) (Oct. 24, 2022) • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(c) (Dec. 21, 2021) • Complaint, FTC v. D-Link Corp., No. 3:17-CV-00039-JD at ¶ 15(a) (N.D. Cal. Mar. 20, 2017) • CISA, Cross-Sector Cybersecurity Performance Goals 17,18 (2022) (controls 5.1, 5.6) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 26, 33, 36, 39, 40, 43 (Apr. 16, 2018) • FINRA, Report on Cybersecurity Practices 21-22 (Feb 2015) • FFIEC Cybersecurity Assessment Tools ver. 1.1 6, 8, 24-28 (May 2017) • PCI-DSS Principal Requirement 5,6,11
Employee training	• 201 Mass. Code Regs. 17.03(2)(b)(1), 17.04(8) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(A)(4) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(iv) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.10, 500.14 (2022) • 16 C.F.R. pt. 314.4(e) • CIS Critical Security Control 14 • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(a) (Feb. 1, 2021)

	• Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 23(E) (N.D. Ga. Jul. 22, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(b) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(c) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 12(b) (Jan. 26, 2021) • Complaint, In re Chegg, Inc., FTC File No. 2023151 at ¶ 9(e) (Oct. 31, 2022) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(b) (Oct. 26, 2018) • CISA, Cross-Sector Cybersecurity Performance Goals 15 (2022) (controls 4.3, 4.4) • Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks, CISA (Aug. 25, 2020) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 31 (Apr. 16, 2018) • FINRA, Report on Cybersecurity Practices 31-32 (Feb 2015) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 10 (May 2022) • FFIEC Cybersecurity Assessment Tools ver. 1.1 11-12 (May 2017) • PCI-DSS Principal Requirement 5, 6, 9, 12
Heightened measures for high-risk activity (e.g. remote access, processing sensitive information, third-party integrations, etc.)	• 201 Mass. Code Regs. 17.03(2)(f) (2010) • N.Y. Gen. Bus. Law, § 899-bb(2)(b)(ii)(A)(6) (2020) • Or. Rev. Stat. tit. 50, § 646A.622(2)(d)(A)(vi) (2021) • N.Y. Comp. Codes R. & Regs. tit. 23, § 500.11, 500.12(b) (2022) • 16 C.F.R. pt. 314.4(f) • Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2021) (citing to 16 CFR 314.4(d), also citing to Kevin McCoy, Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers, USA Today (May 23, 2017)) • Complying with COPPA: Frequently Asked Questions, FTC L(1), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Mar. 17, 2023) (referring to § 312.8) • CIS Critical Security Controls 6.3, 6.4, 12.7, 15, 16 • First Am. Complaint, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 at ¶ 24(j) (3d Cir. 2015) • Complaint, In re Zoom Video Communications, Inc., FTC File No. 1923167 at ¶ 12(c) (Feb. 1, 2021)

	• Complaint, FTC v. Equifax, Inc., No. 1:2019-cv-03297 at ¶ 22(E),23(D) (N.D. Ga. Jul. 22, 2019) • Complaint, In re LightYear Dealer Technologies, LLC, FTC File No. 1723051 at ¶ 11(b) (Sept. 6, 2019) • Complaint, FTC v. Ruby Life Inc. d/b/a AshleyMadison.com, No. 1:16-cv-02438 at ¶ 31(d) (D.D.C. Dec. 14, 2016) • Complaint, In re SkyMed International, Inc., FTC File No. 1923140 at ¶ 13 (Jan. 26, 2021) • Complaint, In re Uber Technologies, Inc., FTC File No. 1523054 at ¶ 18(d), 20 (Oct. 26, 2018) • Complaint, In re InfoTrax Systems, L.C., FTC File No. 1623130 at ¶ 10(g) (Dec. 30, 2019) • Complaint, In re Support King, LLC, FTC File No. 1923003 at ¶ 17(a), (e) (Dec. 21, 2021) • Complaint, In re Lenovo, Inc., FTC File No. 1523134 at ¶ 24 (Jan. 2, 2018) • Complaint, In re Ascension Data & Analytics, LLC, FTC File No. 1923126 at ¶¶ 13, 14–17, 20 (2021) • Complaint, In re TaxSlayer, LLC, FTC File No. 1623063 at ¶ 14(d) (2017) • CISA, Cross-Sector Cybersecurity Performance Goals 14, 19 (2022) (controls 3.4, 6.1, 6.2, 6.3) • NIST, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 28, 29, 39 (Apr. 16, 2018) • FINRA, Report on Cybersecurity Practices 26-30 (Feb 2015) • FINRA, Core Cybersecurity Threats and Effective Controls for Small Firms 6-7 (May 2022) • FFIEC Cybersecurity Assessment Tools ver. 1.1 17,20,28-32 (May 2017) • PCI-DSS Principal Requirement 2, 3, 7, 8 • Karen Scarfone, Security Concerns with Remote Access, https://csrc.nist.gov/CSRC/media/Events/HIPAA-Security-Rule-Implementation-and-Assurance/documents/NIST_Remote_Access.pdf (last visited Mar. 17, 2023) • Kristin Cohen, Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law against Illegal Use and Sharing of Highly Sensitive Data FTC Bus. Blog (July 11, 2022) • ABA Cybersecurity Legal Task Force, Vendor Contracting Project: Cybersecurity Checklist Second Edition 1 (2021)