CLASS Network — Consumer Law Advocates, Scholars & Students

A project of the UC Berkeley Center for Consumer Law & Economic Justice + the National Association of Consumer Advocates

February 18, 2025

Submitted via email

California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834

Re: Public Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies Regulations

Comment of the Consumer Law Advocates, Scholars, and Students (CLASS) Network

Dear Members of the California Privacy Protection Agency Board:

The nationwide Consumer Law Advocates, Scholars & Students (CLASS) Network submits this comment in response to the California Consumer Privacy Protection Agency's request for public comments on its proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies.[1]

Spearheaded by the UC Berkeley Center for Consumer & Economic Justice and the National Association of Consumer Advocates, the CLASS Network is a nationwide initiative dedicated to developing consumer law and economic justice curriculum, experiential opportunities, and coordinated projects at law schools around the country. Our network comprises law students, professors, and advocates at 15+ law schools with student consumer law organizations, as well as 15 law school clinics that provide clinical experience in consumer law and economic justice. Each CLASS chapter holds events and participates in pro bono research and advocacy projects with partner government agencies and non-profit organizations. Public comments submitted by the CLASS Network and its chapters have been relied on in recent rulemakings by the Federal Trade Commission and federal Consumer Financial Protection

[1] Cal. Code Regs., tit. 10, § 7001 *et seq.* (proposed). All further regulatory references are to title 10 of the California Code of Regulations unless otherwise specified.

Bureau. Through its work, the CLASS Network seeks to foster the next generation of advocates for consumers and engage law students in critical issues of economic justice, including the impact of emerging technologies on consumer protection and privacy. This comment presents the contributions of 32 students at 7 CLASS-affiliated schools.

The CLASS Network writes to express its support for the California Consumer Privacy Protection Agency's proposed Rule—specifically, Articles 9 and 11 addressing cybersecurity audits and automated decisionmaking technologies (ADMT).[2] This comment explains the basis of that support and offers examples of data breaches and ADMTs from multiple industries to illustrate the signal importance of this rulemaking. We also offer the following recommendations for the Agency to ensure strong and robust state guidelines on cybersecurity audits and use of ADMTs in the marketplace and workplace:

- Cybersecurity audits should be performed by fully independent auditors and rooted in nationally recognized cybersecurity standards, much like financial audits.
- Cybersecurity audits should result in the tabulation and disclosure of numerical key performance indicators for the most common classes of cybersecurity failures.
- Consumers should be shown clear, up-front disclosures concerning the use of ADMTs and their rights concerning such use before being asked to enter any personal information into a system that incorporates ADMTs.
- Consumers should be given the unconditional right to opt out of having ADMTs process their personal information, either for decisionmaking or model training.
- Companies that deploy ADMTs should be required to perform ongoing parity testing to ensure that ADMTs are not producing disparate outcomes from the human decisionmaking processes they are supposed to replicate.

We also explain why, in our view, the proposed Rule falls within the Agency's remit to protect the personal privacy of Californians.

Finally, Appendices A and B adduce examples that we have identified of egregious data breaches and deceptive ADMTs in multiple industries affecting California consumers and workers. As outlined in the examples in Appendix A, California consumers and workers have had their private personal information, including sensitive information, exposed and stolen in harmful data breaches that exploited vulnerabilities at a variety of private businesses. Routine and thorough cybersecurity audits, like those required by the proposed Rule, would help prevent and mitigate data breaches, as we describe for each example. Separately, as demonstrated by the examples in Appendix B, California consumers and workers are vulnerable to deception and bias

[2] We do not offer any views on the remaining provisions of the proposed Rule.

from ADMTs in an assortment of industries. We strongly agree with the breadth of the proposed Rule as well suited to addressing ADMTs of all kinds.

We thank the Commission for its work in producing a broad and urgently needed Rule to protect the almost 40 million workers, consumers, and residents of California – and many millions more in other jurisdictions -- from the risks inherent in these emerging technologies.

I. THE PROPOSED RULE TAKES ON THE PERVASIVE DATA INSECURITY THAT IS PLAUGING CONSUMERS AND WORKERS.

For the past two decades, data breaches involving personally identifiable information (PII) have been steadily increasing in number, size, and severity.[3] In the first half of 2024 alone, several of the biggest U.S. companies—including AT&T, UnitedHealth, and Ticketmaster, among many others—were severely compromised, resulting in the exposure of over 1 billion unique records.[4] A single breach of the massive data broker National Public Data in August of 2024 may have exposed as many as 2.9 billion additional records, with the attackers boasting that they had obtained social security numbers for "the entire [U.S.] population."[5]

Despite the enormity of these figures, they represent a tiny fraction of the tens of thousands of breaches affecting tens of billions of records over the past two decades.[6] An industry survey found that "84% of respondents said their organization has experienced an identity-related breach" between June 2021 and June 2022, "with 78% citing direct business impact as a result."[7] Although many policy proposals have addressed this problem, the "data suggests that companies and government regulators' attempts to squash the… cyberattacks plaguing organizations have hardly made a dent."[8] The sheer size of the problem, and the paucity of comprehensive regulatory and compliance solutions to address it, demonstrates the need for a more comprehensive and stringent legal regime.

---

[3] *See generally* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022); *see also* STATISTA, *Annual number of data compromises and individuals impacted in the United States from 2005 to 2023*, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[4] Zack Whittaker, *The Biggest Data Breaches in 2024: 1 Billion Stolen Records and Rising*, TECHCRUNCH (Aug. 12, 2024), https://techcrunch.com/2024/08/12/2024-in-data-breaches-1-billion-stolen-records-and-rising/.

[5] Lily Hay Newman, *The Slow-Burn Nightmare of the National Public Data Breach,* WIRED (Aug. 16, 2024), https://www.wired.com/story/national-public-data-breach-leak/.

[6] *See* STATISTA, *supra* note 3. *See also* Vilius Petkauskas, *Mother of all breaches reveals 26 billion records: what we know so far*, CYBERNEWS (Jan. 29, 2024), https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/.

[7] IDENTITY DEFINED SECURITY ALLIANCE, *New Study Reveals 84% of Organizations Experienced an Identity-Related Breach in the Last Year*, (Jun. 22, 2022), https://www.idsalliance.org/press-release/new-study-reveals-84-of-organizations-experienced-an-identity-related-breach-in-the-last-year/.

[8] Sam Sabin, *2023 toll of data breaches and leaks already tops 2022*, AXIOS (Oct. 13, 2023), https://www.axios.com/2023/10/13/2023-data-compromises-surpass-2022.

A. Data Breaches of Consumer Data Routinely Harm California Consumers and Workers.

The loss and theft of private information inflicts enormous damage. The usual consequence of data breach is identity theft: a criminal actor uses a consumer's stolen PII to open new financial accounts or access existing ones, empties them, and then disappears.[9] Approximately one in four victims of data breach will suffer identity theft in the subsequent 12 months—over 9 times the incidence of identity theft experienced by members of the general population.[10] On a per capita basis, California's share of the aggregate annual cost of identity theft exceeds $2 billion.[11] Similarly, California's annual per capita share of credit card fraud, much of which can be traced to data breaches, may exceed $3 billion.[12]

Consumers and employees have minimal ability to protect their personal information from theft by a third-party, and little support for managing the fallout once a breach inevitably happens. Trying to limit the sharing of one's PII is both onerous and futile: many breaches involve subcontractors, data aggregators, credit bureaus, and other companies to whom consumers never voluntarily entrust any PII at all.[13] And once a breach does happen—now a near certainty for companies that handle PII[14]—the fallout can be devastating for consumers. A third of respondents to a recent survey of identity theft victims "reported losses between $100-$500… [and] 15% reported financial losses greater than $1,000."[15] Another survey reported an "average

---

[9] See MONEY, *What is Identity Theft, and How Does it Happen?*, https://money.com/what-is-identity-theft/.
[10] Erika Harrell, *Just the Stats: Data Breach Notifications and Identity Theft, 2021*, BUR. JUST. STAT., U.S. DEP'T JUST., (Jan 2024), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021; Stu Sjouwerman , *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4 (March 7, 2013) https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (showing a similar ratio in 2013).
[11] The total U.S. population is approximately 341 million, and the population of California is approximately 39 million, or 11.44% of that total. See U.S. CENSUS BUR., *U.S. and World Population Clock*, https://www.census.gov/popclock/**.** The aggregate annual cost of identity theft across the U.S. is approximately $20 billion, and 11.44% of that total is $2.3 billion. *See* JAVELIN STRATEGY, *2022 Identity Fraud & Scams Report* (Mar. 29, 2022), https://javelinstrategy.com/2022-Identity-fraud-scams-report.
[12] Credit card fraud totaled $32 billion dollars in 2021, having nearly doubled since 2014. *See* John Egan, *Credit card fraud statistics*, BANKRATE (Jan. 12, 2023), https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/#fraud. 11.44% of $32 billion in 2021, which has nearly doubled since 2014). See U.S. Census Bur., supra note 11.
[13] *See, e.g.,* Corey Fedde, *Consumers wary of Experian's credit monitoring service after data breach*, CHRISTIAN SCI. MONITOR (Oct. 2, 2015), https://www.csmonitor.com/Technology/2015/1002/Consumers-wary-of-Experian-s-credit-monitoring-service-after-data-breach (describing how 15 million T-Mobile customers had their "addresses, birthdates, personal information, and Social Security numbers" exposed in a "security breach of credit reporting agency Experian, which T-Mobile uses to run credit checks on potential customers").
[14] Keman Huang, Xiaoqing Wang, William Wei, & Stuart Madnick, *The Devastating Business Impacts of a Cyber Breach*, HARVARD BUS. R. (May 04, 2023), https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach (reporting that "83% of organizations experienced more than one data breach during 2022").
[15] Rob Lever, *U.S. News & World Report Identity Theft Survey 2023*, U.S. NEWS & WORLD REP., https://www.usnews.com/360-reviews/privacy/identity-theft-protection/identity-theft-fraud-survey.

per-victim loss from traditional identity fraud… [of] $1,551."[16] Unexpected expenses of this magnitude would pose a significant hardship to most consumers—a majority of whom would have difficulty covering a $500 emergency charge.[17]

B. Proposed Article 9 Contains a Well-Crafted Requirement for Regular Cybersecurity Auditing, but Should Also Require the Use of Specific Metrics, Standards, and Objective Tests for Auditor Independence.

The proposed Rule's requirement that all covered businesses conduct regular cybersecurity assessments is an essential first step in reducing the risk of data compromise—but that mandate would be both more rigorous and easier to implement if it were rooted existing nationally-recognized standards sets. There are approximately a dozen robust cybersecurity standard sets promulgated by reputable industry consortiums and government agencies, and audits based on these frameworks can be quite thorough.[18] Unfortunately, many commercially-available cybersecurity assessment services are not based on any of those standards. Instead, a cottage industry of cybersecurity firms offer a motley assortment of automated scans, antivirus products (many of which contain devastating vulnerabilities of their own[19]), and educational materials, most of which look broadly similar but are difficult to directly compare.[20] Some so-called security assessment services offer no more than performative box-checking, are entirely automated, or are based wholly on self-assessment.[21] Given this landscape, it is no surprise that "both providers and clients are dissatisfied by the lack of transparency and consistency in

---

[16] *See* Kenneth Terrel, *Identity Fraud Hit 42 Million People in 2021*, AARP (Apr. 7, 2022), https://www.aarp.org/money/scams-fraud/info-2022/javelin-report.html (reporting that as of September 2023, 63% of Americans reported being "unable to cover a $500 emergency expense").
[17] *See id.*
[18] *See* Paul Kirvan, *Top 12 IT security frameworks and standards explained*, TECHTARGET (Oct. 27, 2023) https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one; *see also* Andrew Plato, *How to Get a Meaningful Security Assessment,* ANITAN (Aug. 18, 2013) ("A good assessor does not just know a security standard, like HIPAA or PCI, but understands the intent of those standards and how they relate to the overall context of an information security program.")
[19] *See* Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NAT'L PUB. RADIO (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (describing the historic breach of a nominally security-enhancing administrative platform used by as many as 18,000 of the largest institutions in the United States, including multiple U.S. government agencies. Notably, SolarWinds hawked its platform as security-enhancing, and continues to do so to this day. *See* SOLARWINDS, *Introducing Secure By Design*, https://www.solarwinds.com/secure-by-design-resources).
[20] See Tony Pepper, *Is the cyber security industry selling snake oil?,* EGRESS (Oct. 18, 2022) https://www.egress.com/blog/security-and-email-security/cybersecurity-hype-how-to-manage-expectations-vs-reality-2022 (reporting that companies looking for reputable cybersecurity assessment services must navigate "a crowded and noisy marketplace… filled with category creation and consolidation, product and feature launches, and buzzwords and acronyms," and that as a result "91% of [surveyed] decision-makers found it difficult to select cybersecurity vendors due to unclear marketing about their specific offerings").
[21] *See id.* (observing that "the cyber security industry is frequently guilty of selling snake oil").

[cybersecurity] industry offerings."[22] The solution to this "wide variation" is clear: "standardi[z]ation is needed."[23]

Although the Agency has articulated a robust list of cybersecurity considerations within this draft Rule, to promote further standardization and facilitate compliance the Agency should expressly encourage covered businesses to seek out cybersecurity services rooted in nationally recognized standards sets. Covered businesses trying to make sense of widely variable security assessment offerings would greatly benefit from having a list of standards sets that are broadly compatible with the Agency's priorities. Because the more mature security assessment vendors already offer assessment services rooted in these standards sets, publishing a list of Agency-approved standards sets would make it much easier for covered businesses to identify high-quality assessment vendors whose outputs will satisfy the Agency's requirements. Examples of well-regarded standards sets that the Agency might choose to endorse include:

- NIST 800-53
- SOC-2
- ISO / IEC 27001 + 27002
- CIS CF
- COBIT
- HITRUST CSF
- PCI-DSS

In future rulemaking, the Agency might consider implementing a program whereby security assessment vendors can become certified to offer CPPA-compliance services. But for now, both the Agency and covered businesses will benefit greatly by using vendor support for existing standards sets to distinguish the more reputable security assessment vendors from the less so.

C. Section 7122 Rightly Requires Audits to be Conducted by an Independent Auditor—Either Internal or External to the Organization—But an Internal Auditor Can Never Be Fully Independent.

The proposed requirement that all covered businesses conduct regular, independent cybersecurity audits provides a strong foundation for robust cybersecurity, but the current

---

[22] *See* William Knowles, Alistair Baron & Tim McGarr, *The simulated security assessment ecosystem: Does penetration testing need standardisation?,* 62 COMP. & SECURITY 296 (2016), https://www.sciencedirect.com/science/article/pii/S0167404816300906 (summarizing complaints from industry that "the quality [of security assessment services] varies immensely … the quality can be atrocious").

[23] *Id. See also* Henry J. Sienkiewicz, *Independence & Objectivity: Fundamental Best Practices for Cybersecurity Assessments*, U.S. CYBERSECURITY MAGAZINE (Spring 2017), https://www.uscybersecurity.net/csmag/independence-objectivity-fundamental-best-practices-for-cybersecurity-assessments/ ("the nascent field of cyber assessment can learn from the financial industry… as with financial audits, cybersecurity assessments need to be presented in a framework that is understood and accepted.").

language permits conflicts of interest that can be easily prevented. Specifically, the proposed Rule's allowance that "the auditor may be internal or external to the business" undermines the mandate's otherwise strong endorsement of auditor independence.[24] As the Agency's draft language recognizes, allowing businesses to delegate audits to parties who have vested interests in obtaining clean audits is likely to skew the results.[25] For this reason, while many of the aforementioned cybersecurity standards bodies encourage self-assessment as the *starting* point for compliance, most of them require that final certification audits be performed by external firms.[26] Accordingly, to ensure that the audit mandate does not promote compliance in name only, the following language should be added to section 7122: **"The auditor must be fully independent, neither party to nor controlled by any party to any past or current relationship with the business apart from the provision of security auditing services."**

The Agency makes clear in the draft language that it appreciates the risk that conflicts of interest pose to meaningful auditing, and CLASS wholeheartedly endorses the Agency's careful work to reduce such risk. The language of Section 7122 exhibits a deep understanding of the potential conflicts of interest that can affect even external auditors. In support of this vigilance, CLASS wishes to highlight that many smaller companies outsource their information technology support services to third-party vendors known as Managed Service Providers or (specialized) Managed Security Service Providers (collectively, MSPs).[27] Businesses typically delegate to their MSPs broad responsibility for all aspects of IT operations, and hold their MSPs primarily responsible for maintaining organizational security and compliance—including any associated failures.[28] Particularly severe deficiencies or disruptions may be deemed grounds for terminating support contracts, the news of which can spread rapidly to other MSP customers.[29] Accordingly, the viability of an MSP's core business operations is directly tied to its reputation for protecting its clients from adverse cybersecurity incidents, including compliance failures and bad audit

---

[24] CPPA Proposed Text of Regulations (Nov. 22, 2024) § 7122(a)(1).
[25] *See id.* (specifying that "the auditor must not participate in the business activities that the auditor may assess in the current or subsequent cybersecurity audits").
[26] *See, e.g.,* Richard Rieben, *Understanding the HITRUST CSF: A Guide for Beginners*, Linford & Co LLP (Mar. 15, 2023), https://linfordco.com/blog/hitrust-csf-framework/ (explaining that self-assessment is an initial step in achieving HITRUST CSF certification, but "organizations are required to use an authorized HITRUST assessor firm to conduct the assessment" that ultimately determines their compliance).
[27] *See* GARTNER GLOSSARY, *Managed Service Provider (MSP)*, https://www.gartner.com/en/information-technology/glossary/msp-management-service-provider.
[28] *See* TuxCare PR Team, *Working as an MSP for Your Clients? You're Responsible for Compliance Too*, TUXCARE BLOG (Apr, 24, 2023), https://tuxcare.com/blog/working-as-an-msp-for-your-clients-youre-responsible-for-compliance-too/ (repeatedly emphasizing that "as a trusted technology partner, MSPs have another important role too: ensuring their customer's systems are compliant with sector-specific and broader compliance laws"; "MSPs are responsible for ensuring that their clients' systems are compliant with applicable regulations"; and "when the cybersecurity buck stops at the MSP (or indeed MSSP) it means that the compliance buck also stops with the MSP.").
[29] *See* Sam Stanton, *Prominent Sacramento law firm sues for $1 million after falling prey to ransomware attack,* SACRAMENTO BEE (Feb. 29, 2024), https://www.sacbee.com/news/local/article286031606.html; *see also Mastagni Holstedt, A.P.C., v. LanTech, LLC.*, 24 CV 003400, Superior Court of California, Sacramento.

results.[30] Nevertheless, many companies frequently expect their MSPs to handle all compliance testing and certification for them: as of 2021 "34 percent of businesses outsource at least part of their compliance needs," and since then the MSP industry has only further embraced the competitive advantages of adding "compliance-as-a-service" contracts to their offerings.[31] But responsible MSPs have significant reservations about such bundling:

> Our explanation for not providing [cybersecurity auditing] along with [our] security solution is simple: As an MSSP provider, testing the system that we put in place and manage creates a conflict. Imagine the IRS allowing your accounting team to perform their own audit instead of doing it themselves or hiring an outside, unbiased third party. It's kind of like letting the fox guard the hen house. Even if it's a well fed, honest and well-mannered fox, it just doesn't look good.[32]

The same principle applies to internal auditors. It would be both unreasonable and unfair to require an employee whose job depends on her organization maintaining a clear cybersecurity bill of health to zealously seek out deficiencies that might divert scarce resources, invite regulatory scrutiny, or frustrate her leadership. Partly for this reason, research has found that internal audits "alone cannot mitigate the probability of a cyber attack" or other adverse cybersecurity outcome.[33] Thus, it is imperative that the final version of Section 7122 eliminate this source of potential conflicts of interest by requiring audits to be performed by parties that are *fully* independent of the organization.

---

[30] *See* Michael Nelson, *Compliance and Security Risks in MSP Outsourcing – How To Resolve?*, SCALE YOUR MSP (Aug. 28, 2024) https://scaleyourmsp.com/blog/compliance-and-security-risks-in-msp-outsourcing-how-to-resolve/ (encouraging businesses shopping for MSPs to "Assess the vendor's history with regulatory compliance" and "Obtain references from other clients, particularly those in similar industries. Review case studies to understand how the vendor has addressed security and compliance challenges in the past."); *see also* CYDEF, *4 Hurdles Facing MSPs When a Client is Breached*, https://cydef.io/4-hurdles-facing-msps-when-a-client-is-breached/ ("When a client suffers, the MSP suffers too. They don't need to be directed impacted by the attack; when a client churns, that also can cause business failure.").

[31] *See* Jenn Fulmer, *What MSPs Need to Know to Offer Compliance Services*, CHANNEL INSIDER (Aug. 4, 2022), https://www.channelinsider.com/managed-services/msps-compliance-services/ ("adding compliance services may give you the edge you need. Manufacturing, financial services, healthcare, and government entities, just to name a few, all have specific regulations they have to follow, and there simply aren't enough qualified compliance specialists available to serve them all. Instead, these organizations are turning to MSPs to fulfill this need which could, in turn, set you up for major success.").

[32] Thinkguard Blog, *When Penetration Testing Creates "Bad Optics*" (Jan 24, 2022), https://www.thinkgard.com/blog/when-penetration-testing-creates-bad-optics.

[33] Sergeja Slapničar, Tina Vuko , Marko Čular, Matej Drašček, *Effectiveness of cybersecurity audit*, 44 INT'L J. OF ACCT. INFO. SYS. 100548 (March 2022) https://www.sciencedirect.com/science/article/pii/S1467089521000506 (questioning whether internal auditing can ever provide the requisite level of independence required to produce accurate findings).

D. Section 7123 Provides an Impressively Comprehensive List of Factors for Audits to Assess, but Should More Clearly Require the Collection and Disclosure to the Agency of Specific Key Performance Metrics.

While the proposed audit requirement covers many important dimensions of cybersecurity, it currently does not expressly require the collection of numerical key performance indicators, and such collection is unlikely to happen without such a mandate. The National Institute of Standards and Time (NIST), one of the leading cybersecurity standards-setting bodies, specifies that "meaningful security metrics are necessary to quantitatively evaluate and measure the operational effectiveness and system performance of a network."[34] Despite this clear directive, the cybersecurity auditing industry does not generally have an established best practice of collecting such data; to the contrary, "existing [cybersecurity assessment] methods have suffered from… [the] lack of quantitative metrics and measures for comprehensive security assessment… limitations that reduce their usefulness and effectiveness."[35] Numerical audit data are essential because while narrative descriptions of an organization's posture can be easily massaged to hide risks, hard metrics are much less susceptible to manipulation (short of overt deceit). Accordingly, Section 7152 of the proposed Rule should include a requirement that cybersecurity audits collect numeric key performance indicator data wherever possible, and at the very least for the following metrics:

- Percent and number of organizational devices missing two or more critical software updates
- Percent and number of organizational devices protected by full disk encryption
- Percent and number of staff who have completed annual security training
- Number of software systems for which single user accounts are being shared by multiple people

Additionally, Section 7157 should require that these key metrics be included in all risk assessment submissions to the Agency. The inclusion of these metrics will enhance accountability, allow the Agency to identify and track the most common sources of organizational risk, and facilitate the development of targeted resources to address the most prevalent classes of vulnerabilities.

---

[34] Yi Cheng, Julia Deng, Jason Li, Scott DeLoach, Anoop Singhal, Xinming Ou, *Metrics of Security, Cyber Defense and Situational Awareness*, 917850 NAT'L INST. STANDARDS & TIME PUB. 27 (Dec 15, 2014), https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917850.
[35] *Id*. at 8.

II. THE PROPOSED RULE ENACTS VITAL SAFEGUARDS FOR AUTOMATED DECISONMAKING TECHNOLOGIES, BUT MORE MUST BE DONE.

ADMTs are often celebrated for their supposed efficiency, ability to accurately synthesize vast amounts of information, and immunity to biases and stereotypes—but ADMTs are neither infallible nor objective.[36] To the contrary, ADMTs operate strictly within the confines of pre-determined associations and fail to incorporate the nuanced complexities of human experiences and ethical considerations critical to sound decisonmaking.[37] By disregarding these vital elements, ADMTs risk perpetuating biases, reinforcing inequalities, and undermining the progress they are supposedly designed to advance.[38] The proposed Regulations offer careful and well-crafted guidance to address these potential harmful outcomes, but would benefit from additional requirements that ADMT implementers proactively monitor for algorithmically-perpetuated bias.

A. ADMT Products Present Significant Problems for California Consumers and Workers.

Automated decisonmaking technology (ADMT) products are highly prone to reinforcing existing biases, making harmful errors, and obscuring the mechanics of their decisonmaking processes in a way that makes it difficult to identify and redress wrongful decisions. Accordingly, ADMTs can pose significant risks to California's workers and consumers. ADMTs are increasingly deployed across critical sectors in California and across the nation, including housing, employment, education, healthcare, financial services, and criminal justice.[39] When

---

[36] The popular view that ADMTs are superior to human decisonmaking draws from arguments explored in legal scholarship. One perspective, known as the "Awful Human Argument," suggests that human decisonmaking is inherently flawed, advocating for the superiority of machine-based decisions. Another, the "Better Together Argument," proposes that ADMTs can enhance human decisonmaking processes. These arguments urge a shift toward automated decisonmaking systems believed to outperform human-only methods. *See* Daniel J. Solove & Hideyuki Matsumi, "AI, Algorithms, and Awful Humans," *Fordham Law Review*, vol. 92, no. 5, art. 8, 2024.

[37] See Emilio Ferrara, *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies*" 6 *Sci* 3 (2004) https://doi.org/10.3390/sci6010003 ("In the realm of generative AI, addressing bias is even more challenging as it requires a holistic strategy. This begins with the pre-processing of data to ensure diversity and representativeness. This involves the deliberate collection and inclusion of varied data sources that reflect the breadth of human experience, thus preventing the overrepresentation of any single demographic in training datasets. Model selection must then prioritize algorithms that are transparent and capable of detecting when they are generating biased outputs.")

[38] *See id.* ("these powerful computational tools, if not diligently designed and audited, have the potential to perpetuate and even amplify existing biases, particularly those related to race, gender, and other societal constructs").

[39] For example, the use of ADMTs to expedite hiring is widespread: 70% of companies and 99% of Fortune 500 companies now use automated tools in their hiring processes. Companies argue that these tools promote efficiency, since hundreds of applicants apply to each open position, and ADMTs can help quickly cull unqualified candidates. *See* Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired*, ACLU News & Commentary (Aug. 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-

ADMTs are used without sufficient guardrails, workers may unfairly lose employment opportunities,[40] renters may be wrongly denied housing,[41] and marginalized groups may be subject to even more systemic discrimination,[42] among other harms. To mitigate these risks, any proposed regulation must expressly grant consumers and workers the ability to opt out of and obtain information about the use of ADMTs and provide robust protections against retaliation for doing so.

Using ADMTs to make "significant decisions" can increase rather than decrease deception, unfairness, and inequity.[43] Although algorithms are frequently touted as more objective than human decisionmakers, often the opposite is true: ADMTs can entrench and exacerbate existing societal biases.[44] Bias can enter ADMTs at many stages. For example, if a tool is built using on datasets that contains biases—as much real-world data does—the algorithm will faithfully reproduce the racial, gender, and other disparities present in the training data.[45] ADMTs can be designed to intentionally discriminate, or may have discriminatory impact

---

prevent-you-from-getting-hired; ReNika Moore, Testimony, *Navigating Employment Discrimination in AI and Automated Systems: A New Civil Rights Frontier*, U.S. EEOC (Jan. 31, 2023), https://www.eeoc.gov/meetings/meeting-january-31-2023-navigating-employment-discrimination-ai-and-automated-systems-new/moore. *See also* Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn 44 (Dec. 10, 2018), https://www.upturn.org/work/help-wanted

[40] *See, e.g.*, Rachel V. See & Annette Tyman, *Mobley v. Workday: Court Holds AI Service Providers Could Be Directly Liable for Employment Discrimination Under "Agent" Theory*, Seyfarth Legal Update, (Jul. 19, 2024), https://www.lexology.com/library/detail.aspx?g=dc00c0f2-40e0-4e87-a6e1-e41111206850. *See also* Joseph B. Fuller, et al., *Hidden Workers: Untapped Talent*, Harv. Bus. Sch. & Accenture 20, (Oct. 4, 2021), https://www.hbs.edu/managing-the-future-of-work/Documents/research/hiddenworkers09032021.pdf.

[41] *See, e.g.,* Gary Rhoades, *Ghosts in the Machine: How Past and Present Biases Haunt Algorithmic Tenant Screening Systems*, 49 Human Rights 13 (2024); *Louis v. Saferent Sols.*, 685 F. Supp. 3d 19 (D. Mass. 2023); *Arnold v. Saferent Sols.*, 2024 WL 4555386 at *1 (E.D. Mich. Oct. 23, 2024) (slip op.); Echols v. Saferent Sols., 2022 WL 4970312 at *1 (D. Ariz. Oct. 4, 2022). *See also Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols*., 2023 WL 4669482 at *1 (D. Conn. July 20, 2023) (about another tenant screening product, CrimSAFE).

[42] *See, e.g.*, Crystal Grant, *Algorithms Are Making Decisions About Health Care, Which May Only Worsen Medical Racism*, ACLU NEWS & COMMENTARY (Oct. 3, 2022), https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism.

[43] *See* Cal. Code Regs., tit. 11, § 7200(a)(1) (proposed) (defining "significant decision" as "a decision that [unless exempt] . . . results in access to, or the provision or denial of financial or lending services; housing; insurance; education enrollment or opportunity; criminal justice; employment or independent contracting opportunities or compensation; healthcare services; or essential goods or services").

[44] *See generally* Ashwini K.P., *Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance*, U.N. Doc. A/HRC/56/68 (July 2024); Cathy O'Neill, *Weapons of Math Destruction* (2016). *See also CFPB and Federal Partners Confirm Automated Systems and Advanced Technology Not an Excuse for Lawbreaking Behavior*, CFPB NEWSROOM (Apr. 25, 2023) (ADMTs can "automate discrimination," according to FTC Chair Lina Khan); Tim O'Brien, *Compounding Injustice: The Cascading Effect of Algorithmic Bias in Risk Assessments*, 13 GEO. J. L. & MOD. CRITICAL RACE PERSP. 39, 56–57 (2021) (describing the ways that gender, racial, and other biases are replicated and entrenched by algorithms).

[45] *See* Julia Busiek, *Three Fixed for AI's Bias Problem*, U.C. NEWS (Mar. 21, 2024), https://www.universityofcalifornia.edu/news/three-fixes-ais-bias-problem (explaining the data-science principle of "garbage in, garbage out"—i.e., biased input data produces biased outcomes); Molly Griffard, *A Bias-Free Predictive Policing Tool?: An Evaluation of the NYPD's Patternizr*, 47 FORDHAM URB. L.J. 43, 49–50 (2019) (describing how "algorithms are prone to reproduc[ing] biases in the data sets on which the algorithms are trained"). While socioeconomic status is not a protected classification under California or federal law, algorithms reinforce socioeconomic disparities as well.

despite their creators' or users' intentions.[46] Moreover, regardless of the quality of the substantive data ADMTs are fed, their decisonmaking processes can also be independently fallible. ADMTs frequently make significant mistakes—applying assumptions derived from common scenarios to uncommon situations in nonsensical ways, or wholly making up facts—and those errors can have tremendous impacts on consumers.[47] Consumers may be wrongfully accused of crimes, or lose access to housing, employment, insurance, and other basic necessities.[48] ADMTs used in housing, hiring, and educational access applications can unfairly screen out candidates; evidence shows that people from already-marginalized groups, such as people of color, disabled people, LGTBQ+ people, and low-income people, are disproportionately screened out by these tools.[49] And because of the "black-box" nature of many ADMTs, it is frequently impossible to identify the factors that contribute to any given adverse decision, leaving consumers without clear recourse against biased or factually-baseless decisions.[50] Finally, although the elimination of human discretion and its potential bias is often seen as a benefit of ADMTs, in many instances humans can perform more nuanced and sophisticated analysis than ADMTs can—and human oversight is thus an essential component of any responsible ADMT deployment.[51]

---

[46] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 674–75 (2016) (explaining how algorithms can discriminate unintentionally or be programed to discriminate intentionally); Ben Shneiderman, *Opinion, The Dangers of Faulty, Biased, or Malicious Algorithms Requires Independent Oversight*, 113 PNAS 13538, 13538 (2016) (discussing malicious and unintentionally harmful algorithms).

[47] See IBM, *What are AI hallucinations?* (Sept. 1, 2023), https://www.ibm.com/think/topics/ai-hallucinations (noting that "making sure a human being is validating and reviewing AI outputs is a final backstop measure to prevent hallucination").

[48] *See, e.g.*, Carrie Kirby, *When Algorithms Harm Us*, U. IOWA COLL. OF L. (Nov. 30, 2022), https://law.uiowa.edu/iowa-law-magazine/news/2022/11/when-algorithms-harm-us (describing instances of wrongful arrest and of misidentification as a white nationalist, both due to algorithmic error); Grant, *supra* note 42 (explaining that medical algorithm errors leading to worse care for Black patients).

[49] *See* Zhisheng Chen, *Ethics and Discrimination in Artificial Intelligence-Enabled Recruitment Practices*, 10 Humanities and Social Sciences Communications 1, 1 (Sept. 13, 2023) (examining algorithmic bias that results in discriminatory hiring practices); Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, THE MARKUP (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms ("The quality of the data you're putting into the underwriting algorithm is crucial"); Chad Marlow et al., *Digital Dystopia: the Danger in Buying What the EdTech Surveillance Industry is Selling* at 8–10, ACLU (2023) (discussing harms of school surveillance technology).

[50] *See* Varun Bhatnagar, *The Evidentiary Implications of Interpreting Black-box Algorithms*, 20 Nw. J. of L. & Intellectual Property 433, 433–434 (2023) (explaining the potential harms of black-box algorithms); Carmen Cheung, *Making Sense of the Black Box: Algorithms and Accountability*, 64 CRIM. L. Q. 539, 545 (2017) (explaining that even "knowing the inputs [to an algorithm] provides limited insight if the process of analysis remains inaccessible"). *See also CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms*, CFPB NEWSROOM (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms (discussing the risks to consumers of black-box algorithms).

[51] *See* LEXISNEXIS, *Generative AI: The importance of human oversight in the law*, https://www.lexisnexis.co.uk/insights/generative-ai-the-importance-of-human-oversight-in-the-law/index.html, ("Human oversight also mitigates other prominent AI risk. It can minimize the introduction of bias through simple steps. It can ensure inputs are carefully curated and of a much higher quality, while simultaneously ensuring

The risks associated with adoption of ADMTs, which can cause significant harm in nearly any sector, include: (1) the risk of ADMTs replicating preexisting societal biases; (2) the risk of factual fabrication or analytic error; (3) the difficulty of identifying and correcting such problems due to the "black box" design of ADMT algorithms making it difficult or impossible to explain how any given decision was reached; (4) the tension between the faults of human bias and the benefits of human discretion; and (5) the practical concerns consumers may have about opting out of ADMT use. Each of these risks is addressed in turn below.

1. ADMTs Replicate Existing Biases, Thereby Entrenching Discrimination.

When the underlying data on which a model is trained encodes existing societal biases, the model is likely to replicate those biases in its output.[52] For example, Amazon's 2018 recruiting tool was scrapped because of its systematic bias against women candidates.[53] Using historic data trends of resumes submitted and candidates hired from the past ten years, Amazon's tool taught itself that male candidates were preferable.[54] Attempts to tweak the algorithm to eliminate this bias were unsuccessful, and the tool was ultimately abandoned.[55] This problem is well-known and pervasive across ADMT applications[56] and presents significant threats to California consumers and workers, especially those belonging to already marginalized groups. In the criminal justice context, facial recognition and reoffending probability assessment algorithms lead to baseless accusations, racial profiling, and discriminatory legal outcomes.[57]

---

effective data governance. It can make sure outputs are more accurate, more reliable, free from hallucinations, and more up-to-date. In short, human oversight drastically improves the results of the AI and boosts user trust.").

[52] *See* Chen, *supra* note 9, at 1 (examining algorithmic bias that results in discriminatory hiring practices); Martinez & Kirchner, *supra* note 9 ("The quality of the data you're putting into the underwriting algorithm is crucial").

[53] Jeffrey Dastin, *Insight—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-idUSKCN1MK08G.

[54] *Id.*

[55] *Id.*

[56] Cheung, *supra* note 50, at 542 ("That pre-existing biases or mistakes in input data can skew outputs is well-known.").

[57] Facial recognition technology, utilized by law enforcement, exhibits substantial biases that disproportionately affect individuals with darker skin tones. A study by the National Institute of Standards and Technology (NIST) found that these technologies are more likely to produce false positives among these groups, potentially leading to unjust arrests or convictions. Additionally, an ACLU test of Amazon's "Rekognition" software highlighted its inaccuracies by incorrectly matching 28 members of Congress with criminal mugshots, illustrating the risk across diverse political and demographic lines. These examples underscore the urgent need for standards to manage biases in AI systems effectively. *See*, *e.g.*, Reva Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, Natl'l Inst. Standards & Technol. Spec. Publ'n. 1270, (Mar. 2022), https://doi.org/10.6028/NIST.SP.1270; *See also* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28*, ACLU OF N. CAL. (Jul. 26, 2018), https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28; Alexandra Taylor, *AI Prediction Tools Claim to Alleviate a Crowded American Justice System… But Should They Be Used?*, Stanford Politics (Sept. 13, 2020), https://stanfordpolitics.org/2020/09/13/ai-prediction-tools-claim-to-alleviate-an-overcrowded-american-justice-system-but-should-they-be-used.

2. ADMTs Are Often Opaque, Which Makes Tracing Bias and Error Difficult.

Even when consumers know that a decision affecting their rights was mistaken, they may not know if or how an algorithm was involved in the decision. And even when the use of ADMTs is clearly disclosed, tracing how an algorithm arrived at a particular decision is often extremely difficult.[58] Because ADMTs are both extremely complicated and generally proprietary, it is often difficult to tell what factors led to an adverse decision for a consumer or worker.[59] Opacity can derive from companies' unwillingness to disclose the details of their algorithms, or from actual properties of the model that make their results unexplainable.[60] In either case, individual consumers and workers are left powerless to address adverse outcomes that are biased or based on faulty logic or incorrect facts, and companies cannot be held accountable for making repeated or systematic mistakes.

3. ADMTs Make Harmful Errors.

Despite the popular belief that computers are infallibly rational, ADMTs can and do make mistakes.[61] When ADMTs are applied to "significant decisions,"[62] those errors can have especially serious consequences. Numerous pending cases against one tenant-screening platform allege that incorrect decisions based on data errors resulted in people being wrongfully denied access to housing.[63] An ongoing class action alleges that an AI tool incorrectly denied medically necessary insurance claims.[64] A healthcare-risk prediction algorithm allegedly incorporated incorrect metrics, leading to harmful outcomes for some patients.[65] A criminal risk-assessment scoring tool that has been used in California and other states for sentencing was found to incorrectly label Black defendants as future criminals at almost twice the rate of white

---

[58] *Id.* at 545 (explaining the problems consumers face in understanding algorithmic decisions).
[59] *Id.* (noting that privacy, trade secrets, and fairness concerns may counsel against revealing the details of algorithms); Kaven Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, CONSUMER REPORTS (Mar. 11, 2021), https://www.consumerreports.org/electronics/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/ (explaining details of adverse decisions are often available for traditional screenings but not algorithmic screenings).
[60] Lou Blouin, *AI's Mysterious 'Black Box' Problem, Explained*, UNIV. MICH. DEARBORN NEWS (Mar. 6, 2023), https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained (describing unexplainable algorithms).
[61] *See, e.g.,* Mikaël Chelli et. al., Hallucination Rates and Reference Accuracy of ChatGPT and Bard for Systematic Reviews: Comparative Analysis, J. MED. INTERNET RES. 2024 May 22:26:e53164. doi: 10.2196/53164. (finding the rates at which leading generative AI tools fabricated false information to be "39.6% (55/139) for GPT-3.5, 28.6% (34/119) for GPT-4, and 91.4% (95/104) for Bard (P<.001)",
[62] 47-Z Cal. Regulatory Notice Reg. 1494, 1502.
[63] *See* Rhoades, *supra* note 41.
[64] *See* Ian Lopez, *Humana's Alleged Use of AI to Deny Claims Draws Class Action*, BLOOMBERG L. (Dec. 12, 2023), https://www.bloomberglaw.com/bloomberglawnews/health-law-and-business/X3ATVO9K000000?bna_news_filter=health-law-and-business#jcite (discussing the ongoing *Barrows v. Humana* litigation).
[65] *See* Grant, *supra* note 42; Zaid Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCIENCE 447, 447 (2019).

defendants.[66] And a recently-filed class action lawsuit alleges that Cigna Corporation used an algorithm to automatically deny payments for treatments that did not meet specific preset criteria, circumventing the legally-required individual physician review process.[67]

The COVID-19 pandemic ushered in a new era of remote work and education, forcing numerous industries to implement new digital tools to increase efficiency.[68] Student monitoring tools like Gaggle, GoGuardian, and Bark incorporate automated flagging tools that search students' online activity and flag content related to sex, drugs, and violence. Such tools disproportionately flag already-marginalized students—particularly students of color, students with disabilities, and LGTBQ+ students—subjecting them to increased scrutiny and disciplinary actions.[69]

4. Human Discretion Can Solve Problems and Counteract Bias.

Though proponents of ADMTs often argue that computerized decisonmaking is preferable to human decisonmaking because it eliminates human bias,[70] the reality is far more complicated.[71] For example, using ADMTs in hiring often benefits candidates who most closely resemble the job posting, and prevents a more holistic analysis of a candidate's experience and abilities that a human could make.[72] Hiring ADMTs thus exclude from consideration viable

---

[66] *See* Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016); *see also* Cheung, *supra* note 50, at 544 ("[T]he potential for false positives [from COMPAS] is not trivial.").
[67] *See Kisting-Leung et al. v. Cigna Corp.,* No. 2:23-cv-01477 (E.D. Cal. filed Dec. 3, 2024), https://litigationtracker.law.georgetown.edu/wp-content/uploads/2023/08/Kisting-Leung_20230724_COMPLAINT.pdf.
[68] Elizabeth Laird et al., *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI*, CTR. FOR DEMOCRACY & TECH. (Sep. 2023), https://cdt.org/wp-content/uploads/2023/09/091923-CDT-Off-Task-web.pdf (discussing how school districts have exponentially increased the use of online surveillance tools to monitor student engagement).
[69] According to a Center for Democracy and Technology (CDT) nationwide survey of the usage of school safety technology largely driven by AI, many of these school surveillance tools produce false positives, which can lead to students experiencing excessive, unsubstantiated disciplinary action or interaction with law enforcement. Jason Kelley, *Student Monitoring Tools Should Not Flag LGTBQ+ Keywords*, ELEC. FRONTIER FOUND. (Jun. 22, 2023), https://www.eff.org/deeplinks/2023/06/student-monitoring-tools-should-not-flag-lgbtq-keywords; https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/; Marlow, *supra* note 9, at 8-10; Todd Feathers, *Takeaways From Our Investigation Into Wisconsin's Racially Inequitable Dropout Algorithm*, MARKUP (Apr. 27, 2023), https://themarkup.org/the-breakdown/2023/04/27/takeaways-from-our-investigation-into-wisconsins-racially-inequitable-dropout-algorithm (describing AI tool that uses race and socioeconomic status to generate student drop-out predictions).
[70] *See, e.g.*, COMPUT. & COMMC'NS INDUS. ASS'N, *Preliminary Comment Letter on Proposed Rulemaking on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations* at 16 (Mar. 27, 2023), https://cppa.ca.gov/regulations/pdf/rm2_pre_comments_1_26.pdf#page=365.
[71] *See, e.g.*, Philip Gaborden & Eva Rosen, *How Do Landlords' Screening Processes Discriminate Against Tenants?*, HOUS. SOL. LAB (June 25, 2024), https://localhousingsolutions.org/how-do-landlords-screening-processes-discriminate-against-tenants/ (explaining how neither algorithmic nor human screening is enough to fix societal inequality because of biases inherent in each).
[72] *See generally* ReNika Moore, Testimony, *Navigating Employment Discrimination in AI and Automated Systems: A New Civil Rights Frontier*, U.S. EEOC (Jan. 31, 2023),

candidates whose resumes do not match the specific criteria of a job posting, but who could excel after some basic training.[73] The same principle applies to many other contexts in which ADMTs are already being used. In one case, a criminal risk-assessment algorithm would have set a teenage defendant's bail at $25,000—but a judge used his discretion to set it at $2,500 instead, allowing the teen to post bail and be released. (He was ultimately acquitted).[74] Tenant-screening algorithms have shown similar blind spots, summarily rejecting qualified applicants on the basis of incorrect and outdated data—often disproportionally along racial lines.[75] In some of these contexts, the use of ADMTs can cause enormous harm even if human review ultimately catches an error; indeed, false criminal accusations made by algorithms have already caused severe and irreversible injury.[76] Because human decisonmaking can pick up on factors and nuances that ADMTs cannot, it is vital that ADMTs not be allowed to make consequential decisions without human oversight.[77]

5. Consumers And Workers May Face Retaliation for Opting Out of ADMTs.

Although the Proposed Rule expressly provides that consumers and workers must have the right to opt out of ADMT processes[78] and prohibits retaliation against anyone who exercises that right,[79] consumers have ample reason to worry that their chances of obtaining a job, home, or fair criminal sentence will be harmed by opting out. In New York, where job-seekers have the right to opt out of automated application screening, a 2024 study showed that opting out essentially destroys a candidate's chance of even making it to the next stage of review.[80]

Automated decisonmaking tools are increasingly deemed necessary for efficiency and functionality across sectors. Given that ADMTs *will* be used and *will* affect consumers and workers, the Rule must address issues of bias in algorithmic tools and issues of consumers' informed consent when engaging with platforms that use these tools. We are especially

---

https://www.eeoc.gov/meetings/meeting-january-31-2023-navigating-employment-discrimination-ai-and-automated-systems-new/moore. *See also* Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN 44 (Dec. 10, 2018), https://www.upturn.org/work/help-wanted.

[73] Fuller, *supra* note 40.

[74] O'Brien, *supra* note 44, at 41.

[75] See Nadiyah J. Humber, A Home for Digital Equity: Algorithmic Redlining and Property Technology, 111 CAL. L. REV. 1421, 1425-26 (2023).

[76] See Elaisha Stokes, *Wrongful arrest exposes racial bias in facial recognition technology*, CBS NEWS (Nov. 19, 2020), https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/ (recounting the wrongful arrest of Michael Oliver, solely on the basis of an erroneous match made by a facial-recognition tool commonly used by law enforcement, resulting in him losing his job, car, and home because of his lengthy pre-trial incarceration).

[77] *See* LEXISNEXIS, *supra* note 51.

[78] 47-Z Cal. Regulatory Notice Reg. 1494, 1498.

[79] *Id.* at 1496.

[80] Te-Ping Chen, *Your Résumé Might Be Getting Tossed by AI. How to Push Back*, WALL ST. J. (Feb. 20, 2024), https://www.wsj.com/lifestyle/careers/if-humans-wont-read-your-resume-should-you-let-the-robot-72bb641c.

concerned about the practical consequences of consumers' and workers' choice to opt out of ADMT technology absent clear protections against resulting discrimination.[81] Although Article 7 of the Notice of Proposed Rulemaking and California Civil Code Section 1798.125 includes anti-retaliation provisions, stakeholders have pointed out that opting out meaningfully can be prohibitively difficult.[82] For example, some companies use third party platforms with their own proprietary AI tools that screen or rank applicants, and thus feed data into multiple layers of ADMTs from which applicants would have to opt-out individually. The CPPA should therefore clarify how liability works under the new Rule when companies process consumer data using third-party tools that themselves incorporate ADMTs.[83]

B. There are Significant Opportunities to Strengthen the Proposed Rule to Better Protect Consumer Rights.

1. Greater Alignment with the GDPR would Enhance Consumer Protections while Making Compliance with the Proposed Rule Less Burdensome.

The proposed Rule generally aligns well with the requirements of the GDPR, but eliminating remaining discrepancies would both better protect consumers and make the implementation of the Rule less burdensome for affected companies. The CCPA and the GDPR both establish comprehensive data protection regimes, in contrast to the more sector-specific approaches used in U.S. federal laws such as the Health Insurance Portability & Accountability Act (HIPAA) and the Fair Credit Reporting Act (FCRA).[84] Both the CCPA and the GDPR require transparency regarding how personal data are handled and the right to view any such data a company holds about a party. However, key discrepancies remain between the GDPR and the proposed Rule that will make compliance with both regulatory schemes more onerous for the many companies that do business in both jurisdictions—unless the frameworks are reconciled. Given that the GDPR's implementing rules are already finalized, the best way to eliminate these burdens would be to align the proposed Rule with the GDPR with respect to the assurance of basic consumer rights of access and appeal, opt-in consent, and heightened protections for the processing of sensitive data.

---

[81] California Civ. Code § 1798.125 (prohibiting retaliation against an employee, applicant for employment, or independent contractor, in response to a consumer opting-out or exercising other rights).
[82] 47-Z Cal. Regulatory Notice Reg. 1494, 1498; California Civ. Code § 1798.125 (West 2018) (prohibiting retaliation against an employee, applicant for employment, or independent contractor, in response to a consumer opting-out or exercising other rights).
[83] *See* Brief for Attorneys for EEOC as Amicus Curiae Supporting Plaintiff, *Mobley v. Workday, Inc*., 2024 US Dist LEXIS 126336, [ND Cal July 12, 2024, No. 23-cv-00770-RFL]).
[84] *See* Daniel Solove & Paul Schwartz, INFO. PRIVACY L. 33, 844 (8th Edition 2023); Peter Swire & DeBrae Kennedy-Mayo, U.S. Private-Sector Privacy L. and Practice for Info. Privacy Prof'ls, 139 (4th Edition 2024).

Both the CCPA and the GDPR require any company that does significant business in their respective jurisdictions to comply with their rules—and the globalized nature of the contemporary business landscape means that a significant number of companies are subject to both frameworks.[85] Both frameworks have broad extraterritoriality clauses requiring corporations to comply with all of their terms regardless of where the corporations are located.[86] Given that the GDPR's requirements apply to any company that handles the date of any E.U. citizen, most large companies already have GDPR compliance programs in place and thus will be well positioned to comply with new rules that align with those pre-existing standards.[87] Accordingly, the best way to reduce the implementation burden associated with the Agency's proposed Rule would be to align it to the greatest extent possible with existing GDPR standards, thus allowing many companies to achieve compliance by making only minor tweaks to their pre-existing GDPR compliance frameworks. The following substantive recommendations are partly informed by this broad goal.

2. Require clear, plain-language disclosures about all ADMT uses, decisions, and consumer rights, and make those rights more absolute.

The proposed Rule enacts a strong foundational requirement that ADMT implementers respect and prominently advertise certain key consumer rights—but those rights are not as extensive or absolute as they could be. Section 7220 requires consumers to be given a "Pre-Use notice" whenever an ADMT will be used to process their data, describing the logic and "key parameters" of the ADMT and the "specific purpose" for which it is being used.[88] In theory, this Notice must explain how consumers can access a detailed explanation of any ADMT decision concerning them,[89] appeal any such decision to a human arbitrator,[90] and opt-out of ADMT use altogether[91]—but all of these rights are subject to extensive exceptions that make them all effectively optional.[92] In particular, no company is required to provide a right to appeal an ADMT verdict to a human arbitrator, but companies that do are excused from having to provide an opt-out right. [93] Similarly, the right to access the ADMT outputs for a particular consumer is not available if an ADMT is used "solely for training," even though consumers' data are still

---

[85] https://biztechmagazine.com/article/2021/03/gdpr-and-ccpa-businesses-must-comply-both-and-theyre-not-same (arguing that "Virtually All U.S. Businesses Must Comply With These Laws," as "Most firms do business across these state and international boundaries, and [both] regulators assert their ability to protect the personal information of their residents worldwide.")
[86] See Cal. Civil Code, §1798.140 (d); see also Claes G. Granmar, *Global applicability of the GDPR in context*, 11 INT'L DATA PRIVACY L., 225, 226 (2012).
[87] *See Future of Privacy Forum Report on Comparing Privacy laws: GDPR v. CCPA*, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf; Solove & Schwartz, *supra* note 85, at 849.
[88] Cal. Code Regs., tit. 10, § 7220(c)(5), (1) (proposed) (Nov. 22, 2024).
[89] Cal. Code Regs., tit. 10, § 7222 (proposed) (Nov. 22, 2024).
[90] Cal. Code Regs., tit. 10, § 7220(c)(2)(A) (proposed) (Nov. 22, 2024).
[91] Cal. Code Regs., tit. 10, § 7221 (proposed) (Nov. 22, 2024).
[92] Cal. Code Regs., tit. 10, § 7220(c)(2)-(3) (proposed) (Nov. 22, 2024).
[93] Cal. Code Regs., tit. 10, §7221(b)(2)(A) (proposed) (Nov. 22, 2024).

being processed by and permanently incorporated into an ADMT.[94] By contrast, Article 22 of the GDPR provides considerably more robust protections, including a requirement for affirmative *opt-in* consent for ADMT use, an absolute right to appeal adverse decisions issued by ADMTs to human arbitrators, and an unconditional right to detailed explanation of any algorithmically-generated decision. [95]

The proposed rule expressly acknowledges the dangers of discrimination and erroneous decisions that may accompany the use of ADMTs, but leaves consumers defenseless against such risks by failing to unconditionally guarantee the rights of access, appeal, and refusal.[96] Such protections are vital to providing recourse for the (inevitable) errors that algorithms will make, to advancing the stated intent of Article 11, and to minimizing compliance burdens by preventing companies from having to implement largely-redundant compliance programs for the CPPA and GDPR. Making these consumer rights unconditional would better advance the stated objective of Article 11 (to foster innovation by adopting efficient technology while also providing consumers with more controls and rights) and better align the proposed Rule with the GDPR.[97]

Additionally, any information provided to consumers must be readily understandable. Currently, proposed § 7222(b) includes a requirement that all output from access requests be furnished in "plain language." Likewise, the pre-use notice obligated in proposed § 7220 also must be written in "plain language." However, principles of "plain language" can vary widely. For example, a twelve-page long Terms of Service document written at an 8th-grade reading level might facially satisfy that requirement—but if the description of important consumer rights is buried at the bottom of pages eight and nine, its "plainness" will do very little to increase consumer awareness.[98]

CLASS recommends that the Agency incorporate a concrete, explicit definition of "plain language" to ensure that the required disclosures are fully accessible, and meaningfully increase consumer awareness of their rights. Such a requirement already exists in the Civil Code, but is currently-narrowly scoped to products that handle genetic information. We recommend that the Agency replicate the disclosure standard of Cal Civ. Code Section 56.18(a)(6):

> clear, meaningful, and prominent notice regarding the collection, use, maintenance, or disclosure of [personal information processed by ADMTs] for a specific purpose. The nature of the data collection, use, maintenance, or disclosure shall be conveyed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand it."

---

[94] Cal. Code Regs., tit. 10, §7220(c)(3)(A) (proposed) (Nov. 22, 2024).
[95] Gabriela Zanfir-Fortuna, *The EU General Data Protection Regulation: A Commentary*, 416 (2020).
[96] CPPA Initial Statement of Reasons, Article 10 p.60-62
[97] CPPA Initial Statement of Reasons, Article 11 p.80-81.
[98] *See Gerber v. Twitter*, N.D. Cal. 4:23-cv-00186-KAW (finding Twitter's terms of service "at least somewhat procedurally unconscionable," despite the terms at issue appearing under a "bolded header in 30-point font", as "the these terms were buried in lengthy forms drafted by the party who wished to enforce them").

Finally, on the broad theme of disclosures, CLASS would like to point out the speciousness of the primary criticism of the right to access ADMT outputs that appears in responses to the Agency's Invitation for Preliminary Comments (concerning potential violation of trade secrets).[99] The only information the proposed Rule requires is the specific output of an ADMT with respect to a particular party's personal information. Because the outputs of ADMTs that process personal information will be highly contingent on each individual's data, these outputs are highly unlikely to have independent economic value, which is a key element of the definition of a trade secret under both the UTSA §1(4) and California law.[100] While disclosure of the algorithm used for the ADMT technology could potentially bestow such an advantage, the proposed rule avoids this problem by requiring the disclosure of only individualized ADMT outputs. Moreover, the CCPA expressly provides for the protection of trade secrets in all of the Agency's activities, and nothing about the proposed Rule reduces those pre-existing protections.[101]

3. Either adopt an opt-in consent scheme for the use of ADMTs to process consumer information or strengthen the opt-out right to allow consumers to prevent any of their sensitive information from being ingested into an algorithm.

Optimally, the proposed Rule would adopt a universal requirement for opt-in consumer consent for the use of ADMTs to process their personal information, waivable only in cases of legal necessity. Article 22 of the GDPR allows the use of solely automated decisonmaking technologies only if the data subject has provided express consent or if the technology is necessary for the performance of a contract or authorized by EU or member state law.[102] In relation to express consent the GDPR requires consumers to opt in to the use of ADMT and express their unambiguous consent.[103] By contrast, the current proposed Rule only provides a qualified right to opt out of ADMT processing—and exempts from this requirement any ADMT data processing for security and prevention of fraud; for admission, hiring, allocation of work and compensation; or for work and educational profiling, provided the technology is necessary for those purposes and has been subjected to an evaluation and accuracy and non-discrimination standards.[104] The extensive exceptions to the proposed Rule's opt-out right compromise choice and thereby run afoul of the stated purpose of Article 11: providing more control to

---

[99] *See, e.g.*, Comments of the Association of National Advertisers, p.5; Comments of the CTIA, p.32; Comments of the SIA p.5.
[100] Elizabeth A. Rowe and Sharon K. Sandeen, Trade Secret Law: Cases and Materials, 147 (3d edition 2020); see also Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231,1233 (N.D. Cal. 1995) (holding that a trade secret must "provide[] an actual or potential advantage over others who do not possess the information").
[101] *See* Cal. Civil Code, § 1798.140(f).
[102] WP29 Guidelines for ADM and Profiling § IV (E)p.25
[103] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 §§ 81,93
[104] Cal. Code Regs., tit. 10, § 7222(c)(5)(a) (proposed) (Nov. 22, 2024).

consumers.[105] The GDPR's approach is both in better alignment with the spirit of Article 11 and more efficient than requiring companies to create an entirely new opt-out mechanism where compliant opt-in mechanisms already exist.

Even if the proposed Rule cannot implement a fully opt-in model, it can and should adopt such an approach for the ADMT processing of highly sensitive information, the protection of which is essential both to consumer privacy and international data sharing agreements. Limiting the processing of sensitive personal data in circumstances where opt-in consent is not provided is one of the supplemental principles of the US-EU Data Privacy Framework.[106] Accordingly, minimizing the processing of sensitive personal information is essential to maintaining data sharing between the EU and California—vital economic exchange that could be interrupted if the proposed Rule deviate too far from the GDPR standards.

Regardless of whether consumers opt in or out to exercise their ADMT rights, those rights should be more precisely and comprehensively defined. In particular, the Rule should allow consumers to opt out of both having ADMTs used to make decisions about them *and* having their personal information used to train ADMTs.[107] If consumers are not allowed to opt-out of companies' use of consumer data to train ADMTs, their information is at risk of misuse and improper disclosure, potentially in perpetuity. Generative AI tools have already proven capable of divulging highly sensitive data present in their training material.[108] Even nominally anonymized data has proven to re-identifiable in some cases.[109] Consumers should have the absolute right to opt out of such risks. The Agency should also provide guidance concerning what non-ADMT alternatives a company can or must offer consumers that opt out, which will likely look quite different across sectors.[110]

Some companies, including staffing agencies, have noted in the preliminary comments that offering an opt-out option wherein a human decisionmaker screens an application rather than an ADMT negates the very purpose of using an ADMT in the first place—i.e., to increase the efficiency of initial screening processes. This argument does not outweigh the harms to consumers that ADMTs may impose and does not negate the importance of the right to opt out.

---

[105] CPPA Initial Statement of Reasons, Article 11 p.78
[106] *See* https://www.dataprivacyframework.gov/framework-article/1–Sensitive-Data
[107] *C.f.* Cal. Code Regs., tit. 10, §7220(c)(3)(A) (proposed) (Nov. 22, 2024) (permitting companies to use consumer data for model training purposes without providing an opt-out option).
[108] *See* Joachim Bartels, *Generative Artificial Intelligence Models May Leak Private Data*, BUS. INFO. INDUS. ASS'N (Mar. 10, 2024), https://www.biia.com/generative-artificial-intelligence-models-leak-private-data/ (reporting that researchers were able to "obtain names, phone numbers, and addresses of individuals and companies by feeding ChatGPT absurd commands that forced a malfunction").
[109] *See* Isha Maranthe, *With AI Training, Data 'Anonymization' Runs Risk of Becoming a Fig Leaf*, LAW TECH. NEWS (Mar. 19, 2024), https://www.law.com/legaltechnews/2024/03/19/with-ai-training-data-anonymization-runs-risk-of-becoming-a-fig-leaf (explaining that generative AI is designed to predict attributes based on other related attributes, and thus excels at adding back in attributes that have been stripped from datasets for privacy reasons).
[110] *See, e.g.,* American Staffing Agency, *Preliminary Comment Letter on Proposed Rulemaking on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations* at 346 (Mar. 27, 2023) https://cppa.ca.gov/regulations/pdf/rm2_pre_comments_1_26.pdf#page=344.

4. ADMTs must be monitored on an ongoing basis to ensure that they are not deviating from the human decisonmaking processes they are supposed to be emulating.

To ensure that ADMTs are not injecting bias, enacting discrimination, or otherwise failing to faithfully follow their operating instructions, ADMTs must be subject to continuous parity testing with human decisionmakers—and disengaged as soon as they start diverging from expected performance. One parity-testing approach that would address multiple aforementioned concerns at once would be to compare the decisions made across demographically-similar cohorts of those screened by ADMTs and those that opt out.[111] This approach would both protect those who opt-out from systemic retaliation and help to confirm that ADMTs are approximating the performance of human decisionmakers.

D. The Agency Appropriately Exercised Its Statutory Authority to Issue the Proposed ADMT Regulations.

The proposed Rule is consistent with both the letter and spirit of California law, which delegates to the Agency broad authority and discretion to issue regulations to protect and enhance the privacy rights of California consumers.[112] This broad delegation has been repeatedly recognized and endorsed by state appellate courts.[113] Furthermore, the Legislature specifically charged the Agency with issuing "regulations governing access and opt-out rights with respect to a business' use of automated decisonmaking technology."[114] The Legislature thus acted within the scope of its authority (which is plenary, and thus goes far beyond the U.S. Congress's enumerated powers), to delegate to the Agency the specific authority to regulate ADMTs, along with broad discretion to decide how to best manage the technology's inherent complexities.[115]

More specifically, requiring businesses to provide consumers with a pre-use notice that defines and clearly explains both the right to know when and how ADMTs are being used and

---

[111] *See* Joy Ebertz, *Parity Testing with Feature Flags*, SPLIT BY HARNESS BLOG, Jan. 26, 2023 ("Feature Parity Testing, sometimes referred to as TAP compare testing, ensures a new system behaves the same as an old one. It is used when replacing part or all of an old system with a new one. At a high level, you mirror your traffic to both systems and compare the results, logging any that are different.").
[112] *See* Cal. Civ. Code § 1798.10(a) ("vest[ing] [the Agency] with full administrative power, authority, and jurisdiction to implement and enforce" whatever regulations the Agency deems appropriate to advance the CPPA's legislative intent).
[113] *See, e.g., Cal. Privacy Prot. Agency v. Superior Court*, 99 Cal. App. 5th 705 (2024) (confirming that the CCPA vested the CPPA "with the authority to administer, implement, and enforce the CCPA through administrative and civil actions.").
[114] Cal. Civ. Code § 1798.185(a)(15).
[115] *See* Article XIV section 4, California Constitution; *see also* David A. Carillo & Danny Y. Chou, *California Constitutional Law: Separation of Powers*, 45 SAN FRANCISCO L. REV. 655, 656 (2022) (explaining that "state governments, by contrast [to the federal government], have plenary power, limited only by the federal supremacy clause and by individual rights otherwise protected in the state constitution. These fundamental differences [include] the greater power of the state government to regulate the lives of its citizens.").

the right to opt out of such uses fall directly under the plain meaning of the authorizing statute concerning "access and opt-out rights."[116] The statute specifies that the relevant regulations under this provision may:

> [I]nclud[e] profiling and requiring a business' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.[117]

The proposed Rule's requirement that businesses provide a general description of the process they use to verify a consumer's request to access ADMT was thus expressly anticipated and authorized by the Legislature, which expressly mandated that businesses provide meaningful information about their decisionmaking processes to affected consumers.[118]

The fact that other consumer rights in the CCPA are mandated by statute (e.g., "[a] consumer shall have the right to request that a business delete… personal information") further supports the Agency's broad discretion to regulate ADMTs however it sees fit. Indeed, the statutory text clearly empowers the Agency to "fill up the details" of ADMT regulations, and gives whatever regulations are ultimately promulgated the full force of law.[119] The lack of precise definition of any substantive ADMT rights in the CCPA enhances rather than detracts from the Agency's authority to promulgate rules in this space.[120] Given the Agency's clear legislative mandate to promulgate rules concerning ADMTs, it would be a violation of law to wait for further legislative direction before acting. Although the Legislature is currently considering how to regulate "automated decision tools" that are used for "consequential decisions,"[121] waiting for further legislative action (the timeline for which is highly uncertain) would deprive consumers of urgently-needed protections against high-risk ADMT practices, and unnecessarily prolong the ADMT-driven consumer harms that are already occurring.

Furthermore, in September 2024, the Governor signed into law amendments to the CCPA's definition of personal information to clarify that the term includes physical, digital, and

---

[116] Cal. Civ. Code § 1798.185(a)(15).
[117] *Id*.
[118] *See id.*
[119] Cal. Civ. Code § 1798.105(a) (emphasis added); *Wendz v. State Dep't of Educ*. 93 Cal. App. 5th 607 (2023) (holding that "[t]he Legislature may, after declaring a policy and fixing a primary standard, confer upon executive or administrative officers the "power to *fill up the details*" by prescribing administrative rules and regulations to promote the purposes of the legislation and to carry it into effect …).
[120] *See id.* at 623 ('"Where an agency exercises discretion explicitly conferred on it, it is presumed to act within legislative intent. "… [T]he absence of any specific [statutory] provisions regarding the regulation of [an issue] does not mean that such a regulation exceeds statutory authority … ." [Citations.] [The administrative agency] is authorized to "'*fill up the details* '" of the statutory scheme. [Citation.]' [Citations.]" Moreover, "'where power is given to perform an act, the authority to employ all necessary means to accomplish the end is always one of the implications of the law.'")
Wendz v. State Dep't of Educ., 93 Cal. App. 5th 607, 623, 311 Cal. Rptr. 3d 213, 227 (2023)
[121] *See* Assembly Bill (AB) 331 (as amended in Assembly Mar. 16, 2023), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill id=202320240AB331.

abstract digital formats, including metadata or artificial intelligence ("AI") systems capable of outputting personal information.[122] Section 1798.185 of the CCPA also gives the Attorney General and CPPA authority to adopt regulations that update or add categories of personal information in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.[123] Since many ADMTs make decisions directly based on consumers' personal information, the proliferation of these tools is clearly a "change in technology" that necessitates an update to the definition and regulation of personal information. Indeed, the primary purpose of many ADMTs is to expedite the processing of consumers' personal information, and regulating these technologies is rapidly becoming an essential component of consumer privacy regulation. Thus, the Agency is empowered to regulate both the overall use of personal information and the specific use of ADMTs in the processing of such information.

III. CONCLUSION.

We applaud the Agency for its efforts to protect California consumers and workers from devastating personal data breaches and harmful ADMTs. We welcome the Agency's initiative and appreciate the opportunity to provide these comments.

If you have any questions or if we can provide further information, please do not hesitate to contact us.

Sincerely,

Jordan Hefcart, J.D. '25, UC Berkeley School of Law
David S. Nahmias, Esq., CLASS Network Director and Legal Director,
UC BERKELEY CENTER FOR CONSUMER LAW AND ECONOMIC JUSTICE

Student Comment Authors:
Alexis Barrera, B.A. '25, UC Berkeley
Thanasis Christou, LLM '25 UC Berkeley School of Law
Julia Davidson, J.D. '26, Fordham University School of Law
Sonali Durham, J.D. '26, New York University School of Law
Jennifer Ghoshray, LLM '25 UC Berkeley School of Law
Alex Izbiky, J.D. '25, University of Michigan School of Law
Harshini Malli, J.D. '25, UC Berkeley School of Law
Rosie Moss, J.D. '26, University of Michigan School of Law

[122] AB 1008 (2023-2024); California Privacy Protection Agency, Notice of Proposed Rulemaking, 3 (2024).
[123] Cal. Civ. Code § 1798.185(a)(1), (d) (2024).

Niyati Narang, J.D. ’26, UC Berkeley School of Law
Ilke Okan, LLM ’25, UC Berkeley School of Law
Viktoria Popovska, J.D. ’27, The George Washington University Law School

Research Support:

Lily Button, B.A. ’25, UC Berkeley
Alexa Chavara, J.D. ’27, UC Berkeley School of Law
Greyson Cox, J.D. ’27, University of Maryland School of Law
Viktor Dimas, J.D. ’27, UC Berkeley School of Law
Kosha Chetan Doshi, J.D. ’27, UC Berkeley School of Law
Shikhar Gupta, J.D. ’26, New York University School of Law
Jacqueline Hsing, J.D. ’27, UC Berkeley School of Law
Jola Ilori, J.D. ’27, Georgetown University Law Center
Nikki Iyer, B.A. ’27, UC Berkeley
Lauren Kuo, B.A. ’26, UC Berkeley
Yang Man, LLM ’25, UC Berkeley School of Law
Mirella Piestun, LLM ’25, UC Berkeley School of Law
Sijia Qiu, LLM ’25, UC Berkeley School of Law
Tereza Rezabkova, LLM ’25, UC Berkeley School of Law
Abby Lourdes Roman, B.A. ’26, UC Berkeley
Amanda Ellison Funder Shaw, J.D. ’27, UC Berkeley School of Law
Bright Shi, LLM ’25, UC Berkeley School of Law
Ishika Singhal, J.D. ’27, UC Berkeley School of Law
Hananya Avataram Sunderrak, LLM ’25, UC Berkeley School of Law
Adam Taslitz, B.A. ’27, UC Berkeley

APPENDIX A:
RECENT DATA BREACHES AFFECTING CALIFORNIANS

1. **Cencora, Inc.** [124]

In February 2024, a cyberattack on Cencora Inc. (formerly AmerisourceBergen), and its affiliate Lash Group LLC exposed the personally identifiable and private health information of over 1.43 million individuals, including names, addresses, health diagnoses, and medications. Pharmaceutical partners such as Bristol-Myers Squibb, Pfizer, and Bayer were affected, raising significant concerns over data security in the healthcare sector. The breach led to a class-action lawsuit being filed in June 2024 (*Harrell v. Cencora, Inc*., Case No. 2:24-cv-02524, E.D. Pa. 2024), alleging negligence, insufficient safeguards, and delayed notification. While no evidence of public misuse has been reported, Cencora offered affected individuals credit monitoring services and implemented enhanced cybersecurity measures. The incident underscored the need for stronger data protection and accountability in handling sensitive healthcare information.

Insufficient threat detection, weak access controls, and unpatched vulnerabilities in Cencora systems may have contributed to the breach. It also involves insufficient oversight or weaker security practices in third-party entities handling sensitive data. The proposed Rule's cybersecurity audit requirements could have mitigated the risks leading to the Cencora Inc. breach by requiring companies to proactively identify and address vulnerabilities, including weak access controls, unpatched systems, and insufficient oversight of third-party entities (§ 7123(b)(2)(D), § 7123(b)(2)(O)). Similarly, mandatory threat detection, vulnerability scans, and robust incident response plans (§ 7123(b)(2)(G), § 7123(b)(2)(Q)) might have strengthened Cencora's ability to detect and respond to the attack promptly, reducing the exposure of sensitive personal and health data. Finally, third-party compliance and executive accountability (§ 7123(b)(2)(O), § 7124) could have improved Lash Group LLC's cybersecurity practices and ensured timely breach notification.

---

[124] This summary is based on the following sources: *Katrina Manson, Hackers got Record Ransom of $75 Million for Cencora Breach*, BLOOMBERG (Sept. 18, 2024), https://www.bloomberg.com/news/articles/2024-09-18/gang-got-75-million-for-cencora-hack-in-largest-known-ransom; *Max Mitchell, Bristol-Myers Squibb, Cencora Face Data Breach Class Action,* L. INTELLIGENCER (Jun. 12, 2024), https://www.law.com/thelegalintelligencer/2024/06/12/bristol-myers-squibb-cencora-face-data-breach-class-action/?slreturn=20250105153750; Steve Alder, *Cencora: Additional Data Exfiltrated in February 2024 Cyberattack,* HIPAA J. (Aug. 2, 2024), https://www.hipaajournal.com/cencora-cyberattack-data-breach/.

2. UnitedHealth Group Inc. [125]

In February 2024, UnitedHealth Group's technology unit, Change Healthcare, experienced a significant cyberattack attributed to the ALPHV/BlackCat ransomware group, compromising the personal information of approximately 100 million individuals. The breach, one of the largest in U.S. healthcare history, exposed sensitive data such as health insurance member IDs, diagnoses, treatment details, Social Security numbers, and billing codes. It caused widespread disruptions in claims processing, impacting patients and providers nationwide. UnitedHealth reported the breach on February 21st and began notifying affected individuals in June, as required. The breach also led to an estimated $705 million in business disruption costs and prompted UnitedHealth to issue loans to affected providers while enhancing its cybersecurity measures to prevent future incidents.

The cyberattack was primarily facilitated by exploiting compromised credentials and the absence of multifactor authentication (MFA) on a Citrix remote access service. Hackers from the ALPHV/BlackCat group obtained valid user credentials, which allowed them unauthorized access to Change Healthcare's systems. The lack of MFA—a security measure requiring users to provide multiple forms of verification before gaining access—meant that possessing a single set of credentials was sufficient for the attackers to infiltrate the system. This vulnerability underscores the importance of robust authentication mechanisms to prevent unauthorized access and protect sensitive data. The proposed cybersecurity audit standards under Article 9 likely could have mitigated the risks leading to the UnitedHealth Group data breach by requiring regular identification and remediation of security gaps (§ 7123(c)). The absence of multifactor authentication (MFA) on the Citrix remote access service—a vulnerability exploited in the breach—would have been flagged during the mandatory audit of authentication measures (§ 7123(b)(2)(A)). Internal and external vulnerability scans, penetration testing, and continuous network monitoring (§ 7123(b)(2)(G), § 7123(b)(2)(I)), might have detected the relevant weaknesses before exploitation. Oversight requirements for third-party service providers (§ 7123(b)(2)(O)) might have better ensured compliance with robust security practices, addressing systemic risks. Finally, the emphasis on incident response

---

[125] This summary is based on the following sources: Reuters, *Hack at UnitedHealth's tech unit impacted 100 mln people, US health dept says* (Oct 24,2024), https://www.reuters.com/technology/cybersecurity/hack-unitedhealths-tech-unit-impacted-100-mln-people-2024-10-24; Umar Shakir, *UnitedHealth data breach leaked info on over 100 million people,* VERGE (Oct. 25, 2024), https://www.theverge.com/2024/10/25/24279288/unitedhealth-change-breach-100-million-leak; James Rundle & Catherine Stupp, *Data Breaches Highlight Lack of Basic Cyber Controls,* WALL ST. J. (July 17, 2024), https://www.wsj.com/articles/data-breaches-highlight-lack-of-basic-cyber-controls-a071ec06; Mickey Keane, Terence A. Russo &Vasilios D. Lolis, *Update on Change Healthcare Class Action Litigation,* GARFUNKEL WILD (Sept. 19, 2024), https://garfunkelwild.com/insights/update-on-change-healthcare-class-action-litigation/; *In re Change Healthcare, Inc., Customer Data Sec. Breach Litig.*, No. MDL 3108, 2024 WL 2884723 (U.S. Jud. Pan. Mult. Lit. June 7, 2024); Ahmed Aboulenein & Zeba Siddiqui, *UnitedHealth says hackers potentially stole a third of Americans' data,* REUTERS (May 5, 2021), https://www.reuters.com/world/us/unitedhealth-ceo-testifies-before-us-senate-house-hack-2024-05-01/; *Change Healthcare Class Action Lawsuit to Proceed in Federal Court,* https://compliancy-group.com/change-healthcare-class-action-lawsuit/.

plans and executive accountability (§ 7123(b)(2)(Q), § 7124) could have expedited containment efforts and reduced harm.

3. **United Services Automobile Association (USAA)**[126]

A class action suit claimed that USAA, a financial services company, had failed to protect consumers' private data on its online insurance quote platform. In 2021, cybercriminals entered stolen names, addresses, and dates of birth into the site to generate automatic car insurance premium quotes. These online quotes contained pre-filled information from the DMV, including the consumers' driver's license numbers. Using the driver's license numbers obtained on the site, cybercriminals filed an unemployment claim using one of the plaintiff's names and took out another insurance policy in another's name.

The plaintiffs suffered the additional risk of identity theft, fraud, and further mitigation costs. They also incurred costs associated with the credit freezes and lowered credit scores resulting from credit inquiries. A routine cybersecurity audit would reveal the risks of auto-populating consumers' driver's license numbers. In particular, Article 9 § 7123 (b)(2)(E)(i) describes the proper management of personal information inventories, and Article 9 § 7123 (c) sets out requirements for cyber security audits.

4. **Blackbaud**[127]

Blackbaud, a software services company, became aware of a data breach in May of 2020 when a hacker accessed Blackbaud's systems and threatened to publish the private data of over 13k customers (whose databases collectively contained the personal information of millions of individuals). Sensitive customer information included in the breach included social security numbers, bank account information, and medical data. Blackbaud paid the requested ransom, and the hacker deleted the data. The hacker accessed Blackbaud systems using a customer's compromised login and password. The company (a) lacked password requirements, such as rotating passwords and password strength minimums, (b) lacked network segmentation, (c) stored customer data for longer

---

[126] This summary is based on the following sources: *Dolan v. United States Automobile Association, Opinion and Order,* https://cases.justia.com/federal/district-courts/new-york/nysdce/7:2021cv05813/562957/41/0.pdf?ts=1660404541; *In Re USAA Data Security Litigation, Jury Trial Demanded*, https://www.classaction.org/media/in-re-usaa-data-security-litigation-consolidated-amended-complaint.pdf; *$3.25M USAA Settlement Aims to Resolve Data Breach Lawsuit Over May 2021 Cyberattack,* https://www.classaction.org/news/3.25m-usaa-settlement-aims-to-resolve-data-breach-lawsuit-over-may-2021-cyberattack#embedded-document.

[127] This summary is based on the following sources: *Blackbaud Announces 2023 Fourth Quarter and Full Year Results, https://investor.blackbaud.com/news-releases/news-release-details/blackbaud-announces-2023-fourth-quarter-and-full-year-results*; *California v. Blackbaud,* Complaint for Injunction, Civil Penalties, and Other Equitable Relief, https://oag.ca.gov/system/files/media/blackbaud-complaint.pdf; *California v. Blackbaud*, Final Judgment and Permanent Injunction, https://oag.ca.gov/system/files/media/blackbaud-proposed-final-judgment-and-permanent-injunction.pdf

than necessary, (d) did not mandate authentication methods, (e) failed to ensure consumers stored their data in encrypted fields, and (f) did not implement sufficient cybersecurity threat detection methods.

The proposed rule would require multi-factor authentication, password strength minimums, encryption of personal information, and zero-trust architecture that would likely have helped prevent the Blackbaud breach (Article 9 § 7123 (b)(2)(A-D).

5. **Illuminate Education**[128]

Illuminate Education, an education software platform used to collect, report, organize, and analyze student data, was affected by a cyberattack in January 2022. The cyberattack infiltrated Illuminate company databases containing extensive student data, which resided on the Amazon Web Services (AWS) online storage system. The cyberattack affected school districts across the country, including the Los Angeles Unified School District. The exact number of individuals affected by the data breach in California is unknown, but over 38 school districts with over 900,000 students enrolled at the time were targeted. Illuminate states that there was "no evidence that any information was subject to actual or attempted misuse" and that it has implemented enhanced security measures. Illuminate has previously promoted its security measures and signed onto an industry pledge to show support for safeguarding students' data.

The breach impacted many classes of highly-sensitive student data, including names, dates of birth, races and ethnicities, test scores, tardiness rates, migrant status, behavioral incidents, and descriptions of disabilities. Under Section 7121 of the Proposed Rule, businesses like Illuminate that process consumers' personal information would have to conduct a cybersecurity audit once every calendar year. Had this requirement been in place before the breach, Illuminate might have been able to identify and mitigate the vulnerabilities their AWS configuration system that were exploited. Similarly, Section 7123's specific mandate for a regular "inventory and management of personal information and the business's information system" as well as "secure configuration of hardware and software," could have uncovered weaknesses in the system's data management and protection.

---

[128] This summary is based on the following sources: *A Cyberattack Illuminates the Shaky State of Student Privacy*, https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html; *Illuminate Education data breach now reported in Los Angeles schools, too*, https://www.k12dive.com/news/illuminate-education-data-breach-now-reported-in-los-angeles-schools-too/624938/; *List of All K-12 Schools Known to be Impacted by Illuminate Breach of Student Data*, https://thejournal.com/Articles/2022/05/15/List-of-All-Schools-Confirmed-Impacted-by-Illuminate-Education-Data-Breach.aspx?Page=1; *A Cyberattack Illuminates the Shaky State of Student Privacy*, https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html; *J.M. v. Illuminate Education, Inc*., 103 Cal. App. 5th 1125.

6. **Kiteworks, formerly known as Accellion**[129]

Accellion, Inc. is the developer of a file-sharing transfer tool called File Transfer Appliance ("FTA"), intended to "facilitate secure, encrypted file sharing that exceeded limits imposed on the size of email attachments." Hundreds of companies, private organizations, and government entities used Accellion's file transfer services. When individuals transact with organizations that use Accellion's FTA software, they are usually required to provide personal private information, which Accellion then transfers. Before December 2020, Accellion allegedly became aware that the FTA product was "nearing the end of its life" and encouraged customers to switch to a new product called Kiteworks. On December 16th, 2020, an Accellion customer was alerted by the FTA's anomaly detector that unauthorized third parties had exploited the FTA. Upon investigation, Accellion confirmed that the FTA software contained two security vulnerabilities: SQL Injection and OS Command Execution. Between December 16th and December 23rd, Accellion released two patches to address the vulnerabilities and notified its clients between December 2020 and January 2021. On January 20th, 2021, a second attack occurred, involving two vulnerabilities described as Server-Side Request Forgery and OS Command Execution. At this point, Accellion advised its clients to shut down their FTA systems.

The data breach involved zero-day vulnerabilities in the company's File Transfer Appliance. "In December 2020 and then again in January 2021, cyber-criminals exploited multiple' zero-day 'vulnerabilities—vulnerabilities that had never been discovered in FTA's decades of service, despite penetration testing and other monitoring by both Accellion and its customers, as well as scrutiny by external security researchers through Accellion's bug bounty program—in the FTA, allowing the criminals to illegally access information stored on FTA Customers' systems," the filing explained. The information exposed included "names, dates of birth, Social Security numbers, driver's license numbers and/or state identification numbers, bank account information, employment information, and personal health information," collectively referred to as Plaintiff's "personally identifiable information" ("PII").

Section 7123 of the proposed Rule would require each covered business to annually inventory all personal information it collects and audit its information system and secure hardware and software configuration. The audit process would require specific examination of security patch management and software updates and upgrades—the kind of due diligence that might have prevented FTA users from continuing to use the tool after its end-of-life advisory was published. Additionally, the required penetration testing

[129] This summary is based on the following sources: *Accellion reaches $8.1 mln settlement to resolve data breach litigation*, https://www.reuters.com/legal/litigation/accellion-reaches-81-mln-settlement-resolve-data-breach-litigation-2022-01-13/; *What is an Accellion Cyber Attack?*, https://socradar.io/what-is-an-accellion-cyber-attack/; *In re Accellion, Inc. Data Breach Litig.*, 713 F. Supp. 3d 623 (2022).

might have uncovered the vulnerabilities in FTA deployments—since whatever penetration Accellion itself was doing was clearly woefully insufficient.

7. **Delta Dental of California (and all other institutional victims of the MOVEit breach)**[130]

In May 2023, Delta Dental of California became one of hundreds companies and government agencies to have its customers' data compromised by a vulnerability in the MOVEit Transfer software, a widely used file transfer application. The Delta Dental breach alone compromised the personal information of approximately 6.9 million individuals nationwide, including many Californians. The exposed data included Social Security numbers, names, addresses, health insurance details, and financial account information. The breach raised concerns about Delta Dental's third-party software oversight and risk management practices, given its role in handling sensitive health-related data for residents.

The attack exploited a zero-day vulnerability (CVE-2023-34362) in MOVEit Transfer. This SQL injection vulnerability likely occurred due to insufficient patch management and inadequate vendor oversight, allowing attackers to steal unencrypted sensitive data. A routine cybersecurity audit and penetration test under proposed Article 9 could have identified the MOVEit Transfer software vulnerability exploited in the Delta Dental breach.

8. **Patelco Credit Union**[131]

On June 29th, 2024, Patelco Credit Union, a California-based financial institution, experienced a ransomware attack, leading to the shutdown of critical banking systems, including online banking, mobile apps, and call centers. Members could not access account information, transfer funds, or make payments for several days. Limited services, such as ATM withdrawals and debit card transactions, remained available but at reduced capacity. Sensitive personal data, including Social Security numbers, account details, and other personally identifiable information (PII), was potentially exposed and shared on the

[130] This summary is based on the following sources: *Delta Dental of California Data Breach: 7 Million Individuals Affected*, https://www.hipaajournal.com/delta-dental-california-data-breach/; *May 2023 MOVEit Data Breach Triggers Class Action Against Delta Dental*, https://www.classaction.org/news/may-2023-moveit-data-breach-triggers-class-action-against-delta-dental; *Notice of Data Breach*, https://www1.deltadentalins.com/content/dam/ddins/en/pdf/banners/notice-of-moveit-data-security-incident-en.pdf; *Delta Dental Says Data Breach Exposed 7 Million Customers,* https://www.securityweek.com/delta-dental-of-california-discloses-data-breach-impacting-6-9-million-people/.

[131] This summary is based on the following sources: *Sabita J. Soneji Appointed to Leadership in Consolidated Class Action Against Patelco Credit Union*, https://www.tzlegal.com/news/soneji-appointed-leadership-consolidated-class-action-patelco/; *Patelco Credit Union confirms data breach affecting 726,000 customers,* https://www.techmonitor.ai/technology/cybersecurity/patelco-credit-union-confirms-data-breach-affecting-726000-customers?; Patelco credit union $500-limit after cyberattack frustrating customers, https://www.ktvu.com/news/patelco-credit-union-500-limit-after-cyberattack-frustrating-customers Patelco Outage?, https://www.reddit.com/r/bayarea/comments/1ds63dp/patelco_outage/.

dark web. The breach caused significant disruptions for members during payment cycles, as recurring payments and direct deposits failed.

The attack exploited gaps in Patelco's cybersecurity, including a lack of advanced intrusion detection systems, outdated systems and infrastructure, and weak incident response preparedness. Proposed CPPA standards, including vulnerability scanning (§ 7123(b)(7)) and incident response plans (§ 7123(b)(17)), could have helped prevent or reduce the breach's impact.

9. **Postmeds/Truepill**[132]

Postmeds (d/b/a Truepill) is a digital pharmacy that fulfills customers' mail-order prescriptions nationwide. It suffered a data breach on August 30th, 2023, when malicious actors accessed Postmeds' databases, acquired unencrypted information that Postmeds shared with third parties, and disseminated it on the dark web. Over 2.3 million customers were affected by the data breach. The Plaintiffs in a subsequent class action lawsuit asserted that Postmeds 1) failed to disclose details about what demographic information was compromised/details about the root cause of the breach/vulnerabilities that were exploited/remedial measures undertaken to ensure another breach does not occur; 2) failed to use adequate security protocols (e.g., encryption, deleting information, spam filters, firewalls, etc.); 3) knew there was a specific risk against pharmaceutical companies; and 4) failed to comply with FTC/HIPAA cybersecurity guidelines and industry standards.

The breach targeted unencrypted data in files that were transmitted to third parties. The attackers collected customers' personally identifiable and protected health information, including their names, DOBs, SSNs, medical records numbers, diagnosis information, treatment information, prescription information, and health insurance information. A required cybersecurity audit might have helped the company to identify vulnerabilities in their data management and transmission systems before they were exploited. Also, the proposed requirements regarding encryption at rest and in transit (§ 7123(2)(B)) could have prevented this type of attack.

---

[132] This summary is based on the following sources: *Postmeds Agrees to $7.5 Million Settlement to Resolve Data Brach Lawsuit*, https://www.hipaajournal.com/postmeds-truepill-sued-over-2-3-million-record-data-breach/; *Reeds v. Postmeds,* Class Action Complaint, https://advance.lexis.com/f/courtlinkdocument/jobstatus/downloadfile/0ebaa4ac-c00b-492b-9ed9-516522965d95/urn:contentItem:69X4-C4T3-RSFG-G3GF-00000-00/1/0/d90162596e6016/0/s3/US_DIS_CAND_4_23cv5710_d90162596e6016_CLASS_ACTION_COMPLAINT_AND_JURY_TRIAL_DEMANDED_aga; *In Re: PostMeds, Inc. Data Breach Litigation, Order Granting Preliminary Approval of Settlement*, https://advance.lexis.com/f/courtlinkdocument/jobstatus/downloadfile/0ebaa4ac-c00b-492b-9ed9-516522965d95/urn:contentItem:6DH7-5H03-RS95-S2MF-00000-00/105/0/d90162596e9291/0/s3/US_DIS_CAND_4_23cv5710_d90162596e9291_ORDER_by_Judge_Haywood_S_Gilliam_Jr_GRANTING_97_PR.

10. 23andMe[133]

23andMe provides consumers with genetic testing services, personalized ancestry, and health-related insights. On October 10th, 2023, 23andMe filed an 8-K with the SEC confirming a data breach, where hackers gained access to 14,000 accounts, obtaining the data of around 6.9 million users (half of 23andMe's users). Individual datasets were sold on the dark web, including specific datasets that targeted Chinese and Ashkenazi Jewish users. Plaintiffs asserted that 1) the stolen data was circulating for months before 23andMe's disclosure; 2) 23andMe did not provide adequate information on the scope of the data breach; 3) 23andMe was negligent in its website design, allowing easy access to user data; and 4) 23andMe failed to implement adequate security safeguards.

The 23andMe attackers used a technique called "credential stuffing," wherein they obtained passwords from other data breaches on other websites and used those credentials to gain access to the same users' 23andMe accounts. This technique succeeds if users reuse weak passwords across multiple platforms. Additionally, the affected users did not enable multi-factor authentication on their 23andMe accounts, allowing hackers to access their accounts simply by entering a password. Though the hackers only gained access to 14,000 accounts this way, they used 23andMe's DNA Relatives feature (which allows customers to share some of their data with other users automatically) to access data from 6.9 million users. Hackers accessed the following types of information: name, birth year, relationship labels, percentage of DNA shared with relatives, ancestry reports, family trees, self-reported location, any uploaded photos, raw genotype data, and health information (like disease predisposition reports or carrier-status reports).

Required cybersecurity audits might have encouraged 23andMe to more seriously assess the unique vulnerabilities associated with genetic data. Additionally, deploying mandatory multi-factor authentication (§ 7123(2)(A)) and automatic intrusion-detection systems (§ 7123(2)(I)) could have limited or even prevented this type of credential-stuffing attack.

---

[133] This summary is based on the following sources: Steve Alder, *23andMe User Data Stolen in Credential Stuffing Attack,* HIPAA J. (Oct. 10, 2023), https://www.hipaajournal.com/23andme-user-data-stolen-credential-stuffing-campaign/; Steve Alder, *6.9 Million 23andMe Users Affected by Data Breach,* HIPAA J. (Dec. 5, 2023), https://www.hipaajournal.com/6-9-million-23andme-users-affected-by-data-breach/; Steve Alder, *23andMe Settles Data Breach Lawsuit for $30 Million*, HIPAA J. (Sept. 16, 2024), https://www.hipaajournal.com/23andme-class-action-data-breach-settlement/; Lars Daniel, *23andMe To Pay Up To $10,000 To Data Breach Victims—Are You Eligible?,* FORBES (Oct. 15, 2024), https://www.forbes.com/sites/larsdaniel/2024/10/15/23andme-to-pay-up-to-10000-to-data-breach-victims-are-you-eligible/.

11. Snowflake Inc.[134]

In April 2024, cloud data company Snowflake experienced a breach affecting millions of people, including customers of Advance Auto Parts, Ticketmaster, AT&T, Santander Bank, and Neiman Marcus. The hacker who breached the company used credentials harvested through information-stealing malware, exploiting inadequate identity and access controls that permitted many organizations to access to their Snowflake databases without mandatory multi-factor authentication.

Hackers accessed sensitive data from clients such as AT&T, Ticketmaster, and Santander Bank by exploiting unencrypted usernames and passwords stored in JIRA. The accounts did not enable multi-factor authentication (MFA), making it easy to infiltrate. The breach accessed over 30 million bank account details, including 6 million account numbers and balances and 28 million credit card numbers. AT&T reported that nearly all its customers' call and text records from May to October 2022 were exposed. Ticketmaster faced unauthorized access to event ticket barcodes, including those for major concerts. Despite the FBI's attempts to seize online forums to sell the stolen data, the stolen information still appears on online marketplaces. As a third-party cloud-based data host platform, Snowflake stores the data for its corporate clients, including the personal information of millions of consumers. This means Snowflake Inc. meets the processing threshold under Article 9 to necessitate cybersecurity audits under §§ 7121-23. The proposed regulation under Article 9 provides for the annual independent audit to identify vulnerabilities. Such a review could have identified the weaknesses of Snowflake's system and prevented the breach. For example, the Article 9 audit includes a review of multiple security components, including multi-factor authentication, strong, unique passwords, and encryption of personal information. The chief information security officer for Snowflake, Brad Jones, stated that the incident appears to be a "targeted campaign directed at users with single-factor authentication."

The component measures of an Article 9 audit might have identified this noncompliance. Had Snowflake been better equipped and compliant with such CCPA revisions, this breach might have been wholly prevented, given the company's admissions regarding the vulnerability exploited when the hacker accessed the personal information. Since the breach, Snowflake has implemented these recommended changes to address data breaches in the future, including making changes to the multi-factor authentication process and increasing the strength and uniqueness of user password requirements.

---

[134] This summary is based on the following sources: *The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever,* https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/; *Snowflake customers caught in identity-based attack spree,* https://www.cybersecuritydive.com/news/snowflake-customer-databases-breached/717801/; *Hacker behind Snowflake customer data breaches remains active,* https://cyberscoop.com/snowflake-hacker-judische-labscon-2024/.

12. Kaiser Permanente[135]

Kaiser Permanente (Kaiser) provides health care coverage to over 9.4 million Californians yearly. Kaiser collects extensive personal information, including patient names, addresses, phone numbers, and email addresses, as well as highly sensitive PII (SSA, info on financial accounts and health insurance, info to run health screening, education/employment history, etc.).

On September 3rd, 2024, Kaiser Permanente learned that an unauthorized party had gained access to two employee email accounts. The attackers used this access to collect extensive patient information, including names, dates of birth, medical record numbers, and medical information.

Proposed Article 9's required regular independent cybersecurity audits (§ 7121) could have helped to significantly limit or prevent this breach—particularly the required analysis of account management and access controls. Section 7123 would require an understanding of each employee's role and the amount of data necessary to perform their duties and restricting any data outside that range. Additionally, vulnerability scans and penetration testing could have helped identify system weaknesses.

[135] This summary is based on the following sources: *Kaiser Permanente reports email data breach,* https://www.techtarget.com/healthtechsecurity/news/366615144/Kaiser-Permanente-reports-email-data-breach; *Kaiser Permanente 2024 Data Breach Investigation*, https://www.myinjuryattorney.com/kaiser-permanente-data-breach-investigation-2024/; *Kaiser Permanente Data Breach: What to Know,* https://www.forthepeople.com/blog/kaiser-permanente-data-breach-what-know/.

Appendix B: Examples of ADMTs

1. **A.M. Simpkins & Associates' S.A.F.E. Algorithm**

A.M. Simpkins & Associates contracts with institutions of higher education (IHEs) to market their service: S.A.F.E.[136] S.A.F.E. uses "advanced algorithms to scrutinize applicant data" for indicators of fraud. IHEs using S.A.F.E. may use the algorithmic outputs to inform their admissions decisions.

S.A.F.E. itself is a service sold by A.M. Simpkins & Associates for use by IHEs, so the documentation on the website is limited and no direct notices to consumers are provided. It is not immediately clear which IHEs utilize S.A.F.E., whether those institutions are in California, or whether those IHEs provide the relevant consumer notices to applicants. The direct harms to California consumers are relatively limited. This use of ADMT is primarily to prevent fraudulent activity, e.g., attempting to fraudulently obtain federal financial aid or securing access to a university email account to gather data for phishing purposes. However, if misused, this use of ADMT may harm prospective students by flagging their application as fraudulent. Additionally, while the use of ADMT is designed to protect the university and save taxpayer money, it may raise data privacy issues if the corporation or the university are subject to a cyberattack or data breach. Many of these systems use biometric data like facial recognition to verify an individual's identity, which raises privacy concerns.

The output of the technology is a flag or indicator on a prospective applicant's file in a Student Information System (SIS) which is then used by an admissions professional at an IHE to decide the application's viability. This is one of the educational uses specifically mentioned in the proposed regulations under § 7200(a)(1)(A)(i). The admissions professional does have the discretion to review the work of the program before making a final decision, but the marketing materials suggest that the purpose is to save time by reducing the need for human review of every single application. Under § 7221(b)(1)(B), this ADMT would likely not need to provide applicants with the opportunity to opt-out of the data collection since its sole purpose is to detect applicants attempting to defraud the IHE. This is relevant because the IHEs that are particularly attractive to fraudsters are generally open-access or low-barrier IHEs that do not charge application fees.[137]

2. **Sift**

Sift is a fraud prevention platform that uses ADMT to analyze consumer transactions and behaviors in real time.[138] By processing vast amounts of data, including browsing history, purchase patterns, and device information, Sift generates risk scores to determine whether a transaction is likely to be

[136] A.M. Simpkins & Assoc., "*S.A.F.E.: Detect False Applications in Real-Time*" (Dec, 30, 2024) https://amsa-highered.com/safe/.
[137] Swaak, Taylor, *As Fake Applications Soar, Colleges Turn to Ai*, The Chronicle of Higher Education. Accessed January 6, 2025. https://www.chronicle.com/article/colleges-see-alarming-rates-of-fake-applications-so-theyre-turning-to-ai.
[138] "AI-Powered Fraud Decisioning." Sift. https://sift.com/. Accessed January 5, 2025.

fraudulent.[139] Businesses use these scores to decide whether to approve or decline transactions, or even flag accounts for further review.[140]

Sift provides notice to users when their data is being processed for fraud detection, particularly in the context of transactions. However, consumers may not always be fully aware of the extent of the data being collected or how it is used to generate risk scores. Sift's algorithm may unintentionally flag legitimate transactions as fraudulent, especially for vulnerable groups such as older adults, low-income consumers, or those who are not tech-savvy. These false positives can lead to denied transactions, disrupted services, and reputational harm. Vulnerable consumers may also be disproportionately affected by the platform's reliance on behavioral profiling, which may not account for contextual or socio-economic factors influencing their transaction history. Sift's ADMT qualifies under the CPPA's proposed regulations (§ 7001(f)) because it processes personal information (e.g., transaction and browsing data) and uses computation to generate risk scores. These scores substantially facilitate human decision-making by directly influencing whether a transaction is approved or declined. Additionally, Sift's profiling activities—such as evaluating spending habits and behavioral patterns to assess fraud risk—are explicitly included in the definition of ADMT under the proposed regulations.[141]

3. **Visa**

Visa's system analyzes millions of transactions in real-time to detect fraud patterns, using AI to decline suspicious payments.[142] By evaluating each CNP transaction against enumeration patterns, the new risk scoring model derives a two-digit risk score that helps predict the likelihood of enumeration to help better determine when to approve or decline transactions.

The main concern with this technology is the fact that the AI algorithm relies on a significant amount of user data to continually train itself while operating with minimal human oversight, presenting a large risk of false positives as well as false negatives. Visa's system falls within the definition of this rule as it processes individuals' current and past purchase data that is subsequently used to evaluate the transactions.

---

[139] Sift, *Sift Ushers in ERA of AI-Powered Fraud Decisioning amid Surging Company Momentum and Evolving Market Dynamics*, GlobeNewswire News Room (Feb 20, 2024), https://www.globenewswire.com/news-release/2024/02/20/2832122/0/en/Sift-Ushers-in-Era-of-AI-Powered-Fraud-Decisioning-Amid-Surging-Company-Momentum-and-Evolving-Market-Dynamics.html.

[140] Sift, *SIFT Analytics Unveils Data Trends, Challenges, Opportunities, and Future Outlook*, SIFT Analytics Group (Feb. 6, 2024), https://sift-ag.com/news/sift-analytics-unveils-data-trends-challenges-opportunities-and-future-outlook/.

[141] Sift, *Sift Secures 40 Patents, Reinforcing Leadership in Digital Trust & Safety*, GlobeNewswire News Room (Jan. 4, 2024), https://www.globenewswire.com/news-release/2024/01/04/2804225/0/en/Sift-Secures-40-Patents-Reinforcing-Leadership-in-Digital-Trust-Safety.html..

[142] VISA, *Visa Announces Generative AI-Powered Fraud Solution to Combat Account Attacks*, https://investor.visa.com/news/news-details/2024/Visa-Announces-Generative-AI-Powered-Fraud-Solution-to-Combat-Account-Attacks/default.aspx. Accessed January 6, 2025.

4. **Candor Technology, Inc.**

Candor Technology, Inc. provides a suite of different services--Candor PreQual, CandorPlus, Candor LES, and Candor LQS--which assist financial institutions with mortgage underwriting.[143] Their website refers to Candor as a "decision engine."[144] PreQual is a prequalification service, which provides "near instantaneous borrower insight and decisioning."[145] Candor LES "automates the underwriting process."[146] CandorPlus and Candor LQS extend the automation beyond the beginning stages and into the later lifecycle of an institution's mortgage lending decision, including closing.[147] Candor markets its services to financial institutions, not directly to consumers. Accordingly, no notice could be found on their website that would satisfy the notification requirements under the proposed regulations. Those financial institutions may or may not disclose that their underwriting process is automated in full or in part. Candor's website is clear that it provides ADMT, though without using that term, and expressly mentions algorithms, AI, and machine learning.[148] Candor's Privacy Policy also provides notice to consumers that they have may have certain rights to access, modify, delete, opt out, or restrict the use of their data depending on their jurisdiction.[149]

Candor is utilized by FBC Mortgage, LLC and Bay Equity Home Loans per testimonials on Candor's website. Both corporations operate branches in California, which suggests that Californian citizens may run into Candor's ADMT. Other financial institutions besides these two may utilize Candor and operate in California. A consumer in California seeking a loan may experience an "instantaneous" denial through Candor PreQual, implying that a decision may be rendered before an underwriter ever examines the file. This could harm consumers in a number of ways if the algorithms, AI models, or machine learning models are miscalibrated or poorly trained. Additionally, existing biases in mortgage underwriting may be deeply entrenched in the ADMT's decisions if training data was inadequately screened or adjusted to account for underwriter bias. Candor's website also refers to a "MetaScore" that summarizes "loan and data quality." Depending on how this score is calculated or how it is utilized, this MetaScore may affect the rates or lengths of mortgages offered to applicants or may alter the way that a financial institution interacts with a consumer after the mortgage has been issued.

5. **Upstart**

---

[143] Candor Technology, *Award-Winning Ai Underwriting*, https://www.candortechnology.com/. Accessed January 6, 2025.
[144] Candor Technology, *Award-Winning Ai Underwriting*, https://www.candortechnology.com/services. Accessed January 6, 2025.
[145] Candor Technology, *Prequal: Ai Loan Underwriting,* https://www.candortechnology.com/candor-prequal. Accessed January 6, 2025.
[146] Candor Technology, *Les: Award-Winning Ai Underwriting*, https://www.candortechnology.com/candor-lesbb487beb. Accessed January 6, 2025.
[147] Candor Technology, *Candorplus: Ai Mortgage Underwriting*, https://www.candortechnology.com/candorplusab7a0c2a. Accessed January 6, 2025.
[148] Candor Technology, *Loan Quality Services: Ai Loan Underwriting*, https://www.candortechnology.com/hmda-data-analysis. Accessed January 6, 2025.
[149] Candor Technology, *Privacy Policy*, https://www.candortechnology.com/privacy-policy. Accessed January 6, 2025.

Upstart is an AI-powered lending platform that uses ADMT to assess loan eligibility.[150] The platform analyzes various data points, including credit scores, income, education, and job history, to generate a risk assessment score that determines loan approval.[151] Upstart claims that its technology enables it to offer better rates to borrowers who may not have access to traditional credit scoring systems.[152]

Upstart provides notice to users about the data being collected for credit assessments, and users must consent to the collection and processing of their personal information as part of the loan application process. While Upstart claims to increase inclusivity in lending, its reliance on ADMT may inadvertently perpetuate biases. Marginalized groups, such as individuals with non-traditional financial histories, younger borrowers, or those from underserved communities, may face disadvantages due to the algorithm's potential for discriminatory patterns. The lack of transparency in how risk scores are generated can also leave consumers unaware of how their personal data impacts loan outcomes, eroding trust and limiting recourse.

6. **Fama**

Fama uses AI-driven ADMTs to analyze job candidates' social media activity and online presence.[153] The tool scans posts, comments, and interactions to flag content deemed inappropriate or indicative of risk factors like discriminatory behavior or substance abuse.[154] Employers use these insights to decide whether to move forward with a candidate.

Fama provides limited notice to users, as the analysis often happens without the individual's direct involvement or explicit consent. The tool risks perpetuating biases, misinterpreting context, and penalizing individuals for outdated or irrelevant online activity. This can disproportionately harm vulnerable groups, such as young people or those from marginalized backgrounds.[155]

7. **Predictim**

Predictim is a platform that uses ADMT to assess babysitters and caregivers by analyzing their social media activity.[156] The tool employs AI and machine learning to generate risk scores based on attributes

---

[150] PR Newswire, *Upstart Announces First AI-Powered Credit Decision API* (May 20, 2020), https://www.prnewswire.com/news-releases/upstart-announces-first-ai-powered-credit-decision-api-301062546.html.
[151] Leonardo Leal, *Upstart: Using Machine Learning to Transform the Personal Loan Experience*, Harvard MBA Student Perspectives (Nov. 26, 2019), https://d3.harvard.edu/platform-digit/submission/upstart-using-machine-learning-to-transform-the-personal-loan-experience/.
[152] PYMNTS.com, *FinTech IPO Outlook: Profits and Platforms Take Center Stage* (Jan. 3, 2025), https://www.pymnts.com/news/retail/2024/was-your-favorite-holiday-tradition-once-marketing-campaign/.
[153] AI for All, *Using AI for Hiring with Fama's Ben Mones*, YouTube (Jan. 5, 2024), https://www.youtube.com/watch?v=ziL0Pnvb8OA.
[154] Edge Delta, *Fama Case Study*, https://edgedelta.com/company/case-studies/fama. Accessed January 6, 2025.
[155] Rebecca Heilweil, *Beware of These Futuristic Background Checks*, Vox (May 11, 2020), https://www.vox.com/recode/2020/5/11/21166291/artificial-intelligence-ai-background-check-checkr-fama.
[156] Brian Merchant, *Predictim Claims Its AI Can Flag 'risky' Babysitters. So I Tried It on the People Who Watch My Kids*, Gizmodo (Dec 6, 2018), https://gizmodo.com/predictim-claims-its-ai-can-flag-risky-babysitters-so-1830913997.

such as trustworthiness, professionalism, and likelihood of engaging in harmful behaviors.[157] Parents or guardians use these scores to decide whether to hire a caregiver.[158]

Predictim provides notice to the users who initiate the screening (e.g., parents), but individuals being evaluated (e.g., caregivers) often receive no direct notice or opportunity to consent to the analysis of their social media data.[159] Predictim's algorithmic evaluations can misinterpret social media content, resulting in inaccurate or biased assessments. For instance, humor, cultural nuances, or harmless interactions could be flagged as "high risk." This poses significant reputational harm to caregivers, particularly those from underrepresented or marginalized communities, who may face unjust hiring decisions based on flawed risk scores. Additionally, such practices can disproportionately impact younger caregivers, whose social media history may not reflect their current behavior or maturity.

8. **Equivant**

Equivant (formerly Northpointe) provides U.S. Courts with the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), a tool used to evaluate the risk of recidivism.[160] COMPAS is a 137-question survey that considers factors such as age, sex, and offense history.[161] COMPAS provide a case-management plan for each offender and provides risk estimates. The risk estimates are considered by the correctional counselors and are used to determine what programs best fit the incarcerated individual's timeline. Judges also receive a prediction of defendants' recidivism risk. Versions of COMPAS are used for youth, reentry, and pretrial.

Regarding the provision of notice, information about COMPAS is displayed on the California Department of Corrections and Rehabilitation's website and in their FAQ. The risk of a computer algorithm that assesses the likelihood of recidivism is that it can lead to unequal treatment in the criminal justice system.[162] Judges use these risk assessments during criminal sentencing. If judges act on these predictions, they can further entrench racial and socioeconomic biases in the court system. COMPAS falls within the definition of ADMT under § 7001(f)(3). COMPAS is a profiling tool that gathers and evaluates an incarcerated individual's personal data to make predictions. The California Department of Corrections and Rehabilitation's Division of Rehabilitative Programs FAQ state that the COMPAS assessment is one of the most influential tools that CDCR uses to determine an incarcerated individual's rehabilitative needs and likelihood of reoffending.

---

[157] Dave Lee, *Predictim Babysitter App: Facebook and Twitter Take Action*, BBC News (Nov. 27, 2018). https://www.bbc.com/news/technology-46354276.
[158] Drew Harwell, *Wanted: The 'Perfect Babysitter.' Must Pass AI Scan for Respect and Attitude*, Washington Post (Nov. 23, 2018), https://www.washingtonpost.com/technology/2018/11/16/wanted-perfect-babysitter-must-pass-ai-scan-respect-attitude/.
[159] Kyle Wiggers, *Babysitter Screening App Predictim Uses AI to Sniff out Bullies*, VentureBeat (Oct. 4, 2018), https://venturebeat.com/ai/babysitter-screening-app-predictim-uses-ai-to-sniff-out-bullies/.
[160] Division of Rehabilitative Programs (DRP), *Rehabilitative Process*, California Dep't of Corrections (Nov. 15, 2024), https://www.cdcr.ca.gov/rehabilitation/about/process/.
[161] Christoph Engel, Lorenz Linhardt, and Marcel Schubert. *Code Is Law: How Compas Affects the Way the Judiciary Handles the Risk of Recidivism*, *Artificial Intell. L.*, (April 2, 2024) https://link.springer.com/article/10.1007/s10506-024-09389-8.
[162] Angwin, Julia, Jeff Larson, Lauren Kirchner, and Surya Mattu. *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

9. **Arnold Ventures: The Public Safety Assessment (PSA) system**

The Public Safety Assessment (PSA) system was developed by the Arnold Foundation (Arnold Ventures), a philanthropy organization.[163] Various state and local jurisdictions who choose to adopt the system must complete a list of requirements to tailor it to their jurisdiction. The PSA system is an actuarial assessment that estimates failure to appear in court pretrial and likeliness of new arrests while on pretrial release.[164] The system generates scores for defendants based on: (1) Age at current arrest; (2) Current violent offense; (3) Pending charge at the time of the offense; (4) Prior misdemeanor conviction; (5) Prior felony conviction; (6) Prior violent conviction; (7) Prior failure to appear in the past two years; (8) Prior failure to appear older than two years; and (9) Prior sentence to incarceration. The score generated by the system is then reviewed primarily by judges during pretrial hearings to inform their decisions regarding pretrial release, bail conditions, and whether the defendant poses a risk of committing another crime or failing to appear in court. If a defendant has a high PSA score, judges may be inclined to deny bail or impose structure conditions for release, and defendants may face disadvantages in negotiating bail or plea deals. It has been utilized in at least 23 CA counties from 2014-2024.

There is some notice provided by the PSA technology. The factors and methods used to calculate PSA scores are publicly available online, and jurisdictions are recommended by the Arnold Foundation to make individual PSA scores available to the defendant, judicial officer, defense, council and prosecution. However, jurisdictions are not required to do this. This ADMT is intended to filter out bias by excluding age, ethnicity, or geographic location. However, research by universities such as the Ford School of Public Policy at the University of Michigan has found that the data used by these tools are a result of the individual biases it is created to avoid, such as outdated policing and sentencing practices and racial and socioeconomic profiling.[165] The tools also rely dramatically on variables influenced heavily by socioeconomic and racial disparities, such as data points (7) and (8) on failures to appear in court. The Ford School found that the majority of missed court dates were not for intentional reasons, but instead because of missed busses, inability to find childcare, or inability to get time off work. As the system relies on historical data to generate scores, reliance on PSA scores to determine bail or release conditions poses the risk of creating a feedback loop in which a defendant's high score can lead them to disadvantages preparing a legal defense, harsher convictions, and lower future PSA scores as a result.

10. **Microsoft**

[163] Advancing Pretrial Policy & Research (APPR), *PSA Map* (Aug. 13, 2024), https://advancingpretrial.org/psa/psa-map/.
[164] California Judiciary, *Pretrial Risk Assessment Tool Validation* (June 2021), https://www.courts.ca.gov/documents/Pretrial-Risk-Assessment-Tool-Validation_June-2021_FinalPosted.pdf.
[165] Gerald R. Ford School of Public Policy, *Pretrial Risk Assessment Tools Found to Be Subjective and Biased* (May 4, 2023), https://fordschool.umich.edu/news/2023/pretrial-risk-assessment-tools-found-be-subjective-and-biased.

The Azure AI Face service is a facial-recognition algorithm created by Microsoft.[166] The program allows businesses and developers to integrate facial recognition into their applications. Common uses of the Face service from its website include verifying user identities, liveliness detection, touchless access controls, and face redactions.

While Microsoft encourages business to provide clear and accessible notifications about when their program is being deployed, whether or not notice is provided to individuals about the use of Azure AI Face seems to depend on the organization that adopts it. It is common practice for organizations to include User Agreements, opt-in agreements, or on-site signage for physical locations, much of which is dictated by the requirements of CCPA regulation. However, "invisible" uses like retail surveillance, crowd monitoring, online content moderation, and customer sentiment analysis make notifying affected people far more difficult.

Microsoft's AI facial recognition technology is known to be biased along both gendered and racial lines. The technology was found to perform best on lighter male faces, with an error rate of 0.0% compared to its worst performance in darker female faces, at 20.8%.[167] There is a disparity in error rate of 8.1% between men and female generally, with men being the better-detected sex. Lighter males have a 6% lower error rate than darker males, and lighter females have a 19.1% lower error rate than darker females. Microsoft no longer allows the use of its AI facial recognition technology by police forces in an attempt to avoid bias. Other systems of policy enforcement like retail and security systems, however, are not barred from its use. Facial recognition is commonly deployed in stores as customer identification, security, and tracking customer satisfaction.[168] These permitted uses disproportionately put female and darker-skinned individuals at risk of being misidentified for crimes committed in stores such as shoplifting, perpetuating racial profiling. Additional concerns arise in the use of facial recognition technology in airports for similar reasons.[169] Misidentification risks rise significantly for Asian and Black people in comparison to those who are white.

11. **NaviHealth**

NaviHealth Predict evaluates claims for post-acute care, which includes stays in skilled nursing facilities and in-home care, and determines what care is medically necessary to approve or deny the claims.[170] UnitedHealth uses this technology on its own patients and contracts out the algorithm for use by other insurers.

---

[166] Azure AI services, *What Is the Azure Ai Face Service?*, Microsoft Learn, https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-identity. Accessed January 5, 2025.
[167] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* 81 Proceedings of Machine Learning Research 77 (2018).
[168] Conal McCurry and Lauren Baldwin. *Facial Recognition: Balancing Security and Privacy in the Retail Sector*, WTW (April 2, 2024). https://www.wtwco.com/en-us/insights/2024/04/facial-recognition-balancing-security-and-privacy-in-the-retail-sector.
[169] Lisa Marshall, *Why New Facial-Recognition Airport Screenings Are Raising Concerns,* CU Boulder Today (July 11, 2023), https://www.colorado.edu/today/2023/07/11/why-new-facial-recognition-airport-screenings-are-raising-concerns.
[170] Willis Ryder Arnold & Meghna Chakrabarti, *How Insurance Companies Use AI to Deny Claims*, WBUR (Dec. 18, 2024) https://www.wbur.org/onpoint/2024/12/18/unitedhealth-ai-insurance-claims-healthcare.

It is not clear that patients understand that an algorithm is evaluating their claims, and it is difficult to find information on nH Predict on Optum or United Health's website. This technology causes harm because post-acute care is expensive and wrongfully denied claims burden patients and families.[171] While a case manager does sign off on the algorithm, there is the potential harm caused by automation bias.

12. **Cigna**

Cigna uses the PxDx algorithm to analyze and deny claims in bulk before forwarding them to physician reviewers for final approval.[172] The Cigna review system does not allow medical directors to see patient records before final judgment. Instead, the company doctors sign off on the denials in batches.

Cigna does have information about PxDx on their website where it says it uses PxDx for only 50 low-cost tests and procedures and that it is a simple sorting technology. However, it is unclear how many claims are approved and how many are funneled to doctors for denial. This algorithm can cause harm by wrongfully denying claims, which inflicts enormous burdens on patients and their families.[173] While a doctor or case manager does sign off on the algorithm, there is the potential harm caused by automation bias.

13. **Blue Shield of California**

Claims Data Activator (CDA) is an artificial intelligence (AI) tool designed to streamline the prior authorization process by analyzing claims data to determine medical necessity and expedite decision-making. Prior authorization refers to the process by which a healthcare provider or patient must obtain approval from the insurance company before specific medical treatments, medications, or procedures are provided or covered. This process ensures that the proposed healthcare service is deemed medically necessary and falls under the patient's insurance coverage plan. This automation allegedly allowed Blue Shield to deny certain claims automatically if they did not meet preset criteria.

Blue Shield of California has not publicly announced the adoption of ADMT or CDA on its website. This technology harms consumers as it denies them proper medical care.[174] In a class action litigation against Blue Shield in Alameda Superior Court on March 28, 2024, Plaintiffs allege that Blue Shield operates CDA to instantly reject claims "on the lack of medical necessity grounds, despite a patient's doctor providing documentation as to why medical treatment is medically necessary, and without ever opening patient files."[175] Plaintiffs also allege that this ADMT "enable doctors to automatically deny

---

[171] *Estate of Lokken v. United Healthcare*, Complaint (D. Minn. 0:23-cv-03514) (filed Nov. 14, 2023), https://fingfx.thomsonreuters.com/gfx/legaldocs/lbvgoerodvq/Lokken%20v%20UnitedHealth%20complaint%2011-14.pdf.
[172] Patrick Rucker, Maya Miller, and David Armstrong, *How Cigna Saves Millions by Having Its Doctors Reject Claims without Reading Them*, ProPublica (Mar. 25, 2023), https://www.propublica.org/article/cigna-pxdx-medical-health-insurance-rejection-claims.
[173] *Kisting-Leung v. Cigna*, Complaint (E.D. Cal. 2:23-at-00698) (filed Jul. 24, 2023), https://www.documentcloud.org/documents/23886255-cigna-pxdx-complaint/.
[174] *Jong v. Blue Shield of California*, Complaint (Cal. Sup. Ct. no. 24CV069627) (filed Mar. 28, 2024), https://www.fmglaw.com/wp-content/uploads/2024/04/Jong-v.-Blue-Shield-of-CA-Superior-Court-CA-Alameda-Complaint.pdf.
[175] Freeman Mathis & Gary LLP, *AI Class Action Knocks on California Court's Door* (April 10, 2024), https://www.fmglaw.com/cyber-privacy-security/ai-class-action-knocks-on-california-courts-door/.

coverage en masse for treatments, medications, and testing that do not match a certain preset criteria." According to the complaint, "Nearly 1 in 5 insured adults experienced a denied claim in the past year and with 85% of consumers not filing a formal appeal to their denial." CDA aligns with the CPPA's proposed definition, set to be codified at § 7001(f) and Article 11, as it processes the insureds' personal information—such as medical records—and employs computational methods to make decisions regarding whether the insureds pass the prior authorization. In this context, the algorithm fully replaces or substantially facilitates human decision-making. Once CDA determines that such tests and procedures are not medically accepted or necessary, Blue Shield's doctors sign off on the denials without reviewing the insureds' files or the documentation provided by the insureds' healthcare provider.

14. **Kaiser's AI: Advance Alert Monitor**

Kaiser Permanente's Advance Alert Monitor ADMT uses AI and helps prevent emergencies in the hospital before they happen.[176] Every hour, the program automatically analyzes hospital patients' electronic health data.[177] If the program identifies a patient at risk of serious decline, it sends an alert to a specialized virtual quality nursing team. The nursing team reviews the data to determine what level of on-site intervention is needed. To predict which patients are likely to decline — meaning they might soon need emergency resuscitation or need to be transferred to the intensive care unit — the program uses a powerful analytical engine that considers many patient factors. These factors include laboratory test results and vital signs, such as heart rate, blood pressure, and body temperature.

It appears that the only notice provided is to the doctor and not the patients. The issue with using this AI program to review laboratory test results or vital signs is that it is analyzed against certain average numbers that may not adequately account for unique variations such as racial and ethnic nuances. This has led to false alerts.[178] This technology fits within the definition of ADMT under § 7001(f)(1) and (2) because it leverages machine learning models to deem which vital signs are abnormal so the program can provide some early warning alerts and also "substantially facilitates human decisionmaking" because nurses and doctors use the ADMT's output to determine emergency prevention.

15. **Viz.AI**

Viz.ai, a San Francisco-based company, uses an ADMT algorithm to detect suspected diseases, such as strokes, by analyzing patient data like CT scans.[179] The technology aims to accelerate diagnosis and treatment for patients, reducing detection time and alerting doctors faster when higher care is needed.

Viz.Ai has 13 FDA-approved algorithms and is used by over 1500+ US and European hospitals. However, it is unclear whether the hospital gives patients explicit notice that the physicians utilize Viz.AI in disease detection.

---

[176] Daniel Yang, *Fostering Responsible AI in Health Care*, Kaiser Permanente (Mar. 19, 2024), https://about.kaiserpermanente.org/news/fostering-responsible-ai-in-health-care.
[177] Kaiser Permanente, *Behind-the-Scenes Alert System 'Another Set of Eyes'* (Jan. 14, 2022), https://about.kaiserpermanente.org/health-and-wellness/our-care/behind-the-scenes-alert-system-another-set-of-eyes.
[178] Garrett Leahy & George Kelly, *'Trust Nurses, Not Ai': Workers Protest Use of Artificial Intelligence at Kaiser Hospitals*, San Francisco Standard (Apr. 23, 2024), https://sfstandard.com/2024/04/22/kaiser-nurses-protest-ai-san-francisco/.
[179] Viz.ai, *AI-Powered Care Coordination* (Nov. 20, 2024), https://www.viz.ai/.

A harmful risk of Viz.ai's technology is that its algorithms may fail to detect diseases with atypical symptoms, leading to these patients being deprioritized in the diagnostic process. This could result in delayed treatment or missed opportunities for care. Algorithmic errors may also lead to misdiagnoses. Further, there are concerns about the security of sensitive patient data, and the cloud of patient data created by Viz.Ai may create a risk of data breaches. Viz.Ai does have an online "Trust Center," where it explains its data security measures.

16. **Amazon (Surveillance)**

Amazon created an AI tool that reviewed job applicants' resumes.[180] However, it showed a bias against women because the computer model was trained by observing patterns in resumes submitted to the company, which mostly came from men. The algorithm penalized resumes that included the word "women" and downgraded graduates from all-women's colleges.

There was no notice provided regarding the use of this algorithm. Additionally, it is not clear that the algorithm was used in hiring. This technology is harmful because it encourages clear biases against women in the hiring phase. It also could lead to biases associated with sex, age, race, and other protected classes. Amazon's AI tool follows the CPPA's proposed regulation because it replaces the human decision-making that is involved with hiring because the formula is meant to weed out the resumes that are most likely to succeed or do well in the job position.

17. **HireVue**

HireVue is an HR company that provides digital hiring platforms, including AI-driven video interviews, to clients who are typically large employers.[181] Clients use HireVue's platforms to increase efficiency in the recruiting process, enabling job candidates to record video interviews with responses to AI-generated questions, instead of interviewing with a human job recruiter. HireVue then utilizes individualized algorithms to evaluate candidates based on the criteria set by the employers and make hiring decisions. HireVue claims most companies use its platform as a convenient first step to screen candidates, to replace initial phone interviews and multiple-choice assessments.

In terms of providing notice, HireVue has relevant FAQ sections and articles on its website.[182] Candidates are aware an ADMT is analyzing them, but not aware of what they are being analyzed based on. HireVue claims it evaluates candidates' answers for "skills and competencies" through "situational judgment questions," "scenario-based simulations" and "past behavior questions." However, the FAQs and articles are relatively vague and do not explicitly explain how HireVue's technology works, the algorithm it uses, or how the company measures "skills" or "competencies" and makes hiring decisions. It is unclear how the algorithms work, or what they look for.

---

[180] 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/.

[181] Hirevue, *Companies Using HireVue, Market Share, Customers and Competitors*, https://discovery.hgdata.com/product/hirevue. Accessed January 5, 2025.

[182] Hirevue, *FAQ: Frequently Asked Questions for Candidates*, https://www.hirevue.com/candidates/faq. Accessed January 5, 2025.

HireVue claims its algorithm mitigates hiring bias by focusing exclusively on competencies and skills, and supports DEI efforts–including improving the fairness in hiring of neurodivergent individuals—but extensive criticism of HireVue's one-sided interview process suggests otherwise.[183] Users describe the platform as uncomfortable, impersonal, and unfair, noting that HireVue may decrease the interview performance of candidates and prevent job candidates from gaining insight into the company.[184] Many also express concerns about transparency, questioning who views the interviews, how the video interview data is used, and the workings of HireVue's algorithm. Without clear disclosures, some argue the platform may perpetuate bias rather than reduce it. The company cites credibility from conducting over 70 million interviews, and claims to have used such interviews to build its models. However, this suggests that interviewee data is collected and used to refine HireVue's platform, raising concerns about the monetization of personal data. HireVue claims to store candidates' personal data according to retention periods set by hiring companies. HireVue claims to place liability of holding the data on the companies, which it refers to as the "controllers of interview data," and says candidates can request data deletion. This policy minimizes HireVue's liability in terms of data misusage but creates uncertainty for applicants. Deletion requests may send a negative impression to employers, and it remains unclear if these requests are consistently honored or what happens to the data in the meantime.

Though HireVue is not based in California, 174 California-based companies utilize HireVue in making hiring decisions, significantly affecting CA workers.

18. **Workday**

Workday's AI is used to screen job applicants by analyzing personality traits and other factors through tools like pymetrics. A lawsuit alleges that this AI-driven system disproportionately rejects candidates based on their race, age, and disability.[185] The AI is accused of using biased training data, which leads to discriminatory outcomes.[186] Therefore, the AI's action is to filter out candidates using algorithms that may inadvertently favor certain demographics over others, causing unfair rejections.

Workday does provide a data privacy and framework notice, a cookies notice, and a work privacy statement. They state that they are in compliance with the Data Privacy Framework program. The technology causes harm, as the AI disproportionately weeds out candidates on factors other than qualifications, such as race, age, or disability, and likely profiles candidates by analyzing their personal

---

[183] u/Beginning_Biscotti94, *I genuinely hate Hirevue with a passion*, Reddit, r/recruitinghell (4 years ago), https://www.reddit.com/r/recruitinghell/comments/mkw8fi/i_genuinely_hate_hirevue_with_a_passion/. Accessed January 6, 2025.

[184] u/workersrights2021, *Fuck Hirevue and Any Company That Makes Candidates Do It. Here Is How You You Can See Your Questions Ahead of Time*, Reddit, r/Recruitinghell (4 years ago), https://www.reddit.com/r/recruitinghell/comments/kd1q4w/fuck_hirevue_and_any_company_that_makes/. Accessed January 6, 2025.

[185] Maria Dinzeo, *Lawsuit against HR Platform Accused of Bias in AI Screening Tool*, benefitspro.com (July 19, 2024), https://www.benefitspro.com/2024/07/19/novel-suit-calling-workdays-ai-driven-hiring-tool-biased-advances-setting-up-precedent-setting-showdown-412-171812/?slreturn=20241231152629v.

[186] Laura Malugade, Owen Davis, and Keith Ybanez, *California Court Finds That HR Vendors Using Artificial Intelligence Can Be Liable for Discrimination Claims from Their Customers' Job Applicants*, Labor and Employment Law Insights (Aug. 14, 2024), https://www.laborandemploymentlawinsights.com/2024/08/california-court-finds-that-hr-vendors-using-artificial-intelligence-can-be-liable-for-discrimination-claims-from-their-customers-job-applicants/.

traits. This AI tool aligns with the CPPA's proposed definition given that it likely evaluates the collected data and uses algorithms to decide whether an applicant should move forward in the hiring process.

19. **Uber**

Uber's algorithm calculates drivers' earnings by analyzing several key factors, though not all are disclosed publicly.[187] Known factors include trip distance and duration, location, demand-supply dynamics, driver preferences, and surge pricing.[188] Driver preferences, which encompass privacy data such as their acceptance rates, driving patterns, and past behaviors, are used to match rides and determine optimal pay.

Although Uber briefly explains "Upfront Price" in its FAQ section, the specific factors and data inputs used to calculate these fares remain undisclosed. Uber does not provide workers with clear information on how their data is used in the context of dynamic and upfront pricing. This lack of transparency has raised concerns among drivers about potential earnings reductions and the fairness of the compensation system.

1. Reduced Earnings and Lack of Pay Transparency
   Drivers face reduced earnings and limited transparency regarding their pay. Uber does not disclose how pay is calculated or how drivers' behavioral data influences decisions. Critics argue that the algorithm personalizes pay and task allocation in ways that may unfairly discriminate between drivers. This lack of clarity can result in pay reductions without adequate explanation or justification.

2. Loss of Control Over Work
   Uber's ADMT system uses drivers' behavioral patterns to subtly influence their actions, such as presenting specific trip options or offering bonuses to encourage longer hours. Factors like ride acceptance rates and driving behaviors can affect access to high-demand trips or incentives, effectively pressuring drivers to align with Uber's preferences, often at the cost of their autonomy.

Uber's algorithm aligns with the CPPA's proposed definition, set to be codified at § 7001(f) and Article 11, as it processes drivers' personal information—such as driving patterns and preferences—and employs computational methods to make decisions, including determining drivers' earnings.[189] In this context, the algorithm fully replaces or substantially facilitates human decision-making.

20. **Amazon (Surveillance)**

The AI enables employers like Amazon to continuously monitor workers via unregulated and algorithmically processed video and audio recordings. This level of surveillance allows employers to

---

[187] Dara Kerr, *Secretive Algorithm Will Now Determine Uber Driver Pay in Many Cities*, Markup (Mar. 01, 2022), https://themarkup.org/working-for-an-algorithm/2022/03/01/secretive-algorithm-will-now-determine-uber-driver-pay-in-many-cities.

[188] Uber, *How Are Fares Calculated?*, Uber Support & Customer Service, https://help.uber.com/riders/article/how-are-fares-calculated/?constructor=f2a7ee&nodeId=d2d43bbc-f4bb-4882-b8bb-4bd8acf03a9d. Accessed January 6, 2025.

[189] Sebastian Klovig Skelton, *Uber CEO Denies Pricing Algorithm Uses 'Behavioural Patterns'*, Computer Weekly (Feb. 20, 2024), https://www.computerweekly.com/news/366570421/Uber-CEO-admits-pricing-algorithm-uses-behavioural-patterns.

track and control worker activities in real-time and enforce discipline at a scale that would be impossible for human managers.[190]

There was no notice provided by Amazon. Amazon reportedly used advanced tracking tools, including its "Spocs" (supply chain optimization technologies), to monitor unionization efforts and labor organizing activities among employees.[191] Internal documents revealed Amazon's close surveillance of workers. The AI mainly affects Amazon employees, but more specifically, those with disabilities or injuries who may be unable to meet AI-determined work standards. This is harmful because the AI processes worker activity data to inform decisions such as productivity assessment or disciplinary actions, directly influencing management decisions. A label of "underperformance" has negative consequences for employees.

21. **Pearson's Automated Scoring Systems**

Pearson's Automated Scoring Systems are AI-powered tools designed to evaluate and grade written responses, such as essays and open-ended test answers.[192] These systems use natural language processing (NLP) and machine learning to assess grammar, content relevance, coherence, and critical thinking.

Pearson does provide notice as well as a detailed description of the product on their website. However, Person's automated scoring system may be biased and not understand certain creative nuances. For example, the technology may be biased against certain slang words or linguistic differences across varying geographic regions. In combination with the complete removal of human oversight, this system can lead to profiling candidates based on their writing stylistics or any personal information they divulge in their writing.

22. **Affirm**

Affirm addresses the needs of both customers and merchants by offering different payment options to customers and adjusting their terms to suit a merchant's goods or services.[193] Merchants leverage Adaptive Checkout, which uses Affirm's smart decision engine to deliver personalized payment options based on transaction size and real-time underwriting decisions.[194] For customers, Affirm also individually determines their purchasing power based on machine learning models and customer data.

---

[190] Michael Sainato, *'You Feel like You're in Prison': Workers Claim Amazon's Surveillance Violates Labor Law*, Guardian (May 21, 2024), https://www.theguardian.com/us-news/article/2024/may/21/amazon-surveillance-lawsuit-union.
[191] Jason Del Rey & Shirin Ghaffary. *Leaked: Confidential Amazon Memo Reveals New Software to Track Unions*, Vox (Oct. 6, 2020), https://www.vox.com/recode/2020/10/6/21502639/amazon-union-busting-tracking-memo-spoc.
[192] Pearson Assessments, *Large Scale Educational Assessment, Scoring, and Reporting*, https://www.pearsonassessments.com/large-scale-assessments/k-12-large-scale-assessments/automated-scoring.html. Accessed January 5, 2025.
[193] Melissa Daniels, *Exclusive: Affirm Revamps Its App to Spur Holiday Spending*, Modern Retail (Oct. 31, 2024), https://www.modernretail.co/technology/exclusive-affirm-revamps-its-app-to-spur-holiday-spending/.
[194] Affirm Holdings, Inc., *Affirm Launches Adaptive Checkout, Bringing Greater Choice and Flexibility to Merchants and Consumers* (Sept. 22, 2021), https://investors.affirm.com/news-releases/news-release-details/affirm-launches-adaptive-checkout.

Affirm gives notice to the investors and merchants who use Adaptive Checkout, but not to the customers on what data is being leveraged and how are the decisions being made. The only notice to customers is that Affirm determines purchasing power but does not clarify what signals or data points are used. This technology determines customer underwriting, credit decisioning, customer APRs, loan amounts and cart amounts for customers.[195] However, there is no insight into what factors are considered and could perpetuate and amplify biases based on ZIP code, race, and age, possibly based on the training data. Affirm also does not inform customers how they determine individual purchasing power. There is no oversight, so Affirm can only raise or reduce purchasing power to incentivize spending as needed.

23. **Yardi's Revenue IQ revenue management software**

Revenue IQ revenue management software (formerly RENTmaximizer) helps apartment owners and managers efficiently review and set options for pricing their rental units.[196] Apartment communities that use Revenue IQ have full and independent control of the Revenue IQ settings and their pricing decisions.

There does not seem to be notice to customers, but the main conflict occurs between the technology and property managers. In Washington, there is a lawsuit regarding price-collision to increase rent.[197] However, Yardi published the "logic" to placate the rising lawsuits of price-fixing.

Because property managers (competitors) delegate key aspects of their pricing to an algorithm, the algorithm can encourage and foster biased decision making in the price determination. Also, because the algorithm grows based on the data received from the property managers who are competitors, certain behaviors can easily be replicated across which can encourage the tool to recommend higher prices leading to rent inflation. This technology fits within the definition of ADMT under § 7001(f)(1) and (2) because it leverages machine learning models to determine price recommendations and also "substantially facilitates human decisionmaking" because property managers use the output of the technology as a key factor in determining rent prices.

---

[195] Affirm Holdings, Inc., *Affirm Products: Adaptive Checkout*, https://businesshub.affirm.com/hc/en-ca/articles/16322358615316-Affirm-Products-Adaptive-Checkout. Accessed January 6, 2025.
[196] Yardi, *How Revenue IQ Apartment Unit Pricing Works* (Aug. 19, 2024), https://www.yardi.com/news/legal-news/how-revenue-iq-apartment-unit-pricing-works/.
[197] Katie Arcieri & Justin Wise, *Yardi Ruling Boosts DOJ's Legal Theory in AI Price-Fixing Cases*, Bloomberg Law (Dec. 9, 2024) https://news.bloomberglaw.com/antitrust/yardi-ruling-boosts-dojs-legal-theory-in-ai-price-fixing-cases.