Assessing the Assessments

Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

About EPIC

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research advocacy center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for privacy, algorithmic fairness, and government accountability.

Author

Mayu Tobin-Miyaji, EPIC Law Fellow

Contributions by

John Davisson, Director of Litigation
Sara Geoghegan, Senior Counsel
Kara Williams, Law Fellow
Rebecca Downes, Executive Assistant

Acknowledgements

EPIC would like to thank the Rose Foundation for providing funding that supported our work on this project. Special thanks to Ben Winters and Grant Fergusson for their work in the initial stages of the project. Thank you to Dr. Gemma Galdón-Clavell, Swati Chintala, Samantha Gordon, Danielle Van Lier, Annette Bernhardt, and Dr. Jen King for participating in the public events that informed the project.

We also wish to thank our generous donors, who make our work possible as an independently funded organization.

Table of Contents

Introduction

The unchecked spread of commercial surveillance over the past several decades has led to a data privacy crisis for consumers in the U.S. and has allowed abusive data practices to flourish. The ability to monitor, profile, and target consumers on a mass scale has created a persistent power imbalance that robs individuals of their autonomy and privacy, stifles competition, and undermines democratic systems. And now more than ever, emerging generative and non-generative artificial intelligence systems are also causing harm.

The Electronic Privacy Information Center (EPIC) works to disrupt these data abuses and ensure that entities can no longer extract value from personal data in ways that undermine the public good. To that end, in 2023, EPIC launched a project on *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments*. California and other jurisdictions are increasingly adopting risk assessment requirements, and EPIC aims to ensure that those assessments serve genuine instruments of accountability.

In particular, the California Consumer Privacy Act (CCPA) creates legal rights and obligations that can address many of the harms inflicted by commercial surveillance, including a requirement to perform a risk assessment when personal information is being sold, when automated decisionmaking systems (ADSs) are being used in sensitive contexts, or when personal information is being used to train ADSs. The CCPA is one of the strongest comprehensive state privacy laws in the country and the only such law backed by a dedicated privacy protection agency. Ensuring the robustness of risk assessments required under the CCPA is therefore vital both to deterring exploitative data practices by businesses and to informing consumers about how their data is being processed.

The CCPA is one of the strongest comprehensive state privacy laws in the country and the only such law backed by a dedicated privacy protection agency. Ensuring the robustness of risk assessments required under the CCPA is therefore vital

both to deterring exploitative data practices by businesses and to informing consumers about how their data is being processed.

> “Ensuring the robustness of risk assessments required under the CCPA is therefore vital both to deterring exploitative data practices by businesses and to informing consumers about how their data is being processed.

With the support of the Rose Foundation for Communities and the Environment, EPIC has spent the past two years participating in the CPPA's relevant rulemaking processes, providing educational materials on risk assessments to the public, partnering with stakeholders to ensure that key voices are being heard, and developing this report. Through this project, we have sought to educate consumers and lift up best practices to both regulators and entities processing personal data.

One central focus of our project—the CPPA's adoption of risk assessment rules—has proceeded more slowly than anticipated; the agency is not expected to finalize such rules until later in 2025. This delay has led us to broaden the scope of our research, analysis, and advocacy beyond California. At the same time, it has underscored the outsized role that advocacy in California can play in the legislative landscape nationwide. For other organizations working in the digital privacy space, it is necessary to grasp the essential precedent being set in California. We have also come to better understand the problems that trade secrets protections will pose for the public disclosure of risk assessments. We have begun to develop new strategies to address these challenges and to account for them in the recommendations we make in California and beyond.

Risk assessments are a key accountability mechanism that can help ensure that businesses process personal data or use automated decision systems safely, responsibly, and in ways that minimize the risk of harm to individuals. Part I of this report provides a high-level survey of real-life privacy harms caused by the unrestricted collection and processing of personal information and the irresponsible use of automated decisionmaking systems. Part II discusses the need for robust transparency and accountability mechanisms to prevent and mitigate these

harms, including especially risk assessments. Part III discusses the components of an ideal risk assessment framework; the importance of making such assessments public; and the role of such assessments in broader landscape of privacy protections, algorithmic governance, and impact assessments. Part IV discusses the CCPA's risk assessments requirements and the CPPA's ongoing rulemaking process to develop risk assessment regulations. This includes an analysis of the diluted rules proposed by the Agency in May 2025 and responses to common arguments raised by Big Tech and industry lobbyists against robust regulation. Part V discusses why businesses should conduct thoroughgoing risk assessments as a best practice, even where not required by law, followed by a brief conclusion.

We hope that this report contains useful information for consumers, advocates, policymakers, and businesses that want to deepen their understanding of the risks that personal data processing and automated decisionmaking systems pose—and the ways that risk assessments can best address them.

Part I: Privacy Harms From Unchecked Processing of Data and Use of Automated Decision Systems

The opaque system of collection, sharing, retention, and use (which we refer to broadly as "processing") of consumers' personal data, including for use in automated decision systems, causes a wide array of privacy harms to individuals. In this section, we survey the real-life harms that such unrestricted processing of data can produce in various contexts, including physical, economic, reputational, psychological, autonomy, social stigmatization, discrimination, and relationship harms.[1]

In this report, the term "automated decision system" (ADS) refers to a computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decisionmaking and materially impacts natural persons.[2] It is important for the definition of ADS to be broad enough to capture systems that assist, rather than fully replace, human decisionmaking. Including situations where both humans and an ADS are involved in a decisionmaking process is essential because research shows humans tend to over-rely on automated systems.[3] A definition like this also ensures that humans are not added into the decisionmaking process merely to act as rubber stamps for automated decisions.

Building on top of the ubiquitous collection of data, automated decision systems (ADS) use personal data to automate decisionmaking processes that impact important aspects of Americans' lives, including access to housing, health care, education, employment, financial services, public benefits, and prices for everyday goods or services.[4]

a. The Harms of Commercial Surveillance

Consumers today face ubiquitous online tracking through the opaque collection, processing, and sale of their data, quantifying their life at every turn.[5] Commercial surveillance systems enable companies to collect and commodify every bit of consumers' personal data, including sensitive personal data.[6] To participate in today's economy is to have personal data extracted, aggregated, commercialized,

and sold—as individuals work,[7] eat,[8] pray,[9] study,[10] socialize,[11] browse the internet,[12] seek medical care,[13] plan families,[14] educate children,[15] exercise political freedoms,[16] or simply move about the world.[17]

> “To participate in today’s economy is to have personal data extracted, aggregated, commercialized, and sold—as individuals work, eat, pray, study, socialize, browse the internet, seek medical care, plan families, educate children, exercise political freedoms, or simply move about the world.

Unregulated processing of personal information allows businesses to use personal information that consumers shared with the business for a particular purpose for unrelated, out-of-context uses, fueling the commercial surveillance industry.[18] Businesses routinely process or sell personal information about individuals without their consent in ways the individual did not anticipate, undermining their autonomy and control over their personal information.[19] The processing of personal data for purposes inconsistent with the context in which the data was initially collected from the consumer is a violation of “contextual integrity,”[20] depriving the individual of autonomy and control over their data and knowledge that businesses have about them.[21] Such detailed knowledge about consumers allows businesses to exploit consumers’ vulnerabilities, interests, or associations to sell products.

The aggregation of sensitive personal data into detailed profiles of individual consumers exposes consumers to ever-increasing privacy risks.[22] Data breaches can disclose sensitive personal information. There has been no shortage of high-profile data breaches in the news,[23] including Davita, a dialysis firm whose breach exposed sensitive medical information of hundreds of thousands of kidney disease patients;[24] PowerSchool, an edtech giant whose personal data of students and teachers was compromised by hackers and was extorted into paying ransom;[25] and Hertz, which exposed personal information and driver’s license information of its customers.[26] Data breaches facilitate identity theft, which imposes economic costs to victims to discover and remedy the identity theft and costs billions to the U.S. economy.[27] Nefarious actors can also use breached personal information to stalk, harass, dox, or harm individuals by disclosing their home address, employer, phone numbers, and sensitive or damaging information.[28]

Further, the mass overcollection and sale of consumers' personal information increasingly intertwine with the risks of law enforcement purchasing or otherwise gaining access to large swaths of personal information on individuals without having to obtain a warrant or go through another proper legal channel.[29] This allows for targeting of marginalized or vulnerable communities including immigrants,[30] pregnant people and doctors providing abortion care,[31] LGBTQ+ individuals,[32] and individuals engaging in First Amendment-protected activity.[33] Disclosure, or the prospect of disclosure, of sensitive information can thus threaten physical, reputational, and psychological harms.[34]

b. Behavioral Advertising and Surveillance Pricing

Much of the sweeping data collection that characterizes commercial surveillance feeds into behavioral advertising, which relies on ADSs to function.[35] Behavioral advertising allows advertisers to determine who should be targeted with economic opportunities based on detailed profiles of individuals.[36] For example, news reports have shown that advertisers use characteristics like race, gender, income, or proxies like ZIP codes, to filter and target certain audience segments for advertisements for employment,[37] housing,[38] and educational opportunities.[39] This discriminatory advertising can harm marginalized communities by reinforcing and perpetuating inequities in economic opportunities based on protected characteristics.[40]

"Behavioral advertising allows advertisers to determine who should be targeted with economic opportunities based on detailed profiles of individuals.

Beyond discriminatory advertising, advertisers can infer and target specific individual sensitivities and vulnerabilities to increase clicks and sales.[41] Advertisers target consumers based on statuses including mental and physical health conditions,[42] medical conditions (including pregnancy and addiction),[43] financial instability,[44] bereavement,[45] and unhealthy body stigma.[46] Credit agencies label individuals with categories like "Struggling Elders,"

"Credit agencies label individuals with categories like "Struggling Elders," "Tough Times," and "retiring on empty."

"Tough Times," and "retiring on empty."[47] Armed with profiles of consumers, advertisers can target products that exploit this information asymmetry. For example, payday loan companies target young people in need of cash, who may not understand the consequences of high-interest loans.[48] Anti-abortion groups advertised to people potentially seeking abortions through device locations at or near clinics providing abortion care to send misleading ads for anti-abortion "crisis pregnancy centers."[49]

In addition to targeting advertisements, businesses also use consumer personal information in surveillance pricing to tailor prices to individuals.[50] For example, journalists found that Target charged $100 more for a TV on its app when the consumer was near a Target store versus farther away,[51] Orbitz inferred that Mac users spent more on hotels, steering them to more expensive options,[52] and hotel booking sites charged different prices for the same hotel rooms based on the consumer's location, leading to a difference of more than $500 in one case.[53] Surveillance pricing can allow retailers to take advantage of inferences about consumers' willingness to pay more while keeping them in the dark about lower prices offered to others.

c. The Harms from Automated Decision Systems Are Proliferating Across Industries

Building on top of the ubiquitous collection of data, automated decision systems (ADS) use personal data to automate decisionmaking processes that impact important aspects of everyday people's lives.[54] These systems disproportionately affect marginalized communities; a TechTonic Justice report estimates that virtually all 92 million low-income people in the U.S. have basic aspect of their lives decided by ADS.[55] Despite promises that algorithmic systems can be objective, there is ample evidence that they exert power in ways that replicate past discrimination and prejudices while obfuscating the inner workings under a veil of "objective" algorithms, avoiding accountability.[56] While it is often difficult

"These systems disproportionately affect marginalized communities; a TechTonic Justice report estimates that virtually all 92 million low-income people in the U.S. have basic aspect of their lives decided by ADS.

for individuals to identify the prevalence of algorithmic discrimination and unfair or arbitrary decisionmaking from ADS, there is abundant evidence that both occur across various contexts and cause serious consequences on the wellbeing of everyday people.

1. Employment

Employers can use ADSs at numerous points throughout the employment process: determining which candidates see the job posting and who is interviewed and hired; deciding pay and benefits; evaluating employee performance; assessing employee emotion and sentiment; surveilling employees for unionization efforts; scheduling for shifts; and making demotion, suspension, or termination decisions.[57] The increasing use of ADSs is directly harming workers, disproportionately impacting people of color, women, and immigrants, and worsening their working conditions, hours, pay, and job security. [58]

"The increasing use of ADSs is directly harming workers, disproportionately impacting people of color, women, and immigrants, and worsening their working conditions, hours, pay, and job security.

These systems may screen out candidates based on data that relates to their membership within protected classes (such as age, gender, race, or disability data), creating increased risks of bias and discrimination.[59] This risk can arise from AI being trained on data that reflects historical discrimination or from employers relying on systems that perform worse for certain races, gender, disability, or accents, for example.[60] These systems often perpetuate bias even when the company using them is not intending to discriminate. In one particularly egregious case, an Indigenous and Deaf woman was forced to use HireVue's video interview system that uses automated speech recognition systems to generate transcripts of applicants' spoken responses in video interviews.[61] She was rejected for the position and received feedback directing her to improve her oral communication skills, in an apparent violation of federal and state antidiscrimination laws and the Americans with Disabilities Act.[62]

Employers' increasing use of technologies that track, assess, and evaluate workers— including by tracking time spent completing tasks, web browsing, messages

between coworkers, duration of meetings, keystroke frequencies, and even biometric data—undermines employee privacy and causes harm.[63] For example, unfettered use of productivity management systems is pushing warehouse workers to work at dangerous paces, increasing their chances of injury.[64] Examples of harm are seen in on-demand gig work, such as drivers and nurses, where workers are pressured to work longer for less pay, not take sick time off, not report safety incidents, and face arbitrary or unfair termination or suspension decisions without an effective means to appeal.[65] Surveilling and imposing algorithmic systems on employees causes unsafe working conditions, forces employees to focus on measured metrics that aren't necessary to do their jobs, threatens job security, undermines employees' ability to unionize, and creates psychological stress.[66]

2. Healthcare

Increasing reliance of healthcare providers on algorithmic recommendations, especially in complex diagnostic scenarios, contributes to misdiagnoses, incorrect treatment plans, and discriminatory treatment of patients.[67] For example, Epic Health Systems marketed an algorithm that can predict patients experiencing sepsis at 76-83% accuracy, but a later study of 27,000 patients found that the system was closer to 63% accuracy and produced many false positives while failing to identify risk in 67% of the patients that actually experienced sepsis.[68] In another example, a 2020 study found that an algorithm used in determining eligibility and prioritization for kidney transplants unfairly prevented Black patients from receiving transplants.[69] Racial bias has also been reported in models used in assessing whether a vaginal birth is safe for patients,[70] making diagnoses through chest X-rays,[71] and determining the level of patient need during triage.[72]

Use of ADSs in health insurance decisionmaking also leads to unfair or arbitrary denials, costing individuals money and putting patients' health at risk.[73] United Health used an algorithm to identify "outliers" in receiving mental health treatment to deny coverage to patients and harass mental healthcare providers to limit reimbursements.[74] Many major American health insurance companies contract with companies that use an algorithmic system to adjust the number of prior authorizations that will be reviewed, increasing the chances of delays and denials.[75] These uses of ADSs undermine fair treatment, dignity, autonomy, and health of patients.

3. Law Enforcement and Private Security Systems

Harms from using ADSs in law enforcement include discrimination, overpolicing, erroneous arrests, and surveillance of individuals engaging in First Amendment-protected activities. For example, predictive policing and recidivism prediction tools embed and reinforce historical data that reflects systematically racist policing practices.[76] The predictive policing system SoundThinking (formerly known as ShotSpotter) whose high rates of false positives leads to overpolicing of low-income and Black and brown neighborhoods, perpetuates bias, and endangers residents.[77] Law enforcement use of facial recognition systems, long criticized for higher error rates on non-white faces,[78] has led to wrongful arrests of numerous Black individuals.[79] New York Police Department deployed facial recognition technology to conduct mass surveillance of Black Lives Matter protesters in 2020[80] and the use of facial recognition technology to monitor pro-Palestine protestors also raise civil rights and civil liberties concerns.[81]

“ Law enforcement use of facial recognition systems, long criticized for higher error rates on non-white faces, has led to wrongful arrests of numerous Black individuals.

Increasing uses of facial recognition by businesses open to the public for “security” purposes present similar issues.[82] RiteAid used facial recognition technology that disproportionately falsely identified people of color as likely shoplifters.[83] Increasing adoption of facial recognition technology to identify patrons and potentially prevent entry create a private network of watchlists that individuals don’t know that they might be on and have no ability to appeal, while disproportionately impacting people of color and low-income people.[84]

4. Housing

In housing, ADSs impact tenant screening, mortgages, and applications for public housing, and reports show evidence of disproportionate denial rates and errors that have the greatest impacts on racial minorities and low-income people.[85] A survey of over 400 California landlords reported that almost two-thirds of the landlords received tenant screening reports containing an algorithmic score or recommendation, and that they often rely heavily on the score rather than

scrutinizing the underlying reports.[86] Renters, however, lack notice about what company is assessing their applications, whether an ADS is being used to assess them, and information about the underlying algorithm calculating the score or recommendation.[87] Tenant screening systems frequently introduce errors, and such errors can seriously hinder the applicant's ability to secure housing they can afford in a timely manner, disproportionately harming low-income people and people of color.[88] Algorithms used in making mortgage lending decisions also show racial disparities, rejecting mortgage applications by people of color at higher rates.[89]

> "A survey of over 400 California landlords reported that almost two-thirds of the landlords received tenant screening reports containing an algorithmic score or recommendation, and that they often rely heavily on the score rather than scrutinizing the underlying reports.

5. Education

Across many aspects of the education sector, students are scrutinized by various ADSs[90] that undermine their autonomy, dignity, and control over their sensitive information and private spaces, causing discriminatory outcomes, chilling their speech, and limiting educational information. Algorithms used to predict future student success when making enrollment or scholarship decisions were shown to produce less accurate results for Hispanic and Black students compared to white students.[91] Many schools monitor student activity on school-provided devices, including internet searches, social media posts, and private messages with friends to scan for signs of mental health emergencies.[92] The surveillance persists through all hours of the day, but efficacy of the systems is unproven.[93] Monitoring technology has put students at higher risk of interactions with law enforcement, outed LGBTQ+ students to administrators, eroded trust between students and teachers, and led to a chilling effect on

> "Monitoring technology has put students at higher risk of interactions with law enforcement, outed LGBTQ+ students to administrators, eroded trust between students and teachers, and led to a chilling effect on students' ability to express themselves.

students' ability to express themselves.[94] Content filtering systems on school devices disproportionately filter out content related to reproductive health, LGBTQ+ issues, and people of color that are relevant for classwork.[95] Proctoring remote provision of exams also come with a host of privacy issues,[96] including facial recognition systems that have higher errors for non-white students,[97] invading student privacy by requiring them to show their private living spaces,[98] and flagging disabled or neurodivergent students more often as suspicious of cheating.[99]

d. The Public Is Dissatisfied With This Reality

The public isn't happy with mass data collection, unchecked data use and abuse, and unregulated use of unproven, discriminatory ADSs. In a 2024 survey by Consumer Reports, nearly half of U.S. adults said that they would be "very uncomfortable" if AI programs had a role in the job interview process, and about 4 in 10 adults said they would be "very uncomfortable" if banks used an algorithmic decisionmaking system to determine whether applicants qualified for a loan or to evaluate potential tenants for an apartment, condo, or senior community. [100] Most Americans (83%) said that if an algorithm had been used to determine whether or not they would be interviewed for a job they applied for, they would want to know specifically what information the program used to make the decision.[101] More than 90% of Americans said that if any of these decisions made using an ADS were based on incorrect information that they would want the opportunity to correct this information.[102] Unfortunately, the reality is that these important decisions are already being made using ADSs, and without strong risk assessment requirements or ADS regulations,[103] individuals have no transparency into these systems or recourse if they are harmed. However, requiring entities that process personal data or use an ADS to conduct a thorough risk assessment would be a step toward resolving this information gap.

"Most Americans (83%) said that if an algorithm had been used to determine whether or not they would be interviewed for a job they applied for, they would want to know specifically what information the program used to make the decision.

Part II: Transparency and Accountability Through Risk Assessments

The processing of personal data imposes varying levels of risk to individuals, depending on the types of data and the context of such processing. Despite these risks, consumers are largely kept unaware of them by businesses that profit from such data processing. Further, deploying an ADS to make significant decisions about consumers provides businesses with a cloak of unwarranted rationality and neutrality that tends to hide its inner workings, making accountability for the resulting decisions difficult.[104] Consumers are often left unable to determine what data is collected, for what reason, how it is used (including whether an ADS was used), how decisions are made about them, and how to challenge such decisions.[105] Because ADSs can centralize biased data and assumptions and automate the decisionmaking process, they can expand the scale and frequency of erroneous and unfair outcomes, including discriminatory outcomes.[106]

> "[D]eploying an ADS to make significant decisions about consumers provides businesses with a cloak of unwarranted rationality and neutrality that tends to hide its inner workings, making accountability for the resulting decisions difficult.

For these reasons, it is past time in the United States for regulatory frameworks that provide consumers actionable transparency and meaningful accountability around data processing, especially with ADSs. One key aspect of transparency and accountability is mandating entities that process personal data or deploy ADSs to conduct risk assessments. Requiring businesses to conduct risk assessments before deploying any system that will process personal information, including an ADS, can change the calculus: businesses developing such systems will be incentivized to ensure their systems do not cause harm before selling or deploying them rather than waiting for harms to emerge after deployment.

Risk assessment requirements should work in tandem with other privacy-protective measures, such as data minimization, which EPIC has long advocated for.[107] Data minimization is the premise that entities should only collect and process personal data that is "reasonably necessary and proportionate" to provide or maintain a product or service requested by the individual consumer.[108] This standard better aligns business practices with what individuals expect from the interaction with

the business and limits the collection and processing of personal information to what is necessary for certain legally defined purposes, avoiding the excessive processing that often leads to privacy harms.[109] While data minimization is not the main focus of this report, a robust risk assessment requirement should require that (or be paired with a requirement that) businesses implement data minimization. This integration is discussed further in relevant sections.

Requiring businesses to conduct risk assessments is not a concept unique to data protection. Regulation of high-risk products, such as pharmaceuticals, provides a useful paradigm.[110] The development and approval process of bringing new drugs to market requires extensive testing, documentation, clinical trials, and a formal application to the U.S. Food and Drug Administration ("FDA"). If the FDA decides to move forward, an FDA review team evaluates all research to determine the drug's safety and efficacy balanced against any adverse effects before the drug many be approved. In addition to pharmaceutical companies' duty to ensure the drug is safe and effective for patients, they must provide deployers (prescribers) and consumers (patients) with clear information about appropriate usage and potential adverse effects. While risk assessments in a data protection context will not resemble the FDA process in every detail, that process provides a useful exemplar for putting the burden on those who develop a high-risk product to prove its safety and to provide key information to users through strong pre-deployment and notice requirements.

a. Risk Assessments Overview

A risk assessment (as we use the term here) is an analysis of how personal data will be collected, processed, transferred, or sold by an entity. When implemented properly, risk assessments force businesses to carefully evaluate and disclose the risks of planned data processing to affected consumers and the public at large—including risks associated with AI and automated decisionmaking. Conducting robust risk assessments supports thoughtful adoption of new data practices and risk mitigation procedures instead of allowing hasty deployment of new technologies without consideration of potential harms.[111] Further, a risk assessment can also provide regulators and the public with vital information about processing activities that may pose a threat to privacy and civil rights. Transparency can lead

to better-informed choices from consumers, robust enforcement of privacy rights, and incentives for companies to mitigate harms or terminate harmful systems.

Policymakers, advocates, and businesses often use terms such as "risk assessments," "impact assessments," and "audits" differently, sometimes in overlapping and interchangeable ways. We do not set out to delineate or define all of these terms here. However, one consistent goal of risk assessment requirements is to influence business decisions early and throughout the development and deployment of a system or a data practice, so it is essential that risk assessments are first conducted before those new systems or practices are deployed. In contrast, audits, which analyze the performance of a system against certain defined metrics, are often conducted after the system is developed. A robust transparency and accountability framework should include all of the above: pre-deployment risk assessments, regular updates to those assessments to account for relevant changes over time, and ongoing audits. Together, these mechanisms can ensure that a system continues to work as expected, that harms are detected in a timely manner, and issues are mitigated quickly.

One additional usage note: the term "risk assessment" is sometimes used to describe privacy impact assessments. A privacy impact assessment (or data protection impact assessment) is an analysis of how personally identifiable information will be collected, processed, stored, and transferred.[112] Privacy impact assessments (PIAs) are perhaps most closely associated with the E-Government Act of 2002, which requires federal agencies to identify and publicly disclose the information to be collected, why and for what purpose, with whom the information may be shared, the notice procedure, and how the information will be secured.[113] PIA obligations have been important in providing notice to the public of the new collection of information by federal agencies, and for civil society organizations like EPIC to ensure agencies assess the collection of personal information in their systems. Risk assessments like those required under the California Consumer Privacy Act go further than PIAs to incorporate elements focused on automated decisionmaking systems and weighing the benefits from processing against a broad spectrum of potential risks to the rights of the consumer.

b. Jurisdictions With Risk Assessment Requirements

Recognizing that the processing of personal data and the use of ADSs pose privacy and other risks to consumers, several jurisdictions have adopted risk assessment requirements and recommendations.[114] While Congress and federal regulators have not yet adopted risk assessment requirements for businesses generally, there are relevant federal guidelines for the procurement and use of automated systems. Additionally, some states have passed laws requiring risk assessments for both state and businesses that include provisions for which EPIC regularly advocates. Finally, some jurisdictions outside of the U.S. have also implemented risk assessment requirements for private and public entities.

1. Federal Frameworks

At the federal level, the White House Office of Science and Technology Policy's Blueprint for an AI Bill of Rights (2022) includes a variety of recommendations concerning AI accountability.[115] As relevant here, it recommends:

- "Independent evaluation and plain language reporting in the form of an algorithmic impact assessment, including disparity testing results and mitigation information, should be performed and made public whenever possible to confirm these protections;"[116] and
- "Systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring that demonstrate they are safe and effective based on their intended use, mitigation of unsafe outcomes including those beyond the intended use, and adherence to domain-specific standards."[117]

The AI Risk Management Framework, published by the National Institute of Standards and Technology (NIST), similarly recommends that entities:[118]

- Establish and regularly review documentation policies that, among others, address information related to: (1) AI actors contact information; (2) business justification; (3) scope and usages; (4) assumptions and limitations; (5) description and characterization of training data; (6) algorithmic methodology; (7) evaluated alternative approaches; (8) description of output data; (9) testing and validation results (including explanatory visualizations

and information); (10) down- and up-stream dependencies; (11) plans for deployment, monitoring, and change management; and (12) stakeholder engagement plans.

- Verify that impact assessment activities are appropriate to evaluate the potential negative impact of a system and how quickly a system changes, and that assessments are applied on a regular basis.
- Identify, document and remediate risks arising from AI system components and pre-trained models per organizational risk management procedures, and as part of third-party risk tracking.
- Respond to and document detected or reported negative impacts or issues in AI system performance and trustworthiness.

Lastly, the Office of Management and Budget (OMB) memos[119] that implement the Trump administration's AI executive order,[120] and their precursors under the Biden administration, contain risk assessment requirements for federal agencies' use of AI systems. The OMB memo currently in effect, M-25-21, classifies as "high-impact AI" AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on: (1) civil rights, civil liberties, or privacy; (2) access to education, housing, insurance, credit, employment, and other programs; (3) access to critical government resources or services; (4) human health and safety; (5) critical infrastructure or public safety; or (6) strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.[121]

Use of high-impact AI must comply with heightened risk management practices, including pre-deployment testing, AI impact assessments, and ongoing monitoring. Specifically, an impact assessment must include at a minimum:[122] (1) the intended purpose for the AI and its expected benefit; (2) the quality and appropriateness of the relevant data and model capability; (3) the potential impacts of AI, supported by documentation on potential impacts on the privacy, civil rights, and civil liberties of the public, and of using or not using AI; (4) reassessment scheduling and procedures; (5) related costs analysis; (6) results of independent review by an independent reviewer who was not involved in development; and (7) risk acceptance, supported by a signature from the individual accepting the risk. The Biden administration precursor to this OMB memo

also emphasized higher risk management, including conducting impact assessments, for rights- and safety-impacting AI.[123]

2. State Frameworks

At least 17 states—all states that have a data privacy law other than Iowa and Utah—require entities to conduct some aspects of a risk assessment if they are processing certain personal data or using an ADS.[124] In 15 of these states, the risk assessment (called "data protection assessment") requirements are largely the same because they are mandated through the states' privacy laws, which are all based on the same framework.[125] Unfortunately, the vast majority of these 15 privacy laws are broadly ineffective at protecting consumers' privacy,[126] and they fail to include many of the important aspects of effective risk assessments that are outlined later in this report, such as public access to the assessments. These 15 states—Maryland, New Jersey, Minnesota, Oregon, Delaware, Connecticut, New Hampshire, Montana, Rhode Island, Texas, Kentucky, Nebraska, Virginia, Indiana, and Tennessee—largely require only that entities weigh the benefits to the entity, consumers, other stakeholders, and the public against the risks to the consumer as mitigated by certain safeguards.[127] Even this extremely minimal assessment is required only if entities are processing data for a subset of risky activities, such as profiling consumers or engaging in targeted advertising, rather than (at a minimum) whenever they process sensitive personal data, as this report recommends.

However, the other two states with privacy laws containing risk assessment requirements, California and Colorado, have adopted more robust requirements. The California Consumer Privacy Act (CCPA) mandates that businesses conduct risk assessments covering the processing, use, benefits, and risks related to personal data.[128] The CCPA directs the California Privacy Protection Agency (CPPA) to promulgate regulations that clarify how businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security," should conduct and submit risk assessments to the Agency on a regular basis.[129] The CCPA requires the CPPA to publish information about risk assessments it receives, without specifying how much of the submitted risk assessments should be made public.[130] The CPPA's proposed regulations pertaining to risk assessments are explored further in Part IV.

Colorado has two laws that require entities to conduct risk assessments: the Colorado Privacy Act and the Colorado AI Act. The Colorado Privacy Act and accompanying Colorado Privacy Act Rules explain in detail what the law's "data protection assessments" require.[131] This law, like the other 15 states' laws discussed above, requires entities to conduct a data protection assessment when they engage in particularly risky forms of data processing. At minimum, entities' data protection assessments must include a summary of the processing activity; the categories of personal data that are processed and whether they include sensitive data; the context, nature, and operational elements of the processing activity; the purpose of the processing activity; the benefits to the entity, consumer, other stakeholders, and the public; the sources and nature of risks to the rights of consumers; measures and safeguards the entity will take to reduce these risks; a description of how the benefits outweigh the risks of the processing as mitigated by the safeguards; relevant actors who contributed to the data protection assessment; any audits conducted in relation to the data protection assessment; and dates, names, and signatures of those who reviewed and approved the data protection assessment.[132]

The Colorado AI Act, which was enacted in 2024 and is scheduled to go into effect in February, requires entities that use ADSs to make important decisions about Coloradans' lives to conduct an "impact assessment."[133] The law requires deployers to conduct an impact assessment if they deploy a high-risk AI system[134] to make a consequential decision[135] about a Coloradan.[136] Deployers must also conduct impact assessments annually and within 90 days of an intentional and substantial modification to the system.[137] At minimum, the impact assessment must include a statement of the purpose, intended use cases, deployment context of, and benefits afforded by the system; an analysis of whether the system poses any known or reasonably foreseeable risks of algorithmic discrimination; the nature of any risks of algorithmic discrimination and the steps taken to mitigate these risks; a description of the categories of data the system processes as inputs; the outputs the system produces; an overview of any categories of data the deployer used to customize the system; metrics used to evaluate the performance and known limitations of the system; a description of any transparency measures taken concerning the system; and a description of post-deployment monitoring

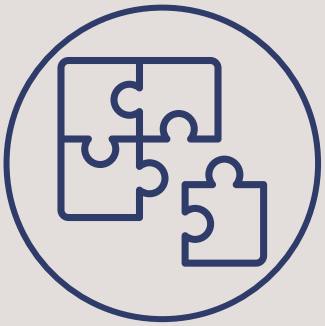
and user safeguards provided concerning the system.[138] The law also gives the Attorney General the authority to promulgate regulations about the requirements of the impact assessments.[139]

3. Frameworks Outside of the U.S.

Outside of the U.S., many jurisdictions have been more proactive in requiring impact assessments from private entities and government entities. The General Data Protection Regulation (GDPR), passed in the European Union in 2016, contains a data protection impact assessment requirement in Article 35.[140] When data processing is likely to result in "high risk" to the rights and freedoms of natural persons, the controller of personal data must conduct an assessment of the anticipated impact of the proposed processing of personal data.[141] The required assessment includes a description of the anticipated processing, the purposes for the processing, the necessity and proportionality of the processing operation in relation to the purposes (data minimization), and an assessment of the risks to the rights and freedoms of the data subjects.[142] The United Kingdom has a GDPR equivalent.[143] Brazil requires a data protection impact assessment that would assess the risks of data processing.[144] Singapore, China, Philippines, Vietnam, South Korea, and South Africa also require a form of data protection impact assessments.[145] Canada requires its government to conduct a mandatory risk assessment to determine the impact of automated decisionmaking systems used in the government and to comply with transparency requirements.[146]

As these jurisdictions illustrate, risk assessments are not a radical concept—if anything, they are a first and relatively noncontroversial step toward transparency and accountability for entities that process personal information. It is past time for any entity processing personal data to incorporate risk assessments into its business activities. Further, by complying with best practices like those laid out in this report, businesses can ensure that they are both in compliance with existing risk assessment requirements and well positioned to adapt when new requirements emerge.

"As these jurisdictions illustrate, risk assessments are not a radical concept—if anything, they are a first and relatively noncontroversial step toward transparency and accountability for entities that process personal information.

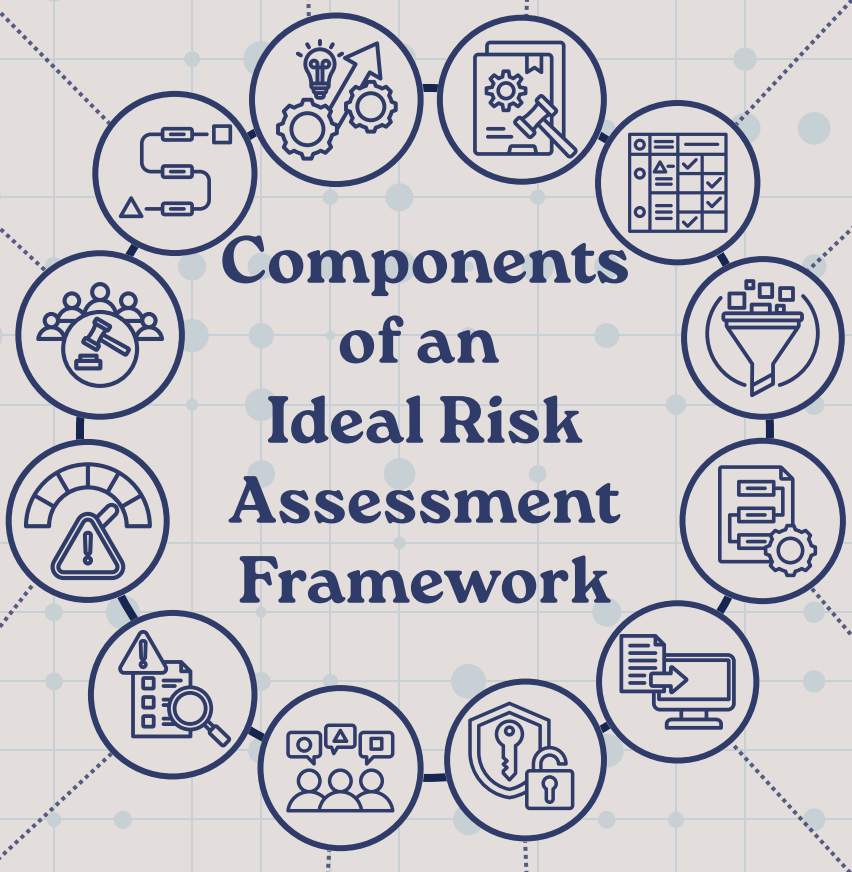


Part III: Components of an Ideal Risk Assessment Framework

This Part lays out EPIC's recommendations for an ideal risk assessment framework that would provide consumers with robust transparency and accountability. Because risk assessments are dependent on factors like processing context, system type, and the kinds of data an entity collects or processes, our recommended framework is intended to ensure flexibility for the assessment of a wide range of processing activities. While the inspiration for this report was the development of risk assessment requirements under the California Consumer Privacy Act, this Part is not limited to the California context.

As we set out in this section, the ideal risk assessment framework includes: (1) enforceable legal obligations that make such risk assessments mandatory; (2) a clear processing threshold that triggers a risk assessment requirement; (3) clear and broad definitions of covered entities; (4) requirement that an assessment be conducted before processing or ADS deployment; (5) mandatory routine submission of the risk assessment to a regulator; (6) public access to risk assessments; (7) broad stakeholder input into risk assessments; (8) clear and thorough substantive information that businesses are required to assess and disclose; (9) identification of methods of measuring privacy impacts; (10) qualified assessors with expertise and independence; and (11) identification of how harms are mitigated and compliance is ensured.[147] We conclude by highlighting several regulatory approaches that can complement risk assessments to strengthen consumer privacy.

Components of an Ideal Risk Assessment Framework



- Beyond Risk Assessments
- Enforceable Legal Obligations
- Robust Enforcement Mechanisms for Non-Compliance
- Clear Thresholds
- Assessors With Expertise and Independence
- Expansive Definition of Covered Entities
- Specified Methods for Measuring Privacy Impacts
- Pre-Deployment Risk Assessments
- Clear and Thorough Content Requirements
- Routine Submission to Regulators
- Broad Stakeholder Input
- Public Access

a. Enforceable Legal Obligations

Consumers cannot continue to rely on companies that process personal data or deploy automated decision systems to self-police their practices.[148] For years, individuals have been forced to rely on industry self-regulation as their only protection against abusive data practices, and requiring companies to conduct and publish risk assessments is a step toward rectifying this lack of protection. Without risk assessments, individuals who are impacted by unchecked collection of data remain in the dark about how their personal information is processed or fed to ADSs for use in decisions that significantly impact their lives. Few companies are voluntarily forthcoming in providing transparency or accountability to affected individuals. This lack of transparency and accountability creates an enormous power imbalance: entities collecting and processing data and deploying ADSs reap insights and profit from millions of data points, create extensive profiles of individuals, and automate life-altering decisions that were once left to human beings—all without the knowledge or understanding of those impacted.

One example of the shortcomings of corporate self-policing is HireVue.[149] HireVue uses an algorithmic system to assess job applicants, which has raised concerns of unfair and discriminatory hiring decisions.[150] Previously, HireVue's screening system relied in part on facial analysis of applicants as they answered questions in automated interviews.[151] In 2021, HireVue boasted that its algorithmic hiring system had undergone an audit by an independent auditor.[152] When the audit was finally made public, HireVue put significant restrictions on their publication.[153] Despite announcing that its audit showed that its software "does not harbor bias," HireVue soon after stopped including facial analysis in its standard offering.[154] Further, the audit was limited to a narrow use case and did not examine more controversial use cases that included facial analysis and employee performance predictions.[155] HireVue overstated the significance of the findings while putting substantial obstacles in the way of public access. Even now, key details about the algorithms the company uses to make judgments in the hiring process are kept secret from job applicants.

Jurisdictions should adopt legal frameworks that require risk assessments rather than relying on companies to voluntarily self-assess their data processing or ADS

use. Without the benefit of a legal or regulatory mandate, consumers have often been forced to rely on the limited capacity of journalists, academics, and advocates to investigate and publish details about companies' data abuse and ADS misuse. This includes, for example, ProPublica's work on an automated decisionmaking system used in the criminal justice system and in medical insurance claim processing;[156] *Gender Shades* by Joy Buolamwini, illuminating severe gender and skin-type bias in facial analysis technology;[157] and Virginia Eubanks' research on harms from automated government benefit systems in *Automating Inequality*.[158] While this work is tremendously valuable and a credit to its authors, it cannot function as the principal transparency and accountability mechanism for consumers against abusive commercial data practices. Risk assessments must be required by law.

b. Clear Thresholds

To provide robust protection for the privacy of consumers, the threshold that triggers the risk assessment obligation should be low to encompass more processing activities that may pose privacy risks. Laws and regulations should set clear thresholds for when a business must conduct a risk assessment. Thus, at minimum, the collection[159] or processing[160] of any sensitive personal data[161] and any use of ADSs should trigger a risk assessment obligation.

> "[A]t minimum, the collection or processing of any sensitive personal data and any use of ADSs should trigger a risk assessment obligation.

First, the collection of sensitive personal data—even in small quantities—is both an easily administrable threshold and one that reflects the inherent risk associated with obtaining and processing such data. Even some processing activities implicating solely non-sensitive personal information (or at least personal information that is not identifiably sensitive at the moment of collection) can pose privacy risks. Jurisdictions should consider adding risk assessment triggers keyed to high-risk processing activities. For example, as discussed later in this report,[162] California Privacy Protection Agency's proposed regulations on risk assessments includes "selling or sharing personal information." Inclusion of this trigger effectively covers

the riskiest processing regarding personal information without capturing all processing of personal information generally.

Second, any use of an ADS should trigger a risk assessment. High-risk applications—such as the use of automated decision systems with respect to a consumer; extensive commercial profiling for behavioral advertising and surveillance pricing; and profiling individuals in an educational setting, a workplace setting, or in spaces open to the public—should unquestionably trigger a risk assessment. As explained in Part I, these uses of ADSs can inflict particularly acute privacy harms, so businesses should conduct a thorough assessment before adopting such systems or practices. Risk assessments for an ADS should also include an assessment of both the collection and processing of personal information to train the underlying model, and separately, the collection and processing of personal information inputted into the ADS to profile or make a decision about a consumer.

c. Expansive Definition of Covered Entities

The duty to conduct a risk assessment should not generally depend on the revenue, size, or number of employees of the entity undertaking the processing or on any other factor unrelated to the data being processed.[163] A business's revenue often does not correlate with how many individuals' personal information it processes or the risks its processing poses to the consumer's privacy. [164] For example, businesses like data brokers may collect relatively little revenue yet build their business model on data processing that endangers the privacy of thousands or millions of consumers. Laws requiring risk assessments should also avoid exemptions for entire industries or classes of entities. In particular, nonprofits, institutions of higher education, healthcare entities covered by the Health Insurance Portability and Accountability Act (HIPAA), financial entities covered by the Gramm-Leach-Bliley Act (GLBA), should all generally be subject to risk assessment obligations to the extent that they process personal information. Further, an entity, including a small business, that is too

> "[A]n entity, including a small business, that is too undercapitalized to adequately safeguard consumer data should simply not be permitted to process it.

undercapitalized to adequately safeguard consumer data should simply not be permitted to process it.[165]

To the extent that small businesses may fear added compliance costs from risk assessment requirements, it is important to note that the risk assessments for smaller-scale and lower-risk processing activities will generally be much less burdensome to complete.[166] But a small business that engages in large-scale, hazardous processing of personal information should not be able to do so without the careful evaluation and mitigation necessitated by a risk assessment. For example, Clearview AI, notorious for its facial recognition tools built on images of individuals scraped from the internet with no consent and sold to law enforcement and other actors,[167] may be considered "small business" insofar as it only has about 35 employees.[168] Yet its data processing poses significant threats to consumer privacy, and its size should not exempt it from conducting risk assessments.

Additionally, risk assessment requirements should apply to both developers and deployers of ADS. Developers are the entities that design, create, maintain, modify, or update the ADS.[169] Deployers are the entities using the ADS, or offering it to the end user.[170] Developers and deployers may be the same party in some cases.[171] For example, in ACLU's case alleging discrimination using an ADS on behalf of a Deaf, Indigenous woman against HireVue and Intuit (referenced in Part I), the developer of the automated hiring system is HireVue, and the deployer is Intuit, which uses HireVue's system to conduct automated video interviews.[172]

Neither the deployer nor the developer should be able to circumvent the obligation to conduct a risk assessment by pointing to the other party as the one responsible for conducting risk assessments. Developers necessarily have the best view into what data and design decisions go into the system's creation and should assess the privacy risks associated with the uses the developer intends to make the system available for—as well as foreseeable other ways the system can be used or misused. However, every context in which a system is deployed presents different considerations, which makes it essential that individual deployers also conduct risk assessments specific to their own use. The risks arising from a particular use of an ADS may be different from what the developer's assessment foresaw or from the use of the same system in a different context. Further, the fit of the ADS

model's training data to the data of the population it may be used to assess or profile will be different in each deployment context, requiring a more tailored assessment.

Returning to an earlier example: HireVue should have conducted and published a full-scale risk assessment of the speech recognition technology used in its job applicant screening system to determine how the technology performed across various populations, including Deaf and Indigenous individuals. Had it done so, HireVue might have better understood that speech recognition technology is often unable to accurately recognize and analyze the speech of Deaf and non-white applicants, including Indigenous English speakers, whose differing speech patterns, word choices, and accents may therefore lead to a lower score.[173] HireVue could then have improved the quality of its system to mitigate the issue or decided that the risks of discrimination outweighed the benefits of using its ADS. Separately, Intuit should have conducted its own risk assessment covering its use HireVue's system, assessing factors like the system's fitness to assess applicants on relevant job qualifications free from discrimination, the system's use limitations, and the presence or absence of mechanisms for applicants to opt out of using the ADS. As this use case demonstrates, developers and deployers should each be responsible for conducting their own risk assessments.

d. Pre-Deployment Risk Assessments

Conducting a risk assessment is "a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project."[174] Thus, risk assessments should be done before and during development of a system that collects or processes personal information—before the system is deployed and when changes can still be made to the way the system will operate. The completed risk assessment should be submitted to the relevant forum (the public, the enforcing agency, or ideally both) a reasonable period of time before the system is deployed.[175]

However, transparency and accountability mechanisms should not stop at deployment. As the federal Office of Management and Budget has noted, a risk assessment "is not a time-restricted activity that is limited to a particular milestone or stage of the information system or [personally identifiable information (PII)] life

cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles."[176] After deployment, the system should be monitored, including for whether the risk assessment correctly assessed potential risks compared to real-world impacts. Risk assessments should also be paired with ongoing oversight, including audits, and new risk assessments should be conducted when material changes are to be made to the system. Material changes could include the collection or processing of a new category of information, the collection or processing the same personal data for a new purpose, changes in a data retention schedule, or updates to the ADS model.

e. Routine Submission to Regulators

The completed risk assessment should be submitted in full to an agency or government official who has legal authority to seek more information and evidence to support risk assessments, challenge assertions in risk assessments, and bring enforcement actions in the case of noncompliance. Covered entities should be required to affirmatively submit their required risk assessment materials to this regulator rather than placing the burden on the regulator to request these materials. This affirmative obligation to submit materials will incentivize entities to ensure they are both conducting their required risk assessments in a timely manner and conducting thorough assessments. Further, the same government body should be able to investigate, or work with other agencies to bring non-risk assessment-related enforcement actions, such as discrimination claims or unfair, deceptive, or abusive acts or practices claims that may stem from disclosures in the risk assessments. The regulator to whom the risk assessments are submitted should also be able to receive public input and complaints to inform its enforcement actions.

f. Public Access

Mandating that risk assessments be made public is one of the most powerful features of an effective risk assessment framework because it challenges the existing information asymmetry that surrounds privacy harms from processing personal information.[177] Public risk assessments should complement notices provided to individuals before personal information is collected or processed and before

individuals are subject to an ADS. While individual notices can provide consumers with some modicum of transparency, choice, and the ability to challenge an institution's processing of personal data or use of ADS, published risk assessments can provide a broader analysis of risks to a wider audience. Risk assessments should be made available to the public in a centralized, easily searchable database and disclosed to consumers in a conspicuous, accessible manner.[178]

"Risk assessments should be made available to the public in a centralized, easily searchable database and disclosed to consumers in a conspicuous, accessible manner.

It is important that risk assessments be made publicly available to reach interested parties who might not otherwise have access to such information. For example, researchers and advocacy organizations can use publicly available assessments to review business practices and challenge findings if necessary. By comparing risk assessments to each other with an expert eye, advocacy organizations can inform consumers of how entities that process their personal information stack up against each other and identify businesses that may not be in full compliance with their privacy and AI obligations. Further, companies, governments, and individuals that purchase products and services implicating personal data may benefit from comparing risk assessments to identify more privacy-protective options.[179]

The added visibility of a public risk assessment compared to one that is solely submitted to an enforcement agency would also provide a stronger incentive for the business conducting the risk assessment to take the process seriously. And public access can facilitate advocacy and debate concerning current and proposed privacy protections and AI safeguards.

Absent a requirement to make risk assessments public, covered entities may continue to avoid public scrutiny concerning their personal data practices, and the likelihood of risk assessments becoming a box-checking exercise will grow.[180] Policymakers, advocates, and the public at large will be less able to understand for themselves the information a business plans to collect or process, what purpose it will be used for, what privacy risks exist, and what steps the business has taken to

mitigate those risks. With no public access, the enforcing agency will bear the burden of combing through risk assessments itself, and enforcement will be further constrained by the budget, resources, and expertise of the agency.[181]

While the entirety of the risk assessments would ideally be made public, a robust public summary of the risk assessments can achieve the goals of transparency and accountability while allowing businesses to keep private information that could compromise trade secrets or system security. Robust summaries with plain language explanations can still inform consumers and the public, including advocates, and ensure that businesses take the time and effort to conduct the risk assessments seriously.[182] At the same time, allowing businesses to keep certain information non-public can encourage the business to honestly assess risks and mitigate issues. If a business is aware that all parts of a risk assessment will be made public, privacy risks that may reflect negatively on the business may not be surfaced and addressed thoroughly.

g. Broad Stakeholder Input

In conducting a risk assessment, the covered entity should seek input from communities that would be impacted by the system to understand potential harms and inform mitigation measures.[183] For example, if a business uses an ADS to make employees' schedules, the employees should be consulted when the business is conducting the risk assessment for that system. Requiring this type of consultation will ensure that businesses better grasp and are better positioned to address the ways that their data processing and ADS use can negatively impact consumers and other stakeholders. The Agency should also make it possible—ideally using the same searchable system through which risk assessments are disclosed—for members of the public to report concerns with published assessments and instances in which businesses appear to have violated statements made therein.

h. Clear and Thorough Content Requirements

With respect to the written content of risk assessments, EPIC recommends the following list of information be included:[184]

- What personal data the business collects or processes;

  Commentary: "Collects or processes" should cover all of the actions with regard to personal information that the business may take, including transferring, selling, retention, and deletion.[185]

- The sources of personal data the business collects or processes;
  - The method through which the data is collected;

  Commentary: I.e. directly from the consumer on a website, from connecting user's personal information with other identifying data to build a profile, through criminal background check, etc.

- The purpose(s) for which the business collects or processes each category of personal data;
  - Why the data is specifically necessary, proportionate, and appropriate to the purpose for which it is being collected or processed, including data processed in the design, development, training, testing, and operation of the system;

  Commentary: If the business's stated purpose is disclosing, selling, or otherwise making available personal information to other parties (to the extent that the jurisdiction's laws so permits), the business should explain that. Detailing why the collection or processing of the data is specifically necessary, proportionate, and appropriate for the stated purpose puts into practice the data minimization principle and forces the business to justify how it is complying with that principle.

- In what context the system will be deployed and how consumers will interact with the system;
- What categories of data the business will create, infer, or generate about consumers through the processing;
  - How such data will be used and for what purpose;
- Which third parties and service providers the business will make personal data available to, and for what purpose;
  - Whether making personal data available to such entities is necessary to provide the service the consumers requested and why;

- What notice or opportunities for consent will be provided to consumers concerning the entity's collection, processing, or disclosure of personal data to third parties;
    - Including notices of consumers' substantive privacy rights to access, correct, delete, opt-out, etc. if they exist in the jurisdiction and explanations of how to exercise such rights;
    - Including an explanation of how to revoke previously given consent, which must not be more burdensome than the process to provide consent;
- The benefits to the business, consumer, public, or other stakeholders that are likely to result from such collection, processing, retention, disclosure, or sale of personal data;
- The potential harms to the consumer or public that might result from such collection, processing, or sale of personal data:
    - Including, but not limited to: threats to data protection (unauthorized access, control, disclosure, or modification); inaccuracies; physical, economic, psychological, or reputational harms; loss of autonomy (coercion, exploiting vulnerabilities, dark patterns, uninformed consent); and discrimination (including disparate impact);
- Risk mitigation measures the business has implemented to address such potential privacy harms;
- Any alternatives to such collection, processing, retention, or transfer of personal information considered by the business and the reason(s) why such alternatives were rejected;
- How the asserted benefits resulting from such collection, processing, or sale to the business, the consumer, other stakeholders, or the public compare to the privacy risks to the consumer or the public; and
- Individuals with relevant qualifications who contributed to the risk assessment and approved it.

The risk assessment should also be accompanied by a plain language summary of the assessment that would be comprehensible to a reasonable consumer, which should be made publicly available.

Because the use of automated decision systems often presents heightened risks compared with other processing of personal data, businesses should be required to conduct additional evaluations of the potential risks before using these systems. These additional criteria should be evaluated on top of the business's traditional risk assessment.

Additional requirements for ADS risk assessments should include:

- A detailed description of the intended purpose and proposed use of the system, including:
  - What decision(s) the system will make or support;

    Commentary: For example, a score and a suggestion to the landlord whether a rental apartment applicant should be accepted or denied.

  - How the system is used to make decision(s), including the amount of human oversight, discretion, or lack thereof in the decisionmaking process;
    - How humans using the system will be trained;
  - Input(s) of the system and how those inputs are relevant to the decision being made;

    Commentary: For example, for a rental application ADS, inputs can include employment status, income, credit score, and a background check information.

  - The source(s) of the input(s) to the system and the means through which the input(s) are collected;
  - The output(s) the system produces;
    - How the output is used in making the decision and how much it is relied upon in making the decision;
    - Whether the output generated by the system is used downstream for any purpose not already articulated;
  - In addition to above, developers of the ADS should also document:
- Evidence to show that the system will function the way it is supposed to:
  - For developers of the ADS only, document:
    - The logic of the system;

        - The source(s) of the training data in the underlying model(s) of the system;
        - How the quality of the training data is maintained, including accuracy, reliability, bias, disparate impact, and data security measures;
    - How the quality of the input(s) is maintained, including accuracy, reliability, risk of bias or disparate impact, and data security measures;
    - How the functioning of the system will be free from inaccuracy, unreliability, bias or disparate impact, and how the business will ensure that;
    - Metrics that are used to measure performance and known limitations of the system;
- How the consumer will be notified of the business's use of the system, including the information in the detailed description above;
    - How consumers can access an explanation of how and why a decision was made and how the ADS contributed to the decision;
    - How consumers can correct inaccurate information and have the decision re-evaluated based on the corrected information;
    - How consumers can opt-out or seek an appeals process, if available in the jurisdiction;
- Third parties that will have access to the input or output data of the system and for what purpose;
- A detailed description of the system's capabilities, including capabilities outside of the scope of its intended use and when the system should not be used; and
- A plan for recurring validation studies and audits of accuracy, bias, and disparate impact.

A developer of an ADS should be required to provide all information necessary for the deployer to conduct its own risk assessment. A developer should also be required to perform its own risk assessments and testing throughout the development process and before either deploying the ADS itself or making it available for sale or use by others.

i. Specified Methods for Measuring Privacy Impacts

Most of the above risk assessment requirements should be straightforward for businesses to comply with. Businesses should be aware of what personal information they collect, process, or sell about consumers, and they should understand how an automated decision system works before they deploy it.

One aspect of impact assessments that has faced criticism is the requirement that businesses assess privacy or human rights impacts and identify what efforts they will undertake to mitigate those risks. Some of the critics who voice this view argue that risk assessments are an abstract exercise that does not materially improve privacy, transparency, or accountability. Although we disagree firmly that this is true of risk assessments in general, it is fair to say that a *poorly executed* risk assessment may do little to protect the rights of those whose data is processed.

"It is important to understand that risk assessments are socio-technical—the system must be assessed in the context in which it would be deployed.

Reflecting on the history of environmental impact assessments illustrates how risk assessment requirements that are not carefully thought out or well enforced can become a box-checking exercise—for example, the requirement for an environmental impact assessment prior to the construction of the Trans-Alaska Pipeline did not lead to objective assessments of the environmental and societal impact on Inuit communities because the assessment process was tainted by the U.S. government's interest in development.[186] It is important to understand that risk assessments are socio-technical—the system must be assessed in the context in which it would be deployed.[187] Poorly designed and conducted risk assessments can allow covered entities to evade assessing certain harms, leading to an incomplete assessment of privacy risks, a lack of mitigation measures and potentially harm individuals.[188]

To avoid the pitfall of risk assessments becoming divorced from real-life harms, the regulator charged with policing risk assessment compliance should provide detailed privacy harms and human rights guidance for the businesses to assess. For instance, examples of psychological harm that businesses should assess could

include emotional distress from disclosure of nonconsensual intimate imagery; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes, without limiting the assessment to such examples.[189] The enforcing agency could provide detailed examples of harms for different privacy risks and provide a workflow that helps businesses identify risks based on previous enforcement actions by the agency and the experience of the agency from assessing privacy risks. Such clarity would be beneficial for covered entities to better comply and for consumers and advocacy organizations to assess compliance with the risk assessment requirements.

Further, assertions by covered entities about the privacy risks and mitigation efforts should be backed by measurable evidence or reputable research. While perfectly quantifying human rights risks is impossible, qualitative, interdisciplinary assessments of the processing activity within the deployment context can yield a useful assessment.[190] The enforcing agency should have interdisciplinary staff to evaluate the risk assessments, and if it finds that the business is making unfounded assertions without evidence, the agency should be authorized to demand supporting documents. Further, post-deployment, if the agency finds that the system poses more privacy risks than identified in a risk assessment, or that the harms do not outweigh the benefits, the agency should be able to compel the business to alter or suspend the relevant data practices, to require updates the assessment, and to investigate the business for misrepresentations or inadequacy in its risk assessment.

j. Assessors With Expertise and Independence

Risk assessments may be conducted internally or through consultation with third parties, but for particularly large-scale or risky processing activities that impact individuals' civil rights, risk assessments should be conducted by an independent entity.[191] To be independent, the assessor should be credible or certified and have no financial interest in the outcome of the risk assessment.[192] Independent assessments are less susceptible to pressure from the entity to produce a positive assessment and are more likely to result in an objective assessment. Because

assessments conducted by an independent party can inform development decisions, they should be repeated when material changes are to be made to the processing of personal information or use of an ADS.

Because risk assessments should be able to inform the development process and should not be siloed, conducting a risk assessment must involve the individuals who took part (or would take part) in the planning, design, implementation, testing, and deployment of the system or practice to be assessed. The individuals who conduct the risk assessment should have relevant qualifications to conduct the risk assessment. As noted earlier, relevant qualifications not only involve technical expertise but also the ability to assess the social context and privacy implications of the data processing or deployment of an ADS, which requires interdisciplinary expertise. If an entity does not have such expertise, it should look to independent assessors rather than conducting an insufficient assessment. The business should be required to identify individuals with relevant qualifications who contributed to and approved the risk assessment to ensure individuals within businesses take the risk assessment requirements seriously.

k. Robust Enforcement Mechanisms for Non-Compliance

A risk assessment mandate should be backed by effective enforcement mechanisms to ensure compliance. As previously noted, one way to simplify enforcement is to ensure that the threshold for the duty to conduct a risk assessment is clear-cut and easy for the enforcing agency to independently assess (rather than relying solely on the business's self-evaluation).

Making risk assessments public would also help ensure compliance. If consumers notice that a business collects their personal information but cannot find a risk assessment or find that the risk assessment is incomplete or inaccurate, they should have the ability to report to the enforcing agency. Even if individual consumers may be unlikely to wade into reading full risk assessments, academics, nonprofits, and consumer advocates can fulfill this watchdog role to assist enforcement efforts.[193] Public risk assessments would be valuable a tool for these intermediaries to assess the risk assessments, educate consumers, and advocate for strong consumer protections.

Further, to prevent businesses from treating potential fines from non-compliance as simply a cost of doing business, risk assessment frameworks should include private right of action for individuals to enforce assessment requirements. A private right of action is the most effective way to incentivize compliance and avoids leaving the protection of consumers' privacy solely up to regulators who make lack adequate resources.

When systems are deployed, real-life harms can occur that may or may not have been identified as potential risks in the risk assessments. To close the gap between the potential harms identified in the risk assessment and the real harms experienced by individuals, there should be conspicuous channels where consumers can bring privacy harms to business's attention, and a business must rectify issues when possible. For example, there should be a process for consumers to check for, and if necessary, correct information used as inputs to an ADS, and request a reevaluation with corrected information. Businesses should have ongoing assessments of harms reported and periodically reevaluate the harms weighed against the purported benefits of the processing. Regulators should sustain the scrutiny on businesses by proactively discovering harms and enforcing the law against violating businesses.

1. Beyond Risk Assessments

Risk assessments will not resolve all issues presented by unregulated data processing or unrestricted deployment of ADS, but requiring risk assessments is a crucial step. Without meaningful transparency, enforcement of any civil or consumer rights is nearly impossible.[194] Risk assessments should complement other transparency and accountability tools to more fully protect consumer privacy rights.

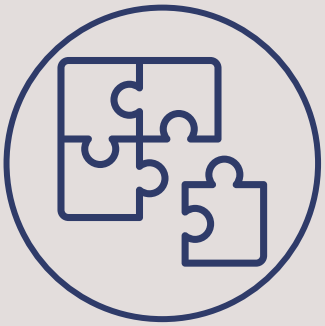
For example, effective algorithmic transparency will require regular independent audits and validation studies based on the purpose and use of the system, including what decisions it will be used to make or support. These measures will require thoughtful consideration of a system's data inputs, its logic, intended benefits, its capabilities (including those outside the scope of its intended or appropriate use), and privacy risks.[195] Audits should also include an assessment of the number of false positives and false negatives for each subgroup of the impacted population,

such as subgroups broken down by gender, race, disability, or language spoken to capture disparate impacts and errors.[196]

In discussing regulatory frameworks, one dynamic that must be addressed is the "specification dilemma," which describes how algorithmic systems can cause harm when they fail to work as specified—i.e., in error—but may just as well cause real harms when working exactly as specified.[197] A good example is facial recognition technology. Errors in facial recognition technology, such as wrongly identifying an individual as the target, can lead to wrongful arrests and reputational and psychological harms. Facial recognition technology is known for exhibiting disparate error rates, often erroneously matching people of color.[198] But even if facial recognition technology worked 100% of the time, it still causes harm, including by chilling freedom of assembly, free association, freedom of expression, and freedom of movement.[199] Risk assessments should thus cover both types of harms: both when the system does not work as intended and when it does.

"But even if facial recognition technology worked 100% of the time, it still causes harm, including by chilling freedom of assembly, free association, freedom of expression, and freedom of movement.

However, companies implementing such systems may not be able or sufficiently incentivized to assess privacy harms caused by their systems working as intended. Thus, risk assessments and audits should be paired with robust privacy and algorithmic protections and robust civil rights language prohibiting data-driven discrimination.[200] Substantive data minimization provisions will limit the data that businesses can collect in the first instance, thus substantially mitigating privacy risks.[201] Other stakeholders in the transparency and accountability ecosystem, such as entities that conduct audits, should be subject to oversight to ensure they are independent.[202] Lastly, legislators should ban particularly high-risk uses of AI that carry serious and documented privacy harms, such as one-to-many facial recognition or sentiment analysis.[203]



Part IV: The California Rulemaking Process

This Part will turn to the ongoing rulemaking process in California for regulations touching on automated decisionmaking technologies[204] and risk assessments. First, we explain the statutory and regulatory backdrop for the rulemaking process. Then, it will describe how the strong proposed regulations in the initial draft have been watered down due to industry pressure, resulting in proposed draft regulations that provide far less transparency and accountability. Finally, we respond to a number of common arguments raised by industry lobbyists to attack the proposed regulations.

Note: Throughout this report, we have used the term "automated decision system (ADS)" to describe AI that is used to make or facilitate human decisionmaking. Because California's proposed regulations use the term "automated decisionmaking technology (ADMTs)" to describe the same technology, we will use that term in the section discussing the proposed regulations.

a. Background on California's Rulemaking

California passed its consumer privacy law, the California Consumer Privacy Act ("CCPA"), in 2018.[205] The CCPA established the right of residents of California to know what personal information about them is being collected; to know whether their information is sold or disclosed and to whom; to limit the sale of personal information to others; and to access their information held by others.[206] The CCPA gives individuals a right to delete their data and prohibits businesses from selling the personal information of California residents under the age of 16 without their opt-in consent.[207] California voters then amended the CCPA in 2020 by adopting the California Privacy Rights Act ("CPRA")[208] via ballot measure.[209] California's dedicated privacy agency, the California Privacy Protection Agency ("CPPA" or "the Agency") was created by CPRA and has rulemaking authority to develop and promulgate regulations[210] to help implement the CCPA. The CPPA shares enforcement authority with the California Attorney General.[211]

The CPPA (as amended by CPRA) mandates risk assessments covering the processing, use, benefits, and risks related to personal data. The CCPA directs the CPPA to promulgate regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or

security," to submit to the CPPA on a regular basis a risk assessment.[212] The risk assessments pertain to the processing of personal information, including whether the processing involves sensitive personal information, and businesses must weigh the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy outweigh the benefits from processing.[213] The CCPA is one of the strongest comprehensive state privacy laws in the country, and effective analysis of CCPA-required risk assessments is key both to informing consumers about how their data is being processed and to deterring data abuses on the part of businesses.

As of the publication of this report in June 2025, there is an open California Privacy Protection Agency rulemaking to clarify risk assessment requirements under the Act—as well as to adopt regulations on automated decisionmaking technology (ADMT), cybersecurity audits, and the application of the CCPA insurance companies.[214] The formal rulemaking process commenced on November 8, 2024. The analysis below is based on the proposed regulations as of May 2025.[215]

b. The Proposed Regulations Would Fail to Deliver Consumers Transparency

The initial proposed regulations were a promising start to providing more consumer privacy protections and transparency and accountability mechanisms through risk assessments. However, under significant pressure from industry lobbyists and Governor Gavin Newsom, the proposed regulations have been substantially weakened in terms of consumer protection, transparency, and accountability.[216]

This Part addresses four key issues with the revised regulations: (1) the definition for ADMT is too narrow, leaving out many harmful and concerning uses of ADMT; (2) some processing activities that pose substantial privacy risks are excluded from the risk assessment requirement threshold; (3) numerous important risk assessment factors, such as the privacy risks of processing and how the business ensures the system works as intended, would not be reported to the CPPA (let alone the public); (4) businesses would not be prohibited from engaging in processing activities

where risks to consumers' privacy outweigh the benefits; and (5) there is very little, if any, ability for the public to access risk assessments conducted by covered entities.

While the proposed regulations still represent a positive step forward in providing California consumers with transparency, the most recent draft of the regulations are a disappointing step back from the strong substantive risk assessment provisions in the previous version.

1. The ADMT Definition Is Too Narrow

The definition that covers ADMT is crucial to ensuring that concerning uses of automated decision systems are covered. EPIC has urged that the definition of ADMT cover situations where the system is used to "assist or replace" human decisionmaking, even if the system does not make the final call.[217] Covering circumstances where both a human and ADMT are involved in a decisionmaking process is essential because research shows humans tend to over-rely on automated systems.[218] The latest proposed definition of ADMT ignores this reality by excluding from coverage ADMTs that assist (but do not fully replace) human decisionmaking.

"Covering circumstances where both a human and ADMT are involved in a decisionmaking process is essential because research shows humans tend to over-rely on automated systems.

The November version of proposed regulations defined ADMT as "any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking."[219] "Substantially facilitate" was defined as "using the output of the technology as a key factor in a human's decisionmaking."[220] This definition, while narrower than the "assist or replace" language that EPIC recommended, did include situations where an ADMT is used to generate a score about a consumer that a human reviewer uses as a primary factor to make a significant decision about them.[221] This definition would have captured, for example, an ADMT that calculates a score about a rental tenant applicant that the landlord would primarily rely on to make a decision about whether to accept or deny the

application, which presents serious risks to consumers including discriminatory and otherwise unfair or erroneous outcomes.[222]

The new proposed definition for ADMT covers "any technology that processes personal information and uses computation to replace human decisionmaking or *substantially replace* human decisionmaking."[223] "Substantially replace human decisionmaking" is defined as a business "us[ing] the technology's output to make a decision without human involvement."[224] The example of a system that generates a score about a consumer that the human reviewer uses as a primary factor in the decision is thus removed from coverage.

The new definition is even narrower than the original proposed definition, insofar as it removes from coverage situations when ADMT is the primary basis for a human decisionmaking or otherwise substantially facilitates the human decisionmaking (without fully replacing it). "Human involvement"—the presence of which would disqualify a system as ADMT—requires only that a person: "A) know how to interpret and use the technology's output to make the decision; B) Review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and C) have the authority to make or change the decision based on their analysis in subsection (B)."[225] Many ADMT examples involve a human decisionmaker in the loop, such as an employer making the final decision to hire or progress a job candidate based on AMDT outputs,[226] law enforcement making the decision to arrest based on a false facial recognition match,[227] or a landlord relying on ADMT score to accept or deny a rental application.[228] But human involvement in a decision impacted by an ADMT does not eliminate the significant privacy concerns. Humans tend to over-rely on ADMT outputs, and business practices may pressure the human in the loop to spend as little time as possible on each decision or may impose other barriers to the human's ability to disagree with the ADMT outputs.[229]

"But human involvement in a decision impacted by an ADMT does not eliminate the significant privacy concerns.

While the "without human involvement" portion of the definition is seemingly included to prevent covered entities from relying on humans to act as rubber stamps for ADMT outputs, in reality, businesses are likely to use this provision to self-certify out of coverage. Even if a human is unqualified to assess or disagree with the ADMT output, has little time to assess each decision, or otherwise feels pressure to rubber-stamp ADMT outputs, businesses will be incentivized to avoid compliance burdens by taking the stance that its system has a human in the loop. Coupled with the lack of public access or an affirmative obligation for companies to submit risk assessments to the CPPA, it will be extremely difficult for regulators to enforce risk assessment requirements as to companies who self-select out of compliance using this loophole.

This is the same strategy some businesses have adopted to circumvent New York City's algorithmic transparency law, Local Law 144,[230] concerning automated decision technology used in employment decisions. The city's regulations cover circumstances in which an automated tool is "substantially assisting" discretionary decisionmaking, which occurs where either (1) the tool's output is the only factor in the decision; (2) the tool's output the most important factor in a set of criteria; or (3) the tool's output is used to override conclusions based on other factors, including human decisionmaking.[231] This standard allows businesses to effectively decide for themselves whether they are covered, as it is difficult for officials to identify a business that should be in compliance but is not.[232] A similar fate likely awaits the CPPA's ADMT regulations if the Agency moves forward with a narrowed definition of ADMT. Many businesses will likely risk an (improbable) enforcement action over their failure to treat automated systems as covered ADMTs rather than proactively comply with the regulations given the considerable challenges and limitations of enforcement.

2. The Risk Assessment Thresholds Fail to Capture ADMTs That Impose Significant Privacy Risks

There are two large categories of triggers for risk assessments under the proposed regulations: (1) a business's actions pertaining to consumer personal information and (2) a business's use of automated decisionmaking technologies. For the first category, the current draft regulations are unchanged from prior versions, and

the thresholds for coverage based on processing personal information are sufficiently broad. For the second category, however, there was a significant narrowing in the revised draft; the proposed regulations no longer require risk assessments or provide other consumer rights for some ADMT uses that pose serious privacy concerns.

For the first category, the proposed regulations identify two processing activities that trigger risk assessment requirements: (1) selling or sharing personal information;[233] or (2) processing sensitive personal information.[234] These thresholds cover the processing activity that EPIC recommends in this report, including the most risky uses of personal information. The "selling or sharing" trigger covers all possible ways that a covered entity could provide another entity access to consumer's personal information.[235] This trigger gets to the heart of the vast marketplace that exists for consumers' personal information and requires businesses to undertake risk assessments before engaging in such "selling or sharing." Further, using the processing of sensitive personal information as a trigger imposes an objective, clearly defined threshold, which provides clarity for businesses and enforcers.

Significant decision:

"decision… that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g. posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel)."

In contrast, the threshold for ADMT uses that triggers the risk assessment requirement has been weakened in this draft compared to prior ones. The November 2024 proposed regulations required companies to conduct risk assessments when they use an ADMT for a "significant decision," [236] "extensive profiling of a consumer," [237] or "training" ADMT.[238] While limited, enumerating these uses of ADMT as triggers for risk assessments ensured that businesses were required to conduct risk assessments to engage in many of the most harmful uses of ADMTs, as highlighted in Part I.

In the latest proposal, the uses of ADMT that trigger risk assessments were narrowed, and many concerning uses were removed from coverage, meaning risk assessments and other ADMT-related provisions do not apply. Namely, the "significant decision" definition no longer includes decisions about criminal justice, insurance, or essential goods or services.[239] Some of the most harmful uses of ADMT arise in criminal justice settings, as incorrect or biased outputs can expose individuals to wrongful arrest and have a tremendous impact on their wellbeing, including employment, housing, and mental health.[240] Removing the risk assessment requirement allows businesses to deploy ADMTs in such contexts without a covered entity assessing the privacy risks or ensuring that the ADMT works accurately as intended and without bias. This puts Californians at risk. The definition of "significant decision" has also been narrowed such that it no longer covers Californians' "access to" the enumerated list of important goods and services; instead, a significant decision is defined as only the "provision or denial of" such goods and services.[241] This narrowing means that businesses no longer need to conduct risk assessments or provide people with other ADMT rights if they use ADMT to price necessities like rent, insurance, or health care so prohibitively high that many people can no longer afford to access them.

Extensive profiling:

"(A) profiling a consumer through systematic observation when they are acting their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ('work or educational profiling');

(B) Profiling a consumer through systematic observation of a publicly accessible place ('public profiling'); or

(C) profiling a consumer for behavioral advertising."

Further, ADMT used for profiling a consumer for behavioral advertising was also removed from the list of risk assessment triggers. While the "selling or sharing" personal information trigger for risk assessments remains—which captures much of the data broker industry—first-party profiling for behavioral advertising would no

longer require risk assessments. Advertisers routinely use characteristics like race, gender, and income or proxies like ZIP codes to filter and target certain audience segments to advertise employment,[242] housing,[243] and educational opportunities.[244] First-party or not, profiling for behavioral advertising poses consumer privacy and equity risks and should therefore trigger the risk assessment requirement.

"First-party or not, profiling for behavioral advertising poses consumer privacy and equity risks and should therefore trigger the risk assessment requirement.

Profiling in public places was removed and replaced with profiling in "sensitive locations," which are defined as "healthcare facilities including hospitals, doctors' offices, urgent care facilities, and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; educational institutions; political party offices; legal services offices; union offices; and places of worship."[245] This new construction leaves out the profiling of consumers in other public spaces—such as retail businesses, streets, entertainment venues, and public transit—from the risk assessment requirements. Profiling in such public, "non-sensitive" spaces still threatens consumer privacy. Businesses often surreptitiously and continuously collect personal information on consumers and create a system of surveillance that can track individuals' locations, habits, and associations as well as gatekeep entry into businesses and entertainment venues on opaque and unaccountable criteria.[246]

The revised proposal narrows the threshold concerning training ADMT as well. The prior version of the regulations would have required a risk assessment when a business is "processing personal information to train ADMT or artificial intelligence that is capable of being used for any of the following: A) for a significant decision concerning a consumer; B) to establish individual identity; C) for physical or biological identification or profiling; D) for the generation of a deepfake; or E) For the operation of generative models, such as large language models."[247] The May 2025 version narrows the initial scope of coverage by replacing "capable of being used for" with "which the business intends to use for," deferring to the business's intent rather than acknowledging the inherent risk that some ADMT can be put to high-impact uses.[248] This again makes it easier for businesses to self-certify out of

risk assessment requirements by claiming they did not intend for the resulting model to be used in a particular way when they were training the model.

Also removed from the list of enumerated use cases are "for the generation of a deepfake" and "for the operation of generative models, such as large language models."[249] These two omissions are concerning because large language models, other generative models, and especially the generation of deepfakes all pose gave privacy concerns. Many tech companies have been training large language models on content scraped from the internet without the knowledge or consent of the data subjects, which include children's data and copyrighted material.[250] This information then becomes baked into the model, with no clear means for consumers to prevent their personal information from being exploited or leaked.[251] This removal effectively allows Big Tech to continue training large language models on any data it can access, without regard to consent or privacy harms. And the use of generative AI to produce deepfakes presents clear privacy risks, which is why the federal government and many states—including California—have taken quick action to regulate this use of AI.[252] This acknowledgment of the risks posed by generative AI models makes it difficult to understand why the CPPA would remove these uses from the scope of the risk assessment requirements.

3. The Proposed Regulations Would Yield Insufficient Assessment of Privacy Risks and ADMT Dangers

The November 2024 proposed regulations required businesses to conduct a detailed risk assessment and submit an abridged version to the CPPA, with the CPPA reserving the right to request the full risk assessment. This draft also required businesses to assess a large portion of the substantive information that Part III of this report recommends, including in a risk assessment. By contrast, the CPPA's revised proposal not only strips out key required elements (including assessing privacy risks), but also requires only the barest of risk assessment information to be submitted to the CPPA by default.

i. The 'Risk Assessment Report' Fails to Require an Analysis of the Risks and Benefits of Processing

The risk assessment requirement in the May 2025 proposed regulations undermines the core goal of risk assessments: forcing businesses to assess whether the benefits of processing outweigh the privacy risks (and be accountable to that assessment). The revised regulations introduce the concept of a "risk assessment report" that a covered business must complete. The proposed regulations lay out specific required components of a risk assessment. However, only a few of these components must be included in the "risk assessment report."[253] Several critical elements, including an assessment of the benefits of the proposed processing and an assessment of the privacy risks of the processing, need not appear in the report.[254] Thus, even though the risk assessment portion requires the business to assess the benefits and privacy risks of processing, the contents of such an analysis would not be routinely reported to the CPPA because they are not required elements of the risk assessment report. This problem is exacerbated by the regulations' lack of an affirmative obligation to disclose more detailed assessment information to the CPPA and by limitations on the CPPA's ability to request and obtain risk assessment report material.

> "The exclusion of the benefits and privacy risks of processing from the risk assessment report runs counter to the text of the CCPA, stymies the goal of risk assessments, and undercuts the CPPA's oversight authority.

The exclusion of the benefits and privacy risks of processing from the risk assessment report runs counter to the text of the CCPA, stymies the goal of risk assessments, and undercuts the CPPA's oversight authority. The CCPA directs the CPPA to promulgate regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to submit to the CPPA on a regular basis a risk assessment.[255] By excluding the assessment of privacy risks from the risk assessment report, the revised regulations will no longer compel an adequate assessment of risks to consumers' privacy or security. Further, because the proposed regulations no longer require businesses to routinely disclose meaningful risk assessment information to the Agency, they fail to fulfill the CCPA's mandate that businesses "submit to the

CPPA on a regular basis a risk assessment."[256] Thus, the CPPA is abdicating its responsibility to ensure that businesses adequately assess "whether the risks to consumers' privacy from the processing personal information outweigh the benefits"—the primary goal of a risk assessment, as stated in the proposed regulations.[257] Finally, the CPPA is diminishing its own ability to gain insight into privacy risks of processing activities that businesses would have had to disclose.

ii. The Content of the 'Risk Assessment Report' Required of Businesses Exhibits Dangerous Gaps

This Part will walk through the substance of subsections (a)(1) through (a)(9), which outline what businesses must do to conduct a risk assessment. While some of the information that is required to be identified and documented aligns with this report's recommended risk assessment framework, there are now large gaps because key requirements were removed from the November 2024 version, significantly weakening the risk assessment requirements.

Subsections (a)(1) through (a)(9), would require the following actions by the business conducting risk assessment:[258]

(1) Identify and document in a risk assessment report the business's purpose for processing consumers' personal information. The purpose must not be identified or described in generic terms, such as 'to improve our services or for 'security purposes.'
(2) Identify and document in a risk assessment report the categories of personal information to be processed, including any categories of sensitive personal information. This must include: the minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.

Commentary:

Subsection (2), by requiring the business to identify the minimum personal information necessary in relation to the purpose, implements the data minimization principle included in the CCPA. The relevant provision states,

> A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.[259]

A business, by identifying the personal data used, is declaring that the personal data processed is reasonably necessary and proportionate to achieve the identified purposes, as the CCPA requires. If the business processes personal information to an extent that is not necessary to achieve those purposes, then the business is in violation the CCPA. This provision requires the business to show their work that they are complying with the data minimization provision of the CCPA.

(3) Identify and document in a risk assessment report the following operational elements of the processing:

(A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.

(B) How long the business plans to retain each category of personal information, or if unknown, the criteria the business plans to use to determine that retention period.

(C) The business's method of interacting with the consumers whose personal information the business plans to process (e.g., via websites, applications, or offline) and the purpose of the interaction (e.g., to provide a good or service).

(D) The approximate number of consumers whose personal information the business plans to process.

(E) What disclosures the business has made or plans to make to the consumer about the processing of their personal information and, how these disclosures were or will be made (e.g., via a just-in-time notice).

(F) The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; and the purpose for which the business discloses or makes the consumers' personal information available to them.

(G) For the uses of automated decisionmaking technology [for significant decisions], the business must identify:

(i) The logic of the automated decisionmaking technology, including any assumptions or limitations of the logic; and

(ii) The output of the automated decisionmaking technology, and how the business will use the output to make a significant decision.

(4) Identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information, as applicable. The benefits must not be identified in generic terms, such as "improving our service."

(5) Identify the negative impacts to consumers' privacy associated with the processing. The business must identify the sources and causes of these negative impacts.

Commentary:

While exclusion from the risk assessment report ultimately undermine the utility of subsection (5), it does helpfully list examples of harms to consumer privacy that businesses should consider assessing. These harms include: (A) unauthorized access, destruction, use, modification, or disclosure of personal information; (B) discrimination on the basis of protected characteristics; (C) impairing consumers' control over their personal information, such as by providing insufficient information to make an informed decision or interfering with consumers' ability to make a choice regarding personal information; (D) coercing or compelling consumers into allowing processing of their personal information; (E) economic harms,

including limiting or depriving consumers of economic opportunities, charging consumers higher prices, or compensating consumers at lower rates based upon profiling; (F) physical harms to consumers or to property, including processing that creates the opportunity for physical or sexual violence; (G) reputational harms, including stigmatization; and (H) psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation. A risk assessment framework should identify a minimum baseline of privacy risks that businesses must assess and give examples to provide businesses with clarity, as these proposed regulations do.

Regrettably, however, the May 2025 version removed from the list of privacy harms "disclosing a consumer's media consumption (e.g. books they have read or videos they have watched) in a manner that chills or deters their speech, expression, or exploration of ideas."[260] As some of the examples of ADS harms outlined in Part I illustrated, tracking and profiling individuals' media consumption can infringe on consumers' free speech rights, causing a chilling effect and potentially limiting discussion or research of sensitive topics like mental health, LGBTQ+ issues, and reproductive health.[261]

(6) Identify and document in a risk assessment report any safeguards that the business plans to implement for the processing, such as safeguards to address the negative impacts identified in subsection (a)(5).

Commentary:

The new version strikes the following provision, which would have made the provision more robust: "The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures."[262] This removal makes the assessment of mitigation measures less robust because the regulations no longer require businesses to assess the extent to which the negative privacy impacts are mitigated. Once again, this undercuts the overarching goal of risk assessments—to force businesses to weigh the

benefits and risks of processing—which should include an assessment of how effectively the mitigation measures would decrease risks and impact the overall risk-benefit calculus. Removing the requirement that businesses identify how they will maintain knowledge of emergent risks is also counter to the interests of consumers: the CPPA is effectively allowing businesses to stick their heads in the sand after system deployment, even if serious real-life harms emerge.

(7) Identify and document in a risk assessment report whether it will initiate the processing subject to the risk assessment.
(8) Identify and document in a risk assessment report the individuals who provided the information for the risk assessment, except for legal counsel who provided legal advice.
(9) Identify and document in a risk assessment report the date the assessment was reviewed and approved, and the names and positions of the individuals who reviewed or approved the assessment, except for legal counsel who provided legal advice.

Commentary:

To fulfill its CCPA directive to protect consumer privacy, the CPPA should require businesses to conduct and submit the full risk assessment report by default—or an abridged risk assessment at minimum, which the November 2024 version did. The provisions above take a step back from that and only require the business to report the bare minimum information to the CPPA. More than the bare minimum information should be included in the routine submissions required of the businesses for the CPPA to ensure that businesses are conducting sufficient risk assessments.

iii. The Proposed Regulations Fail to Require Businesses to Prove That Their ADMTs Are Safe for Consumers

The revised proposal introduces several other glaring deficiencies with respect to ADMT. First, the May 2025 version removed the provision that required businesses to identify, for uses of ADMT, the actions the business will take to maintain the quality of personal information processed by the ADMT.[263] Under the November 2024 proposal, "quality of personal information" included the completeness,

representativeness, timeliness, validity, accuracy, consistency, and reliability of the sources of the personal information used in a business's application of ADMT. Businesses could have verified the quality of personal information by (1) identifying the source of personal information and its reliability; (2) identifying how the personal information is relevant to the task being automated and will be useful; (3) identifying whether the personal information contains sufficient breadth to address the range of real-world inputs; and (4) identifying how errors are measured and limited.[264] The November 2024 proposed regulations rightly placed the onus of ensuring the quality of the personal information on the business developing and deploying such automated decisionmaking systems to make significant decisions about consumers' lives. This removal suggests to businesses that they are free to deploy systems without robust data integrity practices in place, thus forcing consumers bear the burden of any errors.

Second, the May 2025 version also removes the requirement that businesses evaluate the need for human involvement in decisions involving ADMTs, and consider developing policies, training, and procedures for the human in the loop.[265] Every business deploying ADMTs should assess the appropriate degree of human involvement in the system to mitigate risks of inaccuracy, arbitrariness, and bias. Businesses should also consider how to properly train the personnel involved so they do not give undue weight to ADMT outputs or merely rubber-stamp those outputs. Removing these requirements will ultimately harm consumers.

"Every business deploying ADMTs should assess the appropriate degree of human involvement in the system to mitigate risks of inaccuracy, arbitrariness, and bias.

Lastly, the May 2025 version strikes the provision that would have required businesses to identify whether they evaluated an ADMT to ensure it works as intended for their proposed use and does not discriminate based on an individual's membership in a protected class.[266] Here again, this removal makes it easier for businesses to avoid testing each system before deployment to ensure it works accurately and does not discriminate. Instead of putting the burden on businesses to show that their systems work as intended, the proposed regulations will

allow businesses to deploy untested and potentially dangerous ADMTs while still attesting that they complied with the risk assessment requirements.

4. The Proposed Regulations Fail to Prohibit Processing Activities Where the Risks Outweigh the Benefits

The May 2025 version completely guts the previously prohibition on processing activities where risks to consumers' privacy outweigh the benefits. Under the November 2024 proposal, if the risk assessment process led a business to conclude that a particular form of processing or ADMT application presented more risks than benefits, the business was prohibited from engaging in that activity.[267] The proposal gave some teeth to this provision by allowing the CPPA to assess the completed risk assessments and real-life impacts to determine whether the benefits outweigh the risks of a particular processing activity. The new language takes an enormous step back on this point: it now only states that the "goal of a risk assessment is restricting or prohibiting the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from processing," rather than directly prohibiting such processing.[268] This dramatically weakens the provision and curtails the CPPA's ability to give force and effect to a business's risk analysis.

This weakened language (combined with the removal of the requirement that businesses analyze the benefits and privacy risks from the risk assessment report) calls into doubt whether the CPPA is interested in enforcing businesses' obligation to conduct effective risk assessments. Under the May 2025 draft regulations, the CPPA would have a significantly diminished ability to examine how businesses have weighed the benefits and risks of certain processing activities—and even where it could conduct that evaluation, the CPPA would not necessarily have the power to halt a business's unduly harmful processing of personal information. To incentivize businesses to conduct effective risk assessments and to safeguard against unjustifiably risky data practices, the CPPA should restore the November 2024 language.

5. The Proposed Regulations Require Businesses to Report Minimal Information to the CPPA and Provide for No Public Access

Under the May 2025 proposal, businesses are required to report very little information to the CPPA by default. A business must submit to the CPPA only the following:

> (1) The business's name and a point of contact for the business, including the contact's name, phone number, and email address.
>
> (2) The time period covered by the submission, by month and year.
>
> (3) The number of risk assessments conducted or updated by the business during the time period covered by the submission, in total and for each of the processing activities identified in section 7150, subsection (b). (NOTE: The referenced subsection listed triggers for risk assessments, as discussed earlier).
>
> (4) Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of each of the categories of personal information identified in Civil Code sections 1798.140(v)(1)(A)-(L) or sections 1798.140(ae)(1)(A)-(G), (2)(A)-(C).
>
> > (NOTE: The cross-referenced sections are as follows: 1798.140(v)(1)(A)-(L) define "personal information," (ae)(1)(A)-(F) define "sensitive personal information," and 2(A)-(C) define "processing of biometric information for uniquely identifying a consumer, personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.")
>
> (5) Attestation to the following statement: "I attest that the business has conducted a risk assessment for the processing activities set forth in section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). Under penalty of perjury under the laws of the state of California, I hereby declare that the risk assessment information submitted is true and correct."

(6) The name and business title of the person submitting the risk assessment information, and the date of the certification.

Commentary:

The only substantive details businesses must routinely submit to the Agency are the categories of processing activities that triggered a risk assessment, which alone provide very little insight into a business's assessment of the risks of processing. As a result, the CPPA may have little or nothing to go on to assess the sufficiency of the risk assessment purportedly conducted by the business. By contrast, the abridged risk assessment that the November 2024 proposal would have required businesses to submit to the CPPA: (1) the processing activity triggering the risk assessment; (2) a plain language explanation of its purpose for processing consumers' personal information; (3) the categories of personal information processed, and whether sensitive personal information is included; and (4) a plain language explanation of safeguards the business has implemented.[269] Although EPIC continues to believe that businesses should be compelled to disclose more information to the CPPA than the November 2024 proposal called for, the May 2025 proposal falls far short of even this meager list of information.

The CPPA is required under the CCPA to "provide a public report summarizing the risk assessments filed with the agency."[270] But given that the information required under the revised proposal is so scant, there may very little useful detail for the CPPA to include in such a report. Even if the CPPA's public report included the full risk assessment reports that the CPPA may request from businesses, those reports would not include the assessment of benefits and risks to consumer privacy from the processing. Although the CPPA may be able use its investigatory authority to compel businesses to turn over all documentation pertaining to risk assessments,[271] it seems unlikely that the CPPA would be able to exercise this authority at scale, and it is not clear whether the fruits of such investigation could be freely disclosed in the public report.

Lastly, the May 2025 proposal merely requires self-certification from businesses that they conducted a risk assessment. Self-certification alone is not effective at

protecting consumers from harmful processing, and in fact it can encourage businesses to do as little as possible while complying with the default reporting requirements. The current proposed regulations provide cover for businesses to claim they complied with the risk assessment requirements while having done little to assess the actual risks to consumer privacy, potentially misleading consumers and further failing to protect their privacy. To protect consumers from harmful processing, the CPPA should require businesses to analyze negative privacy risks, mandate more information be submitted to the Agency by default, and make risk assessments public. These requirements would ensure businesses spend more time and effort undertaking effective risk assessments and would give consumers greater transparency. The CPPA should reinstate the November 2024 version of risk assessment requirements and require businesses to make public (at a minimum) the abridged risk assessment.[272]

c. Industry Arguments Against Risk Assessment Regulations Fail

Big Tech and other industry stakeholders have consistently pushed the Agency to weaken its proposed privacy regulations, undermining the Agency's mission and harming consumers while promoting an anti-regulatory agenda.[273] Big Tech and industry lobbyists have poured resources into fighting regulations for decades, which has left consumers with a failed notice-and-choice regime. Tech's infamous goal was to "move fast and break things,"[274] and in the destructive wake of this goal, it has left a broken ecosystem that harms consumers and competition.[275] This broken ecosystem was the very thing that Californians overwhelmingly voted to fix through the ballot initiatives that established the California Consumer Privacy Act and the California Privacy Protection Agency.

"Tech's infamous goal was to "move fast and break things," and in the destructive wake of this goal, it has left a broken ecosystem that harms consumers and competition. as.

This Part responds to the tired arguments that industry has made for years to maintain the status quo—a gift to Big Tech at the expense of the consumer—through written comments, oral testimony, and public communications.[276]

Industry Argument: The Agency has exceeded the scope of its authority.

Industry has often pushed the argument that the CPPA, California's dedicated agency tasked with protecting consumer privacy, is overstepping its legal authority in developing regulations on cybersecurity, risk assessments, and ADMTs. Industry also argues that the Agency should limit itself to privacy-related issues and should not regulate ADMTs more broadly.

Nevertheless, these regulations are squarely within the Agency's authority. The CCPA explicitly authorizes the Agency to promulgate regulations requiring companies "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to submit risk assessments to the Agency.[277] When the risks to privacy outweigh the purported benefits, the goal of the regulations is to restrict or prohibit the processing.[278] The CCPA also explicitly provides the Agency the authority to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology."[279] EPIC joined the ACLU of Northern California in its comments[280] to the Agency addressing this issue:

> The plain terms of the CCPA also enable the agency to promulgate regulations that sweep farther than the specified topics identified in Section 185(a). Section 185 itself makes this clear, directing that authority to issue regulations extends to all areas that would "further the purposes of this title, including, but not limited to, the following areas." Section 1798.185(a). This wider scope of authority is reiterated in Section 185(b), which states that regulations can be adopted "to further the purposes of this title." Those "purposes" are enumerated explicitly in the CPRA and clearly reach the collection, disclosure, and use of personal information: "[i]n enacting this Act, it is the *purpose and intent* of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy. Section 3,

CPRA (emphasis added). Those "consumer rights" are detailed in Section 3(A), which indicates that consumers should, under the law, have rights to control the use of their personal information. *See* CPRA Section 3(A)(2) ("[c]onsumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to the consumer, and they should have meaningful options over how it is collected, used, and disclosed."); *see also* CPRA Section 3(A)(2)(7) ("[c]onsumers should benefit from businesses' *use* of their personal information.") (emphasis added).

Based on these clear statutory directives, the CPPA is acting within its authority—and is, in fact, fulfilling its CCPA-assigned mission—by promulgating these regulations. Industry's repeated argument that regulating ADMTs is outside of the CPPA's authority and should be left to the Legislature is without merit.

Industry Argument: The Agency Should Leave Regulation of Automated Decisionmaking Technology to the Legislature and Governor.

The Agency was created through a ballot measure, the CPRA, whereby Californians expressed their clear desire to have a privacy agency tasked with protecting them. The Legislature and Governor have approved the statutes that give the Agency the explicit authority to regulate data practices that harm consumers. This Agency, and these very regulations, are the exact type of regulation that the Agency was created to address.

Industry Argument: Regulations in California must be harmonized with other, less stringent regulations.

California, like any other state, should not water down its regulations because other jurisdictions impose weaker standards. States are not fulfilling their roles as laboratories of democracy or guardians of consumers if they uncritically adopt exactly what other jurisdictions have done without bringing their own experience and expertise to bear. If other jurisdictions promulgate risk assessment

requirements that have fewer or lower requirements, companies that operate across jurisdictions will likely conduct risk assessments consistent with California's standards—if they are indeed stronger. California should promulgate requirements that create the floor for risk assessments, especially because of its position as the only state with an entire agency dedicated to privacy protections. Further, because California is home to many tech companies and major industry players, it is arguably in the best position to develop regulations that would affect its own resident businesses.

Industry Argument: The training of ADMTs should be excluded from the risk assessment requirements.

As explained above, the statute explicitly provides the Agency the authority to regulate a business's processing of personal information when the processing poses significant risks to consumers' privacy. The voter guide for California's constitutional right to privacy, which was passed by voters and legislatures in 1972, explained the right to privacy was meant to address privacy mischiefs, including "the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party."[281] Using personal information to train AI, when it was not collected for this specific purpose, contradicts California's constitutional right to privacy and is the exact type of misuse of personal information that the Agency is directed to protect consumers against.

Industry Argument: Reporting requirements are onerous and will lead to a deluge of paperwork for industry.

In 2025, companies should already be in the habit of conducting risk assessments before they collect or process personal information. Any entity that is processing information in a way that could harm consumers should calculate the risks and determine what safeguards should be in place to mitigate potential harms. If companies have not done any paperwork regarding risks associated with their processing of personal

"In 2025, companies should already be in the habit of conducting risk assessments before they collect or process personal information.

information, it is past time for them to consider how their data processing may harm consumers. And if a company has already been doing so as a general risk mitigation practice or to comply with requirements in another jurisdiction, the burden of compiling those risks into a CCPA-mandated assessment will be minimal. Because some form of risk assessment is required in many states and many foreign jurisdictions, including the EU,[282] it is likely that many companies are already required to compile this information.

Moreover, assessments actually promote compliance. These assessments will help businesses comply with CCPA provisions like section 7002, which limits data collection to what is necessary,[283] and section 7027, which empowers consumers to restrict the use of sensitive personal information.[284]

Industry Argument: The costs of regulation will hurt businesses, especially small businesses.

The Agency carefully considered the benefits and costs of the regulations it proposed in November 2024. After a detailed economic analysis, the Board determined that those regulations were the best path forward, choosing to circulate them for public comment. The Agency was right to do so. While the Agency has concluded there will be an economic impact from regulation, it also determined that the benefits would outweigh the costs in the long run. It is especially critical to consider non-monetary costs and benefits of the proposed regulations—as the CPPA did—given than many privacy harms are abstract and difficult to quantify.

In terms of monetary costs and benefits, the Agency estimated that the compliance costs per firm would be $6,768 in the first year for the November 2024 proposed risk assessment framework.[285] Moreover, the majority of the costs for a risk assessment would be mitigated by the baseline (given that "quantification of certain benefits and negative impacts to consumers should already be considered by businesses"), and the only additional costs should be organizational.[286] Because many businesses are already subject to the GDPR and Colorado's privacy law, some of the costs will be mitigated.[287] This expense may seem substantial in the short term, but it reflects what is necessary to protect the privacy of Californians in the modern commercial surveillance ecosystem according to the Agency's expert cost-benefit analysis.

Some of these costs would also be offset by covered businesses avoiding falling victim to cybercrime or other expensive cybersecurity incidents. Conducting risk assessments and cybersecurity audits increases the likelihood of detecting and preventing security breaches, which helps to mitigate the monetary losses of cybersecurity incidents.[288] With respect to the November 2024 proposal, the Agency notes: "The direct benefits to California businesses of a 12.6% reduction of these seven cybercrimes are estimated to be approximately $1.5 billion in 2027 and $66.3 billion in 2036."[289]

As far as non-monetary costs and benefits, the Agency acknowledges that the benefits to consumers, competition, health, safety, welfare, and quality of life are difficult to quantify.[290] The Agency explained that these benefits include "avoiding the physical, reputational, and psychological harm that results from unauthorized access, destruction, use, modification, or disclosure of PI; and from unauthorized activity that results in the loss of availability of PI. The unquantified benefits include avoiding the social and psychological costs of identity theft and fraud, such as fear, anxiety, stress, and other inconveniences."[291] Other benefits include increased transparency and awareness, which leads to consumers becoming more informed about their rights. This awareness leads to more consumer control over their personal information, which leads to increased quality, accuracy, and efficiency of data that firms use.[292]

Businesses and the economy also benefit from regulation in ways that are difficult to quantify. Businesses gain more guidance about compliance and lower costs of consumer privacy by standardizing their processes. Businesses will benefit from more trust and loyalty from consumers, as well as increased reputation, which leads to more potential customers.[293]

Moreover, there are also real costs, monetary and otherwise, to not implementing privacy-protective regulations. The Agency was right to determine that promulgating the November 2024 proposed regulations would work more benefits than harms—and it should still trust that conclusion now.

Industry Argument: Regulation stifles innovation.

This argument is one that Big Tech and industry lobbyists raise whenever government is considering meaningful regulation, and this rulemaking process is no exception. However, it is an argument that falls flat here. Regulation actually can promote innovation; regulation and innovation are not opposing ideas. The status quo allows tech giants to move fast and break things. Regulations can make the largest players' business practices fairer to competitors and less harmful to consumers, which in turn promotes competition and innovation. Apple, for example, has been named the most innovative company in the world, "due in part to its creativity in developing features that assist in user privacy and security."[294]

> "[R]egulation and innovation are not opposing ideas.

Innovation without proper safeguards is reckless, as we have seen time and again. Innovation for innovation's sake, or at the expense of privacy, is not something California or other jurisdictions should strive for. Indeed, this is the exact problem that the Agency is supposed to address: the un- and under-regulated industry practices that harm consumers. If a practice is built on harming consumers, that practice should be slowed down or halted, and other less harmful practices should be adopted instead. Innovation should be steered toward practices that protect consumer privacy while providing desirable products and services. This privacy-protective, thoughtful progress is the type of innovation that the CPPA's November 2024 proposal would and should incentivize.

Part V: Risk Assessments as a Best Practice for Businesses

Currently, no jurisdiction has adopted an ideal risk assessment framework. Indeed, California, with one of the strongest privacy laws in the country, may adopt stripped down risk assessment requirements that do not even obligate businesses to disclose critical components of the assessment. However, there may be stronger requirements in the future.[295] Businesses would be well served to stay ahead of the regulatory curve and adopt some of these ideal risk assessment components as best practices before they are mandated by law.

Conducting thorough risk assessments can in fact benefit businesses. First, reckless and harmful data processing can cause reputational damage, loss of consumer trust, loss of business, and the unwanted attention of legislators. Consumers, advocates, journalists, and legislators are increasingly aware of the risks of ADS, and businesses are better off assessing privacy risks and implementing mitigation measures instead of taking shortcuts to deploy unassessed and untested systems. To earn consumer trust—and indeed to protect their own bottom line—businesses should ensure that the risks of their personal data processing to consumers are identified and mitigated.

Second, states are already moving toward more robust risk assessment requirements. By implementing thorough risk assessments now, businesses will be better situated to comply with forthcoming requirements and able to develop best practices without a looming compliance deadline.

Third, businesses should already be assessing privacy risks to limit their own liability. Irresponsible personal data practices can subject businesses to investigation, fines, and litigation. These include penalties and claims based on civil rights laws; privacy laws; unfair, deceptive, and abusive practice (UDAP) laws; breach notification and mitigation laws; and contract law, among others. Regulators—including the Federal Trade Commission (FTC), state attorneys general, and the Data Protection Authorities in EU countries that enforce the GDPR—are already taking action against companies for irresponsible data processing, which can result in hefty fines and diminish a business's reputation and profits.[296] Businesses should already be assessing whether and to what extent their processing of personal data may cause harm that is cognizable under existing law.

Finally, developers, deployers, and consumers can all benefit from the stability and transparency afforded by robust, public risk assessments. For example, if developers can verifiably establish that the ADS they offer is safe, accurate, and non-discriminatory, they stand to gain financially. Businesses and consumers are more likely to purchase a fully vetted system over other systems that lack corroboration. Businesses deploying ADSs would be better able to compare the offerings of different developers, which in turn would promote healthy market competition. Developers would also be able to limit their own liabilities by identifying and resolving system issues that threaten consumers. Consumers who are subject to automated decisionmaking would similarly benefit from the transparency engendered by public risk assessments. Consumers would also feel more confident that ADSs being used to make decisions about them or process their data are them are safe, accurate, and non-discriminatory.

In sum, businesses can and should take the lead on implementing robust risk assessments, which would model responsible business practices, limit liability, and spur privacy competition and innovation.

Conclusion

In many ways, conducting risk assessments before engaging in risky data practices seems a self-evident precaution for responsible businesses to take. A business processing personal information or deploying an ADS should map the categories and sources of personal information; assess the quality of information, the processing system, and outputs; maintain awareness of the risks to consumer privacy; and implement measures that mitigate these risks. None of these steps are controversial or overly burdensome. It is past time that businesses processing personal information demonstrate to consumers that their data practices are not putting them at risk.

In publishing this report, EPIC hopes to provide support and resources to consumers who want businesses to be transparent and accountable when processing their personal information, consumer advocates who are pushing for robust risk assessment regulations, businesses that are striving to develop and maintain responsible data practices, entities that are considering purchasing and deploying automated decisionmaking systems, and policymakers who are working to regulate businesses' processing of personal data and use of ADSs.

[1] *See* Danielle K. Citron & Daniel J. Solove, Privacy Harms, 102 B.U. L. Rev. 793 (2022); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 1 (2018); Gender Shades Project, http://gendershades.org/overview.html.

[2] California Department of General Services, State Administrative Manual, Definitions - 4819.2, https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2. "Automated decision system" does not include a spam email filter, firewall, antivirus software, identity and access management tools, calculator, database, dataset, or other compilation of data. *See* Comments of EPIC and the Consumer Federation of America to Cal. Privacy Prot. Agency, 19–21 (Feb. 19, 2025), https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/ [hereinafter *EPIC CPPA Feb. 2025 Comments*].

[3] Eric Bogert, Aaron Schecter & Richard T. Watson, *Humans rely more on algorithms than social influence as a task becomes more difficult*, Sci Rep 11, 8028 (2021), https://doi.org/10.1038/s41598-021-87480-9.

[4] Comments of EPIC et al. to Cal. Privacy Prot. Agency, 7–9, 43, (Mar. 27, 2023), https://epic.org/wp-content/uploads/2023/03/EPIC-et-al-comments-CCPA-rulemaking-March-2023-2.pdf [hereinafter *EPIC CPPA March 2023 Comments*].

[5] Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security, 7 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter *EPIC FTC Comments on Commercial Surveillance*].

[6] *Hearing before the Innovation, Data, and Com. Subcomm. of the H. Comm. on Energy & Com.*, 119th Cong. (2024) (testimony of John Davisson), https://epic.org/wp-content/uploads/2024/09/EPIC-Testimony-FTC-Sept2024.pdf.

[7] *See, e.g.*, *Workplace Privacy*, EPIC (2023), https://epic.org/issues/data-protection/workplace-privacy/; Benjamin Wiseman, Fed. Trade Comm'n, Remarks of Benjamin Wiseman at the Harvard Journal of Law & Technology on Worker Surveillance and AI (Feb. 8, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Jolt-2-8-24-final.pdf.

[8] *See, e.g.,* Nicole Ozer & Jay Stanley, *Diners Beware: That Meal May Cost You Your Privacy and Security*, ACLU (July 27, 2021), https://www.aclu.org/news/privacy-technology/diners-beware-that-meal-may-cost-you-your-privacy-and-security.

[9] *See, e.g.*, Press Release, FTC, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[10] *See, e.g.*, *Student Privacy*, EPIC (2023), https://epic.org/issues/data-protection/student-privacy/; Press Release, FTC, *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts* (May 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising; Julia Angwin, *The Big Business of Tracking and Profiling Students*, The Markup (Jan. 15, 2022), https://themarkup.org/newsletter/hello-world/the-big-business-of-tracking-and-profiling-students; Elizabeth Laird & Maddy Dwyer, Center for Technology and Democracy, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI* (2023), https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/.

[11] *See, e.g.*, Press Release, FTC, *FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law* (Aug. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law; FTC, A Look Behind the Screens: Examining the Data

Practices of Social Media and Video Streaming Services (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

[12] Press Release, FTC, *FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking* (Feb. 22, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over.

[13] *See, e.g.*, *Health Privacy*, EPIC (2024), https://epic.org/issues/data-protection/health-privacy/; Joseph Cox, *Inside the U.S. Government-Bought Tool that Can Track Phones at Abortion Clinics*, 404 Media (Oct. 23, 2024), https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/; Joseph Cox, *Location Data Firm Offers to Help Cops Track Targets via Doctor Visits,* 404 Media (Dec. 10, 2024), https://www.404media.co/location-data-firm-offers-to-help-cops-track-targets-via-doctor-visits/; Elisa Jillson, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, FTC: Bus. Blog (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases; Colin Lecher & John Keegan, *Suicide Hotlines Promise Anonymity. Dozens of Their Websites Send Sensitive Data to Facebook*, The Markup (June 13, 2023), https://themarkup.org/pixel-hunt/2025/04/28/how-california-sent-residents-personal-health-data-to-linkedin; Todd Feathers, Katie Palmer & Simon Fondrie-Teitler, "*Out Of Control*": *Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, The Markup (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[14] Sara Geoghegan, *Two Years Post-Dobbs: A Commercial Surveillance Landscape That is Confusing, Complicated, and Harmful to Abortion Seekers*, EPIC (June 25, 2022), https://epic.org/two-years-post-dobbs-a-commercial-surveillance-landscape-that-is-confusing-complicated-and-harmful-to-abortion-seekers/; Suzanne Bernstein, *The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America*, EPIC (June 13, 2024), https://epic.org/the-role-of-digital-privacy-in-ensuring-access-to-abortion-and-reproductive-health-care-in-post-dobbs-america/; Lesley Fair, *FTC Says Premom Shared Users' Highly Sensitive Reproductive Health Data: Can it Get More Personal than that?*, FTC: Bus. Blog (May 17, 2023), https://www.ftc.gov/business-guidance/blog/2023/05/ftc-says-premom-shared-users-highly-sensitive-reproductive-health-data-can-it-get-more-personal.

[15] *See, e.g.,* Press Release, FTC, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests* (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[16] *See, e.g.,* Zak Doffman, *Black Lives Matter: U.S. Protesters Tracked by Secretive Phone Location Technology*, Forbes (June 26, 2020), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/; Dell Cameron & Dhruv Mehrotra, *FTC Says Data Brokers Unlawfully Tracked Protestors and US Military Personnel,* Wired (Dec. 2024), https://www.wired.com/story/ftc-mobilewalla-gravy-analytics-orders/; Sam Biddle, *U.S. Marshals Spied on Abortion Protestors Using Dataminr*, The Intercept (May 15, 2023), https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/.

[17] *See, e.g.*, *Location Tracking*, EPIC (2024), https://epic.org/issues/data-protection/location-tracking/; Press Release, FTC, *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data* (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

[18] *See* EPIC FTC Comments on Commercial Surveillance at 30–40.

[19] Tomas Apodaca & Colin Lecher, *How California sent residents' personal health data to LinkedIn*, The Markup (April 28, 2025), https://themarkup.org/pixel-hunt/2025/04/28/how-california-sent-residents-personal-health-data-to-linkedin.
[20] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119, 128 (2004).
[21] *See* EPIC FTC Comments on Commercial Surveillance at 41.
[22] *Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of Caitriona Fitzgerald), https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security; EPIC FTC Comments on Commercial Surveillance at 45–55.
[23] *April 2025: Major Cyber Attacks, Ransomware Attacks and Data Breaches*, Cyber Management Alliance (May 1, 2025), https://www.cm-alliance.com/cybersecurity-blog/april-2025-major-cyber-attacks-ransomware-attacks-and-data-breaches.
[24] Jonathan Greig, *Dialysis company DaVita reviewing data leaked by ransomware gang*, The Record (April 24, 2025), https://therecord.media/dialysis-davita-reviewing-data-leak.
[25] Carly Page, *Edtech giant PowerSchool says hackers accessed personal data of students and teachers*, TechCrunch (Jan. 8, 2025), https://techcrunch.com/2025/01/08/edtech-giant-powerschool-says-hackers-accessed-personal-data-of-students-and-teachers/.
[26] Zack Whittaker, *Hertz says customers' personal data and driver's licenses stolen in data breach*, TechCrunch (April 14, 2025), https://techcrunch.com/2025/04/14/hertz-says-customers-personal-data-and-drivers-licenses-stolen-in-data-breach/.
[27] EPIC FTC Comments on Commercial Surveillance at 186–187. In 2021, the DOJ reported that about 23.9 million people were victims of identity theft and estimated that identity theft cost the U.S. economy more than $16 billion. Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, Department of Justice (Oct. 2023), https://bjs.ojp.gov/library/publications/victims-identity-theft-2021.
[28] EPIC FTC Comments on Commercial Surveillance at 49; Citron & Solove, *supra* note 1, at 831–43.
[29] *EPIC Statement on House Passage of Fourth Amendment is Not for Sale Act*, EPIC (April 17, 2024), https://epic.org/epic-statement-on-house-passage-of-fourth-amendment-is-not-for-sale-act/#:~:text=EPIC%20Statement%20on%20House%20Passage%20of%20Fourth%20Amendment%20Is%20Not%20For%20Sale%20Act,-April%2017%2C%202024&text=Today%2C%20the%20House%20passed%20the,Americans%27%20data%20without%20a%20warrant; Maria Villegas Bravo, *DHS Disregards Internal Policies and Avoids Fourth Amendment Protections to Track Your Location*, EPIC (Feb. 8, 2024), https://epic.org/dhs-disregards-internal-policies-and-avoids-fourth-amendment-protections-to-track-your-location/.
[30] Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, Center on Privacy & Technology at Georgetown Law (2022), https://americandragnet.org.
[31] Jolynn Dillinger & Stephanie K. Pell, *The criminalization of abortion and surveillance of women in a post-Dobbs world*, Brookings (April 18, 2024), https://www.brookings.edu/articles/the-criminalization-of-abortion-and-surveillance-of-women-in-a-post-dobbs-world/; Jennifer Korn & Clare Duffy, *Search histories, location data, text messages: How personal data could be used to enforce anti-abortion laws*, CNN (June 24, 2022), https://www.cnn.com/2022/06/24/tech/abortion-laws-data-privacy/index.html.
[32] Press Release, S.T.O.P. Condemns DHS LGBTQ+ Surveillance, Surveillance Technology Oversight Project (March 3, 2025), https://www.stopspying.org/latest-news/2025/3/3/stop-condemns-dhs-lgbtq-surveillance; Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, Slate (Feb. 24, 2022), https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html; Jay Stanley, *Catholic Group Buying Data to Out Gay Priests is Tip of Location-Tracking Iceberg*, ACLU (April 7, 2023), https://www.aclu.org/news/privacy-technology/catholic-group-buying-data-to-out-gay-priests.

[33] Sam Biddle, *U.S. Marshals Spied on Abortion Protestors Using Dataminr*, The Intercept (May 15, 2023), https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/; Chip Gibbons, *US surveillance of pro-Palestinian speech has a direct line to McCarthyism*, The Guardian (May 22, 2024), https://www.theguardian.com/commentisfree/article/2024/may/22/surveillance-pro-palestine-protest. *See also* supra note 16.
[34] *See* Citron & Solove, *supra* note 1, at 841–845.
[35] EPIC FTC Comments on Commercial Surveillance, at 48–49; Sauvik Das & Yuxi Wu, *How Online Behavioral Advertising Harms People*, Center for Democracy and Technology (Dec. 13, 2023), https://cdt.org/insights/how-online-behavioral-advertising-harms-people/.
[36] Jeremy B. Merrill, *Does Facebook Still Sell Discriminatory Ads?*, The Markup (Aug. 25, 2020), https://themarkup.org/the-breakdown/2020/08/25/does-facebook-still-sell-discriminatory-ads; Bennett Cyphers & Adam Schwartz, *Ban Online Behavioral Advertising*, Electronic Frontier Foundation (Mar. 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising.
[37] *Surveillance Advertising: What About Discrimination?*, Consumer Federation of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-discrimination/; Julia Angwin, Noam Scheiber & Ariana Tobin, *Dozens of Companies Are Using Facebook to Exclude Older Workers from Job Ads*, ProPublica (Dec. 20, 2017), https://www.propublica.org/article/facebook-ads-age-discrimination-targeting; Ariana Tobin & Jeremy B. Merrill, *Facebook Is Letting Job Advertisers Target Only Men*, ProPublica (Sept. 18, 2018), https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men.
[38] Charge of Discrimination, HUD, et al v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.
[39] Press Release, *New Lawsuit Challenges Big Tech Firm Meta for Discrimination in Advertising Higher Education Opportunities*, Lawyers' Committee for Civil Rights Under Law (Feb. 11, 2025), https://www.lawyerscommittee.org/new-lawsuit-challenges-big-tech-firm-meta-for-discrimination-in-advertising-higher-education-opportunities/.
[40] Anita Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907, 913–28 (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon; Till Speicher, *Potential for Discrimination in Online Targeted Advertising*, Proc. of the 1st Conference on Fairness, Accountability and Transparency, 81 Proc. Mach. Learning Rsch. 5 (2018), https://proceedings.mlr.press/v81/speicher18a.html ("The potential for discrimination in targeted advertising arises from the ability of an advertiser to use the extensive personal (demographic, behavioral, and interests) data that ad platforms gather about their users to target their ads. An intentionally malicious—or unintentionally ignorant—advertiser could leverage such data to preferentially target (i.e., include or exclude from targeting) users belonging to certain sensitive social groups (e.g., minority race, religion, or sexual orientation).").
[41] Yuxi Wu, W. Keith Edwards, Sydney Bice & Sauvik Das, *The Slow Violence of Surveillance Capitalism*, 2023 ACM Conference on Fairness, Accountability, and Transparency (June 12-15, 2023), https://dl.acm.org/doi/pdf/10.1145/3593013.3594119.
[42] Stevie Chancellor, Michael L. Birnbaum, Eric D. Caine, Vincent B. Silenzio & Munmun De Choudhury, *A Taxonomy of Ethical Tensions in Inferring Mental Health States from Social Media*, In Proceedings of the conference on fairness, accountability, and transparency, 79–88 (2019), https://dl.acm.org/doi/10.1145/3287560.3287587.
[43] Jon Keegan & Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, The Markup (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.
[44] *Id.*
[45] *Id.*; Rae Nudson, *When Targeted Ads Feel a Little Too Targeted,* Vox (Apr. 9, 2020), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus.

[46] Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads that Persist: Uncovering the Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating*, Proc. ACM Hum.-Comput. Interact. 6, CSCW2, Article 377 (Nov. 2022), https://arxiv.org/abs/2204.03200.
[47] Keegan & Eastwood, *supra* note 43.
[48] Sergio Flores & Nicholas Kjeldgaard, *Payday Loan Ads on Social Media Targeting New, Young Audience*, NBC San Diego (June 16, 2022), https://www.nbcsandiego.com/news/investigations/nbc-7-responds/payday-loan-ads-on-social-media-targeting-new-young-audience/2972920/.
[49] Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—To People Sitting in Clinics*, Lawfare (Sept. 19, 2022), https://www.lawfaremedia.org/article/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics.
[50] Justin Kloczko, Consumer Watchdog, Surveillance Price Gouging (Dec. 2024), https://consumerwatchdog.org/wp-content/uploads/2024/12/Surveillance-Price-Gouging.pdf; Khari Johnson, *AI Can Rip You Off. Here's How California Lawmakers Want to Stop Price Discrimination*, The Markup (March 13, 2025), https://themarkup.org/artificial-intelligence/2025/03/13/ai-can-rip-you-off-heres-how-california-lawmakers-want-to-stop-price-discrimination.
[51] Chris Hrapsky, *The Target app price switch: What you need to know*, Kare 11 (Feb. 6, 2019), https://www.kare11.com/article/money/consumer/the-target-app-price-switch-what-you-need-to-know/89-9ef4106a-895d-4522-8a00-c15cff0a0514.
[52] Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, Wall Street Journal (Aug. 23, 2012), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882.
[53] Keith A. Spencer, *Hotel booking sites show higher prices to travelers from Bay Area*, SF Gate (Feb. 3, 2025), https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.
[54] EPIC CPPA March 2023 Comments at 43; *Algorithms are Making Life-Changing Decisions About You—But How Do They Work?*, Tech Equity (May 20, 2025), https://techequity.us/2025/05/20/life-changing-algorithms-explained/.
[55] Kevin De Liban, TechTonic Justice, Inescapable AI: The Ways AI Decides How Low-Income People Work, Live*, Learn, and Survive* (2024), https://static1.squarespace.com/static/65a1d3be4690143890f61cec/t/673c7170a0d09777066c6e50/1732014450563/ttj-inescapable-ai.pdf [hereinafter *TechTonic Justice Report*].
[56] Emmanuel Moss, Elizabeth Ann Watkins, Ranjit Singh, Madeleine Clare Elish & Jacob Metcalf, Data & Society, Assembling Accountability: Algorithmic Impact Assessment for the Public Interest 4 (June 2021), https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/ [hereinafter *Assembling Accountability*].
[57] Miranda Bogen & Aaron Rieke, Upturn, Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias (Dec. 2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf; Charlotte Lytton, *AI Hiring Tools May be Filtering Out the Best Job Applicants*, BBC (Feb. 16, 2024), https://www.bbc.com/worklife/article/20240214-ai-recruiting-hiring-software-bias-discrimination; Will Knight, *Job Screening Service Halts Facial Analysis of Applicants*, Wired (Jan 12, 2021), https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/; Jo Constantz, *'They Were Spying On Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions*, NewsWeek (Dec. 13, 2021), https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603.
[58] Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired*, ACLU (Aug. 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired.
[59] *See id.*; Owen Davis, Laura Malugade & Keith Ybanez, *California Court Finds that HR Vendors Using Artificial Intelligence Can Be Liable for Discrimination Claims from Their Customers' Job Applicants*, Husch Blackwell (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/; Bogen & Rieke, *supra* note 57.

[60] Marissa Gerchick & Olga Akselrod, *The Critical Role of Research in the Fight for Algorithmic Accountability*, Tech Policy Press (Oct. 23, 2024), https://www.techpolicy.press/the-critical-role-of-research-in-the-fight-for-algorithmic-accountability/.

[61] Vedan Anthony-North, *Complaint Filed Against Intuit and HireVue Over Biased AI Hiring Technology That Works Worse for Deaf and Non-White Applicants*, ACLU of Colorado (March 19, 2025), https://www.aclu.org/press-releases/complaint-filed-against-intuit-and-hirevue-over-biased-ai-hiring-technology-that-works-worse-for-deaf-and-non-white-applicants.

[62] *Id*.

[63] Veena Dubal, *On Algorithmic Wage Discrimination*, 123 Col. L. Rev. 129 (2023); Merve Hickok & Nestor Maslej, *A Policy Primer And Roadmap On AI Worker Surveillance And Productivity Scoring Tools*, AI Ethics 3, 673–687 (2023), https://link.springer.com/article/10.1007/s43681-023-00275-8; Diego Areas Munhoz, '*Robot Bosses' Spur Lawmaker Push to Police AI Job Surveillance*, Bloomberg Law (Sept. 8, 2023), https://news.bloomberglaw.com/daily-labor-report/robot-bosses-spur-lawmaker-push-to-police-ai-job-surveillance; S.A. Applin, *How fast food is becoming a new surveillance ground*, Fast Company (April 8, 2024), https://www.fastcompany.com/91087484/how-fast-food-is-becoming-a-new-surveillance-ground; Vanessa Taylor, *An Employee Surveillance Company Leaked Over 21 Million Screenshots Online*, Gizmodo (April 24, 2025), https://gizmodo.com/an-employee-surveillance-company-leaked-over-21-million-screenshots-online-2000593880.

[64] Martha Ockenfels-Martinez & Sukhdip Purewal Boparai, *The Public Health Crisis Hidden in Amazon Warehouses*, Human Impact Partners and Warehouse Workers Resource Center (2021), https://cdn.prod.website-files.com/67465c90aaa0a803cd5503ad/6748276f01a9f192749b924a_The-Public-Health-Crisis-Hidden-In-Amazon-Warehouses-HIP-WWRC-01-21.pdf.

[65] Katie J. Wells & Funda Ustek Spilda, Roosevelt Institute, Uber for Nursing: How an AI-Powered Gig Model is Threatening Health Care (Dec. 2024), https://rooseveltinstitute.org/wp-content/uploads/2024/12/RI_Uber-for-Nursing_Brief_202412.pdf; Action Center on Race & the Economy, Driven Out by AI: How Uber's deactivations force drivers into chatbot hell and financial crisis (2025), https://acrecampaigns.org/wp-content/uploads/2025/03/Driven-Out-by-AI-report.pdf.

[66] Comments of Public Citizen to the White House Off. of Sci. & Tech., Automated Worker Surveillance and Management (June 29, 2023), https://www.citizen.org/wp-content/uploads/Public-Citizen-Comment-RFI-Automated-Worker-Surveillance-and-Management-6.29.2023.pdf; Comments of EPIC to Dutch DPA on Emotion Recognition Prohibition under EU AI Act, 19–22 (Dec. 17, 2024), https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/; Matt Scherer, *CDT, GFI, Others Send Memos Urging White House to Take Action on Electronic Workplace Surveillance*, Center for Democracy and Technology (April 3, 2024), https://cdt.org/insights/cdt-gfi-others-send-memos-urging-white-house-to-take-action-on-electronic-workplace-surveillance/.

[67] Moustafa Abdelwanis, Hamdan Khalaf Alarafati, Maram Muhanad Saleh Tammam & Mecit Can Emre Simsekler, *Exploring the risks of automation bias in healthcare artificial intelligence applications: A Bowtie analysis*, 5:4 Journal of Safety Science and Resilience 460 (Dec. 2024), https://www.sciencedirect.com/science/article/pii/S2666449624000410#b5.

[68] *See* Tom Simonite, *An Algorithm That Predicts Deadly Infections Is Often Flawed*, Wired (June 21, 2021), https://www.wired.com/story/algorithm-predicts-deadly-infections-often-flawed/. *See also* Heather Landi, *Olive rakes in $400M to turbocharge growth of 'humanized' AI for healthcare*, Fierce Healthcare(July 1, 2021), https://www.fiercehealthcare.com/tech/olive-rakes-400m-to-turbocharge-growth-humanized-ai-for-healthcare; Tyler Buchanan & Erin Brodwin, *Local Health Tech Startup Olive Overpromises*, Axios (Apr. 7, 2022), https://www.axios.com/local/columbus/2022/04/07/local-health-tech-startup-olive-overpromises.

[69] *See* Tom Simonite, *How an algorithm blocked kidney transplants to Black patients*, Wired (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/.
[70] Darshali A. Vyas et al., *Challenging the Use of Race in the Vaginal Birth After Cesarean Section Calculator*, Women's Health Issues 2019 May-June; 29(3):201-204 (May 6, 2019), https://pubmed.ncbi.nlm.nih.gov/31072754/.
[71] Laleh Seyyed-Kalantari, et al., *Underdiagnosis Bias of Artificial Intelligence Algorithms Applied to Chest Radiographs in Under-Served Patient Populations*, 27 Nat Med 2176–2182 (2021), https://www.nature.com/articles/s41591-021-01595-0; Haoran Zhang, Thomas Hartvigsen & Marzyeh Ghassemi, *Algorithmic Fairness in Chest X-Ray Diagnosis: A Case Study*, MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2023 (Feb. 27, 2023), https://mit-serc.pubpub.org/pub/algorithmic-chest/release/2.
[72] Ziad Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, *Dissecting Racial Bias in Algorithm Used to Manage the Health of Populations*, Science (Oct. 25, 2019), https://www.science.org/doi/10.1126/science.aax2342.
[73] *See, e.g.,* Rachana Pradhan, Samantha Liss & KFF Health News, *A Tennessee mom lost Medicaid after the state launched a Deloitte-run system that managed eligibility. Then her life turned upside down*, Fortune (June 24, 2024), https://fortune.com/2024/06/24/a-tennessee-mom-lost-medicaid-after-the-state-launched-a-deloitte-run-system-that-managed-eligibility-then-her-life-turned-upside-down/; Casey Ross & Bob Herman, *Denied by AI: How Medicare Advantage plans use algorithms to cut off care for seniors in need*, STAT (March 13, 2023), https://www.statnews.com/2023/03/13/medicare-advantage-plans-denial-artificial-intelligence/.
[74] *See* Annie Waldman, *How UnitedHealth's Playbook for Limiting Mental Health Coverage Puts Countless Americans' Treatment at Risk*, (Nov. 19, 2024), https://www.propublica.org/article/unitedhealth-mental-health-care-denied-illegal-algorithm.
[75] *See* T. Christian Miller, Patrick Rucker & David Armstrong, *"Not Medically Necessary": Inside the Company Helping America's Biggest Health Insurers Deny Coverage for Care*, ProPublica (Oct. 23, 2024), https://www.propublica.org/article/evicore-health-insurance-denials-cigna-unitedhealthcare-aetna-prior-authorizations.
[76] Eleni Manis, Fatima Ladha, Nina Loshkajian, Aidan McKay & Corinne Worthington, *Seeing Is Misbelieving*, Surveillance Technology Oversight Project (2024), https://www.stopspying.org/seeing-is-misbelieving; Aaron Sankin, Dhruv Mehrota, Surya Mattu, Dell Cameron, Annie Gilbertson, Daniel Lempres & Josh Lash, *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, Gizmodo (Dec. 2, 2021), https://gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977; Julia Angwin, Jeff Larson, Surya Mattu &Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Richard A.Webster, *An Algorithm Deemed This Nearly Blind 70-Year-Old Prisoner a "Moderate Risk." Now He's No Longer Eligible for Parole*., ProPublica (April 10, 2025), https://www.propublica.org/article/tiger-algorithm-louisiana-parole-calvin-alexander.
[77] Todd Feathers, *The Mystery of AI Gunshot-Detection Accuracy Is Finally Unraveling*, Wired (June 25, 2024), https://www.wired.com/story/ai-gunshot-detection-accuracy-san-jose-nyc/ (AI-powered gunshot detection technology from the company Flock Safety was reported of having 34% confirmed false positives from Feb. 2023 to July 2023, despite company claiming it is 90% accurate.).
[78] Christina Swarns, *When Artificial Intelligence Gets It Wrong*, Innocence Project (Sept. 19, 2023), https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/; Marissa Gerchick & Matt Cagle, *When it Comes to Facial Recognition, There is No Such Thing as a Magic Number*, ACLU (Feb. 7, 2024), https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number.
[79] Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, Wired (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/; Alyxaundria Sanford,

Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated, Innocence Project (Feb. 14, 2024), https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/; Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, NY Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[80] *USA: NYPD ordered to hand over documents detailing surveillance of Black Lives Matter protests following lawsuit*, Amnesty International (Aug 1, 2022), https://www.amnesty.org/en/latest/news/2022/08/usa-nypd-black-lives-matter-protests-surveilliance/. *See also* U.S. Gov't Accountability Office, GAO-21-518, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks 17 (June 3, 2021), https://www.gao.gov/assets/gao-21-518.pdf (finding that at least six agencies used facial recognition to surveil Black Lives Matter protestors); Benjamin Powers, *Eyes Over Baltimore: How Police Use Military Technology to Secretly Track You*, Rolling Stone (Jan. 6, 2017), https://www.rollingstone.com/culture/culture-features/eyes-over-baltimore-how-police-use-military-technology-to-secretly-track-you-126885/ (reporting that the Baltimore Police Department used facial recognition and social media surveillance to surveil protestors following the death of Freddie Gray).

[81] Sam Sabin, *Surveillance looms over pro-Palestinian campus protests*, Axios (May 5, 2024), https://www.axios.com/2024/05/03/student-pro-palestine-encampments-campus-surveillance.

[82] Suzanne Smalley, *Facial Recognition Technology Widely Used at Sporting Events, Privacy Watchdog Says*, The Record (May 23, 2024), https://therecord.media/facial-recognition-tech-used-in-sporting-events; Khari Johnson, *Get Used to Facial Recognition in Stadiums*, Wired (Feb. 2, 2023), https://www.wired.com/story/get-used-to-face-recognition-in-stadiums/; Joel R. McConvey, *Facial Recognition Comes to Great American Ballpark with MLB Go-Ahead Entry*, Biometric Update (Aug. 13, 2024), https://www.biometricupdate.com/202408/facial-recognition-comes-to-great-american-ballpark-with-mlb-go-ahead-entry; Abigail Opiah, *Facial Recognition Targets Scalping at Concerts and Festivals*, Biometric Update (Aug. 20, 2024), https://www.biometricupdate.com/202408/facial-recognition-targets-scalping-at-concerts-and-festivals; Manuela López Restrepo, *She Was Denied Entry to a Rockettes Show — Then the Facial Recognition Debate Ignited*, NPR (Jan. 21, 2023), https://www.npr.org/2023/01/21/1150289272/facial-recognition-technology-madison-square-garden-law-new-york.

[83] Eduardo Medina, *Rite Aid's A.I. Facial Recognition Wrongly Tagged People of Color as Shoplifters*, N.Y. Times (Dec. 21, 2023), https://www.nytimes.com/2023/12/21/business/rite-aid-ai-facial-recognition.html; Press Release, FTC, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards* (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[84] Shanti Das, *Facial recognition cameras in supermarkets 'targeted at poor areas' in England*, Guardian (Jan. 27, 2024), https://www.theguardian.com/uk-news/2024/jan/27/facial-recognition-cameras-in-supermarkets-targeted-at-poor-areas-in-england; Jay Stanley, *The Problem with Using Face Recognition on Fans at a Taylor Swift Concert*, ACLU (Dec. 14, 2018), https://www.aclu.org/news/privacy-technology/problem-using-face-recognition-fans-taylor-swift.

[85] Tech Equity Collaborative & Wonyong So, Screened Out of Housing: How AI-Powered Tenant Screening Hurts Renters (July 2024), https://techequity.us/wp-content/uploads/2025/03/Screened-out-of-housing-paper-2025-updates.pdf [hereinafter *Screened Out of Housing*].

[86] *Id.*

[87] *Id.*

[88] Thomas McBrien, Ben Winters, Enid Zhou & Virginia Eubanks, EPIC, Screened & Scored in the District of Columbia 27-28 (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf; Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Center for Democracy and

Technology (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/.
[89] 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; Taylor Giorno, *Fed Watchdog Warns AI, Machine Learning May Perpetuate Bias in Lending*, The Hill (July 18, 2023), https://thehill.com/business/housing/4103358-fed-watchdog-warns-ai-machine-learning-may-perpetuate-bias-in-lending/.
[90] Tara García Mathewson, *He Wanted Privacy. His College Gave Him None*, The Markup (Nov. 30, 2023), https://themarkup.org/machine-learning/2023/11/30/he-wanted-privacy-his-college-gave-him-none.
[91] Denisa Gándara, Hadis Anahideh, Matthew Ison & Lorenzo Picchiarini, *Inside the Black Box: Detecting and Mitigating Algorithmic Bias Across Racialized Groups in College Student-Success Prediction*, AERA Open (July 11, 2024), https://www.aera.net/Newsroom/Inside-the-Black-Box-Detecting-and-Mitigating-Algorithmic-Bias-Across-Racialized-Groups-in-College-Student-Success-Prediction; Erik Ofgang, *Colleges Are Using AI To Predict Student Success. These Predictions Are Often Wrong*, Yahoo News (Aug. 29, 2024), https://www.yahoo.com/news/colleges-using-ai-predict-student-090000670.html.
[92] Ellen Barry, *Spying on Student Devices, Schools Aim to Intercept Self-Harm before it Happens*, N.Y. Times (Dec. 9, 2024), https://www.nytimes.com/2024/12/09/health/suicide-monitoring-software-schools.html.
[93] *Id.*
[94] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke & Hannah Quay-de la Vallee, *Report-Hidden Harms: The Misleading Promise of Monitoring Students Online*, Center for Democracy and Technology (Aug. 3, 2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/; Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, Slate (Feb. 24, 2022), https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html; Claire Bryan & Sharon Lurye, *Student privacy vs. safety: The AI surveillance dilemma in WA schools*, Seattle Times (March 12, 2025), https://www.seattletimes.com/education-lab/student-privacy-vs-safety-the-ai-surveillance-dilemma-in-wa-schools/.
[95] Tara García Mathewson, *Online censorship in schools is 'more pervasive' than expected, new data shows*, Cal Matters (Jan. 16, 2025), https://calmatters.org/education/k-12-education/2025/01/web-filtering/.
[96] Clive Thompson, *What AI College Exam Proctors Are Really Teaching Our Kids*, Wired (Oct. 20, 2020), https://www.wired.com/story/ai-college-exam-proctors-surveillance/.
[97] Mitchell Clark, *Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them*, The Verge (Apr. 8, 2021), https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning.
[98]Itzel Luna, *California colleges still use remote proctoring despite court decision*, Cal Matters (Feb. 27, 2023), https://calmatters.org/education/higher-education/college-beat/2023/02/remote-proctoring-california-colleges/.
[99] Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, Center for Democracy and Technology (Nov. 16, 2020), https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/.
[100] Consumer Reports, AI/Algorithmic Decision Making: Consumer Reports Nationally Representative Phone and Internet Survey (2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/07/Public-Facing-Report-2024-AES-AI-Algorithms-7.25.24.pdf.
[101] *Id.*
[102] *Id.*

[103] Colorado's AI Act, passed in 2024 and scheduled to go into effect in February, would give Coloradans some transparency, rights, and recourse if an entity uses an ADS to make a consequential decision about them. This landmark legislation is the first in the U.S. to give people the right to know when an ADS is used to make a decision about them. Colo. Rev. Stat. § 6-1-1701.
[104] TechTonic Justice Report at 6.
[105] *Id.*
[106] *Id.* at 15.
[107] Caitriona Fitzgerald, Maggie Oates, Matt Schwartz & Kara Williams, The State Data Privacy Act, EPIC (April 2025), https://epic.org/documents/the-state-data-privacy-act/ [hereinafter *The State Data Privacy Act*].
[108] *Data Minimization*, EPIC, https://epic.org/issues/consumer-privacy/data-minimization/.
[109] EPIC FTC Comments on Commercial Surveillance at 30–33.
[110] Accountable Tech, AI Now and EPIC, Zero Trust AI Governance 5 (Aug. 2023), https://ainowinstitute.org/wp-content/uploads/2023/08/Zero-Trust-AI-Governance.pdf [hereinafter *Zero Trust AI Governance*].
[111] EPIC CPPA March 2023 Comments at 30–31.
[112] *Privacy Impact Assessments*, EPIC, https://epic.org/issues/open-government/privacy-impact-assessments/.
[113] E-Government Act of 2002, Pub. L. No. 107–347, § 208, 116 STAT. 2921.
[114] Kara Williams, *Assessing the Assessments: Comparing Risk Assessment Requirements Around the World*, EPIC (Dec. 4, 2023), https://epic.org/impact-comparison/.
[115] White House Off. of Sci. & Tech. Pol'y, B*lueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.
[116] *Id*. at 23.
[117] *Id*. at 15.
[118] Comments of EPIC to the Nat'l Telecomm. and Info. Admin. (June 12, 2023), https://epic.org/wp-content/uploads/2023/06/EPIC-NTIA-Comments-June-2023.pdf.
[119] Off. of Mgmt. & Budget, Exec. Off. of the President, OMB Memo M-25-21: Accelerating Federal Use of AI Through Innovation, Governance, and Public Trust at 10 (April 3, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf [hereinafter *M-25-21 Memo*]; Off. of Mgmt. & Budget, Exec. Off. of the President, OMB Memo M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government (April 3, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf.
[120] Exec. Order No. 14,179, 90 Fed. Reg. 8741.
[121] M-25-21 Memo Section 5.
[122] M-25-21 Memo Section 4(b)(ii).
[123] *OMB Finalizes Long-Awaited Guidance on Federal AI* Use, EPIC (Mar. 28, 2024), https://epic.org/omb-finalizes-long-awaited-guidance-on-federal-ai-use/.
[124] Caitriona Fitzgerald, Kara Williams, R.J. Cross & Ellen Hengesbach, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better*, EPIC & U.S. PIRG Education Fund (Jan. 2025), https://epic.org/documents/the-state-of-privacy-2025-how-state-privacy-laws-fail-to-protect-privacy-and-what-they-can-do-better/.
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] Cal. Civ. Code § 1798.185 (a)14(B).
[129] *Id*.
[130] Cal. Civ. Code § 1798.199.40(d).
[131] Colo. Rev. Stat. § 6-1-1301; 4 C.C.R. 904-3.
[132] 4 C.C.R. 904-3, Rule 8.04 (laying out requirements for data protection assessments).

[133] Colo. Rev. Stat. § 6-1-1701.
[134] "High-risk artificial intelligence system" is defined as "any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision" and contains several enumerated exceptions. *Id*. § 6-1-1701(9). "Substantial factor" is defined as "a factor that assists in making a consequential decision; is capable of altering the outcome of a consequential decision; and is generated by an artificial intelligence system" and explicitly includes "any use of an artificial intelligence system to generate any content, decision, prediction, or recommendation concerning a consumer that is used as a basis to make a consequential decision concerning the consumer." *Id*. § 6-1-1701(11).
[135] "Consequential decision" is defined as "a decision that has material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (a) education enrollment or an education opportunity; (b) employment or an employment opportunity; (c) a financial or lending service; (d) an essential government service; (e) health-care services; (f) housing; (g) insurance; or (h) a legal service." *Id*. § 6-1-1701(3).
[136] *Id*. § 6-1-1703(3)(a)(I).
[137] *Id*. § 6-1-1703(3)(a)(II).
[138] *Id*. § 6-1-1703(3)(b).
[139] *Id*. § 6-1-1707(1)(d).
[140] Ben Wolford, *Data protection Impact Assessment (DPIA)*, GDPR.EU, https://gdpr.eu/data-protection-impact-assessment-template/.
[141] *Id.*
[142] *Id.*
[143] *The UK GDPR*, Information Commissioner's Office, https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/#:~:text=Yes.,and%20obligations%20remain%20the%20same.
[144] *Brazil's Data Protection Authority publishes data protection impact assessment guidance,* Mattos Filho (May 2, 2023), https://www.mattosfilho.com.br/en/unico/data-protection-authority-assessment-guidance/.
[145] Zlatko Delev, *Comparing DPIA Requirements Across Global Jurisdictions*, GDPR Local (Dec. 12, 2024), https://gdprlocal.com/comparing-dpia-requirements-across-global-jurisdictions/#global-dpia-requirements; The Essentials for the South African Protection of Personal Information Act (POPIA) Compliance, Secure Privacy (Oct. 18, 2023), https://secureprivacy.ai/blog/south-africa-popia-compliance.
[146] Algorithmic Impact Assessment Tool, Gov't Canada, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.
[147] This set of components is largely based on the 10 components identified in Assembling Accountability.
[148] Zero Trust AI Governance at page 5.
[149] Ben Winters, *Algorithms' Transparency Problem is Everyone's Problem*, Data & Society: Points (May 10, 2023), https://medium.com/datasociety-points/algorithms-transparency-problem-is-everyone-s-problem-9a28e7e88cdb. *See also* Jay Stanley, *Communities Should Reject Surveillance Products Whose Makers Won't Allow Them to be Independently Evaluated*, ACLU (March 6, 2024), https://www.aclu.org/news/privacy-technology/communities-should-reject-surveillance-products-whose-makers-wont-allow-them-to-be-independently-evaluated.
[150] Complaint and Request for Investigation, Injunction, and Other Relief, In re HireVue (Nov. 6, 2019), https://epic.org/wp-content/uploads/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.
[151] *Id*.
[152] Press Release, *HireVue Leads the Industry with Commitment to Transparent and Ethical Use of AI in Hiring*, Hirevue (Jan. 12, 2021), https://apnews.com/press-release/globenewswire-

mobile/hirevue-leads-the-industry-with-commitment-to-transparent-and-ethical-use-of-ai-in-hiring-37d0fe232bcce86da20a5596cc840552.
[153] The O'Neil Risk Consulting & Algorithmic Auditing result can be downloaded, but HireVue prohibits reproducing any part of the report. *Download Algorithmic Audit Description - O'Neil Risk Consulting & Algorithmic Auditing*, HireVue, https://www.hirevue.com/resources/template/orcaa-report.
[154] Hirevue, *supra* note 152.
[155] Alex C. Engler, *Independent auditors are struggling to hold AI companies accountable*, Fast Company (Jan. 26, 2021), https://www.fastcompany.com/90597594/ai-algorithm-auditing-hirevue.
[156] *See supra* notes 73–75 and accompanying text.
[157] *Gender Shades*, MIT Media Lab, https://www.media.mit.edu/projects/gender-shades/overview/.
[158] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2018).
[159] "Collect" means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means. The State Data Privacy Act at 10.
[160] "Process" and "processing" mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion, or modification of personal data. Id. at 13.
[161] "Sensitive data" means personal data that includes:
(A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, status as transgender or non-binary, union membership, income level or indebtedness, or citizenship or immigration status;
(B) consumer health data;
(C) genetic or biometric data;
(D) personal data of a consumer that a controller knew or should have known, based on knowledge fairly implied under objective circumstances, is a minor;
(E) precise geolocation data;
(F) a government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public
(G) the online activities of a consumer (or device linked or reasonably linkable to a consumer) over time and across websites, online applications, or mobile applications that do not share common branding, or data generated by profiling performed on such data.
(E) precise geolocation data;
(F) a government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public;
(G) the online activities of a consumer (or device linked or reasonably linkable to a consumer) over time and across websites, online applications, or mobile applications that do not share common branding, or data generated by profiling performed on such data.
Id. at 15.
[162] *See infra* Part IV.b.2.
[163] EPIC CPPA March 2023 Comments at 41–42.
[164] *Id*. at 42.
[165] *Id*. at 29.
[166] *Id*. at 42.
[167] Robert Hart, *Clearview AI—Controversial Facial Recognition Firm—Fined $33 Million For 'Illegal Database'*, Forbes (Sept. 3, 2024), https://www.forbes.com/sites/roberthart/2024/09/03/clearview-ai-controversial-facial-recognition-firm-fined-33-million-for-illegal-database/.
[168] *Join Our Team*, Clearview AI, https://www.clearview.ai/careers.
[169] Kara Williams, EPIC, AI Legislation Scorecard: A Rubric for Evaluating AI Bills 2 (2024), https://epic.org/wp-content/uploads/2024/06/EPIC-AI-Legislation-Scorecard-June2024.pdf.

[170] *Id*.
[171] *Id*.
[172] Vedan Anthony-North, *supra* note 61.
[173] *Id*.
[174] Privacy Impact Assessment v (David Wright & Paul de Hert, eds., 2012) (foreword by Gary T. Marx) at 5–6.
[175] EPIC CPPA March 2023 Comments at 38.
[176] Off. of Mgmt. & Budget, Exec. Off. of the President, OMB Circular A-130: Managing Information as a Strategic Resource app. II at 10 (2016).
[177] Assembling Accountability at 20–21.
[178] EPIC CPPA March 2023 Comments at 38–41l; EPIC CPPA Feb. 2025 Comments at 37.
[179] Comments of EPIC to the Off. Of Mgmt. and Budget on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, 22 (Dec. 5, 2023), https://epic.org/wp-content/uploads/2023/12/EPIC-OMB-AI-Guidance-Comments-120523-1.pdf [hereinafter *EPIC Comment on OMB AI Memo*].
[180] EPIC CPPA Feb. 2025 Comments at 35–37.
[181] *Id*. In the GDPR context, the lack of enforcement and public scrutiny had led to lax compliance. Noyb – European Center for Digital Rights, GDPR: A Culture of Non-Compliance? (Jan. 2024), https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance.pdf.
[182] EPIC CPPA Feb. 2025 Comments at 37.
[183] Comments of EPIC to the Homeland Security Department (July 12, 2021), https://epic.org/wp-content/uploads/apa/comments/EPIC-Comment-DHS-Emerging-Technologies-July2021.pdf.
[184] *See also* EPIC CPPA March 2023 Comments; EPIC FTC Comments on Commercial Surveillance at 163–64; EPIC Comment on OMB AI Memo.
[185] The State Data Privacy Act at 10, 13.
[186] Tamara Kneese, *Measuring Justice: Field Notes on Algorithmic Impact Assessments*, Data & Society (Jan. 10, 2024), https://datasociety.net/points/measuring-justice-field-notes-on-algorithmic-impact-assessments/.
[187] Mark Latonero & Aaina Agarwal, Carr Center for Human Rights Policy at Harvard Kennedy School, Human Rights Impact Assessments for AI: Learning from Facebook's Failure in Myanmar (2021), https://www.hks.harvard.edu/sites/default/files/2023-11/2021_13_facebook-failure-in-myanmar_0.pdf.
[188] Assembling Accountability at 26.
[189] November 2024 Proposed Regulations § 7152(a)(5)(I).
[190] Assembling Accountability at 45–46.
[191] *See* Leonardo Horn Iwaya, Ala Sarah Alaqra, Marit Hansen & Simone Fischer- Hübner, *Privacy impact assessments in the wild: A scoping review*, Array vol. 23 (Sept. 2024), https://www.sciencedirect.com/science/article/pii/S2590005624000225.
[192] *See* Dyann Heward-Mills, *See The DPO must be independent, but how?,* IAPP (Aug. 27, 2019), https://iapp.org/news/a/the-dpo-must-be-independent-but-how.
[193] *See* Gerchick & Akselrod, *supra* note 60.
[194] *See* Winters, *supra* note 147.
[195] *See* Gemma Galdon Clavell, European Data Protection Board, Checklist for AI Auditing (2023), https://www.edpb.europa.eu/system/files/2024-06/ai-auditing_checklist-for-ai-auditing-scores_edpb-spe-programme_en.pdf.
[196] *Id*.
[197] Assembling Accountability at 5.
[198] *See supra* note 78.
[199] *See supra* notes 80–81. *See also* Comments of EPIC to the U.S. Commission on Civil Rights (April 8, 2024), https://epic.org/documents/comments-of-epic-to-u-s-commission-on-civil-rights-on-facial-recognition-technology/; U.S. Commission on Civil Rights, The Civil Rights Implications of the

Federal Use of Facial Recognition Technology (Sept. 2024), https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf. "In fact, the greater FRT's technical accuracy the greater the threat from the government's potential misuse of it poses to political freedom and dissent." *Id*. at 157.

[200] Caitriona Fitzgerald, Kara Williams, R.J. Cross, Ellen Hengesbach, EPIC & U.S. PIRG Education Fund, The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better (Jan. 2025), https://epic.org/wp-content/uploads/2025/04/EPIC-PIRG-State-of-Privacy-2025.pdf; Kara Williams, EPIC, AI Legislation Scorecard: A Rubric for Evaluating AI Bills 2 (2024), https://epic.org/wp-content/uploads/2024/06/EPIC-AI-Legislation-Scorecard-June2024.pdf.

[201] EPIC FTC Comments on Commercial Surveillance at 33–66.

[202] *Id*.

[203] Comments of EPIC to the U.S. Commission on Civil Rights (April 8, 2024), https://epic.org/documents/comments-of-epic-to-u-s-commission-on-civil-rights-on-facial-recognition-technology/; Comments of EPIC to Dutch Data Protection Authority (Dec. 17, 2024), https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/.

[204] Throughout this report, we have been using the term "automated decision system (ADS)" to describe AI that is used to make or facilitate human decisionmaking. Because California's proposed regulations use the term "automated decisionmaking technology (ADMTs)" to describe the same technology, we will use that term in the section discussing the proposed regulations.

[205] *Frequently Asked Questions,* California Privacy Protection Agency, https://cppa.ca.gov/faq.html.

[206] *California Consumer Privacy Act*, State of California Dep't of Justice, https://oag.ca.gov/privacy/ccpa.

[207] *Id*.

[208] *Text of the California Privacy Rights Act*, Californians for Consumer Privacy, https://www.caprivacy.org/cpra-text/.

[209] *California's Proposition 24*, EPIC, https://epic.org/californias-proposition-24/.

[210] Laws & Regulations, California Privacy Protection Agency, https://cppa.ca.gov/regulations/index.html.

[211] Cal. Civ. Code § 1798.199.55(a), § 1798.199.90(c).

[212] Cal. Civ. Code § 1798.185 (a)14(B).

[213] *Id*.

[214] *Laws & Regulations*, California Privacy Protection Agency, https://cppa.ca.gov/regulations/.

[215] Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, § 7001 (May 9, 2025), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [hereinafter *May 2025 Proposed Regulations*].

[216] Kara Williams, Testimony on the California Privacy Protection Agency's Draft Regulations on ADMT, Risk Assessments, and Cybersecurity, EPIC (May 2025), https://epic.org/documents/california-testimony-on-the-california-privacy-protection-agencys-draft-regulations-on-admt-risk-assessments-and-cybersecurity/.

[217] *See supra* Part I.

[218] Bogert, Schecter & Watson, *supra* note 3.

[219] Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, § 7001(f) (Nov. 22, 2024) https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [hereinafter *November 2024 Proposed Regulations*].

[220] November 2024 Proposed Regulations § 7001(f)(2).

[221] November 2024 Proposed Regulations § 7001(f)(2).

[222] *See supra* Part I.c.4: Housing; Screened Out of Housing.

[223] May 2025 Proposed Regulations § 7001(e) (emphasis added).

[224] May 2025 Proposed Regulations § 7001(e)(2).

[225] May 2025 Proposed Regulations § 7001(e).
[226] *See* Bogen & Rieke, *supra* note 57.
[227] *See supra* note 79.
[228] *See* McBrien, Winters, Zhou & Eubanks, *supra* note 88; Screened Out of Housing.
[229] Patrick Rucker, Maya Miller & David Armstrong, *How Cigna Saves Millions by Having Its Doctors Reject Claims Without Reading Them*, ProPublica (March 25, 2023), https://www.propublica.org/article/cigna-pxdx-medical-health-insurance-rejection-claims; Casey Ross & Bob Herman, *UnitedHealth pushed employees to follow an algorithm to cut off Medicare patients' rehab care*, STAT (Nov. 14, 2023), https://www.statnews.com/2023/11/14/unitedhealth-algorithm-medicare-advantage-investigation/.
[230] Local Law 2021/144, The New York City Council Legislative Research Center, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=ID%7CText%7C&Search=.
[231] Grace Gedye, *New Research: NYC Algorithmic Transparency Law is Falling Short of Its Goals*, Consumer Reports (Feb. 8, 2024), https://innovation.consumerreports.org/new-research-nyc-algorithmic-transparency-law-is-falling-short-of-its-goals/.
[232] *Id*.
[233] May 2025 Proposed Regulations § 7150(b)(1).
[234] May 2025 Proposed Regulations § 7150(b)(2).
[235] "Sell," "selling," "sale," or "sold,'' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration. Cal. Civ. Code § 1798.140 (ad)(1).
"Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged. *Id*. § 1798.140 (ah) (1).
[236] "Significant decision" in the November 2024 version was defined as "decision… that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g. posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel)." *Id*. § 7200(a)(1).
[237] "Extensive profiling" included "(A) profiling a consumer through systematic observation when they are acting their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ('work or educational profiling'); (B) Profiling a consumer through systematic observation of a publicly accessible place ('public profiling'); or (C) profiling a consumer for behavioral advertising." *Id*. § 7200 (a)(1). "Profiling" was defined in the November 2024 version as "any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements." *Id*. § 7001 (kk).
[238] November 2024 Proposed Regulations § 7150 (b)(3).
[239] May 2025 Proposed Regulations § 7001(ddd).
[240] *See supra* note 76.
[241] May 2025 Proposed Regulations § 7001(ddd).
[242] *Surveillance Advertising: What About Discrimination?*, Consumer Federation of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-discrimination/; Julia Angwin, Noam Scheiber & Ariana Tobin, *Dozens of Companies Are Using Facebook to Exclude Older Workers from Job Ads*, ProPublica (Dec. 20, 2017),

https://www.propublica.org/article/facebook-ads-age-discrimination-targeting; Ariana Tobin & Jeremy B. Merrill, *Facebook Is Letting Job Advertisers Target Only Men*, ProPublica (Sept. 18, 2018), https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men.
[243] Charge of Discrimination, HUD, et al v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.
[244] Press Release, *New Lawsuit Challenges Big Tech Firm Meta for Discrimination in Advertising Higher Education Opportunities*, Lawyers' Committee for Civil Rights Under Law (Feb. 11, 2025), https://www.lawyerscommittee.org/new-lawsuit-challenges-big-tech-firm-meta-for-discrimination-in-advertising-higher-education-opportunities/.
[245] May 2025 Proposed Regulations § 7001(aaa).
[246] *See supra* notes 84-86 and accompanying text.
[247] November 2024 Proposed Regulations § 7200(a)(3).
[248] May 2025 Proposed Regulations § 7150(b)(6).
[249] May 2025 Proposed Regulations § 7150(b)(6)(D)-(E) (struck).
[250] Maggie Harrison Dupré, *AI Is Being Trained on Images of Real Kids Without Consent*, Futurism (June 12, 2024), https://futurism.com/ai-trained-images-kids; Vittoria Elliott, *AI Tools Are Secretly Training on Real Images of Children*, Wired (June 10, 2024), https://www.wired.com/story/ai-tools-are-secretly-training-on-real-childrens-faces/; Vish Gain, *Grok AI is training on user data by default – here's how to stop it*, Silicon Republic (July 29, 2024), https://www.siliconrepublic.com/business/grok-ai-training-x-twitter-default-user-data-privacy-turn-off; https://therecord.media/linkedin-lawsuit-private-messages-ai-training; Suzanne Smalley, *LinkedIn sued for allegedly training AI models with private messages without consent*, The Record (Jan. 23, 2025), https://thehackernews.com/2025/05/meta-to-train-ai-on-eu-user-data-from.html.
[251] Chris Tozzi, *How bad is generative AI data leakage and how can you stop it?*, Tech Target (Dec. 19, 2024), https://www.techtarget.com/searchenterpriseai/answer/How-bad-is-generative-AI-data-leakage-and-how-can-you-stop-it.
[252] Barbara Ortutay, *President Trump signs Take It Down Act, addressing nonconsensual deepfakes. What is it?*, AP (May 20, 2025), https://apnews.com/article/take-it-down-deepfake-trump-melania-first-amendment-741a6e525e81e5e3d8843aac20de8615; *Governor Newsom signs bills to combat deepfake election content*, Office of Gov. Gavin Newsom (Sept. 17, 2024), https://www.gov.ca.gov/2024/09/17/governor-newsom-signs-bills-to-combat-deepfake-election-content/; Zach Williams, *New York Bans Deepfake Revenge Porn Distribution as AI Use Grows*, Bloomberg Law (Oct. 2, 2023), https://news.bloomberglaw.com/in-house-counsel/n-y-outlaws-unlawful-publication-of-deepfake-revenge-porn; Bill Kramer, *More and More States Are Enacting Laws Addressing AI Deepfakes*, MultiState (April 5, 2024), https://www.multistate.us/insider/2024/4/5/more-and-more-states-are-enacting-laws-addressing-ai-deepfakes.
[253] May 2025 Proposed Regulations § 7152.
[254] *Id*. § 7152(a)(4)–(5).
[255] Cal. Civ. Code § 1798.185(a)(14)(B).
[256] *Id.*
[257] May 2025 Proposed Regulations § 7152(a).
[258] *Id*. § 7152(a).
[259] Cal. Civ. Code § 1798.100(c).
[260] May 2025 Proposed Regulations § 7152(a)(5)(E) (struck).
[261] *See supra* notes 29–33, 94–97 and accompanying text.
[262] May 2025 Proposed Regulations § 7152(a)(6).
[263] November 2024 Proposed Regulations § 7152 (a)(2)(B).
[264] *Id*. § 7152 (a)(2)(B)(i)-(ii) (summarized).
[265] May 2025 Proposed Regulations § 7152 (a)(6)(A).
[266] *Id*. § 7152 (6)(B)(i).
[267] November 2024 Proposed Regulations § 7154.
[268] May 2025 Proposed Regulations § 7154.

[269] November 2024 Proposed Regulations § 7257(b)(2).
[270] Cal. Civ. Code § 1798.199.40(d).
[271] "The agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title." *Id* § 1798.199.65.
[272] *See* EPIC CPPA Feb. 2025 Comments.
[273] Khari Johnson, *California Regulator Weakens AI Rules, Giving Big Tech More Leeway to Track You*, Cal Matters (May 7, 2025), https://calmatters.org/economy/technology/2025/05/california-regulator-weakens-ai-rules-giving-big-tech-more-leeway-to-track-you/.
[274] Patrice Taddonio, *WATCH: Inside Facebook's Early Days*, PBS (Oct. 29, 2018), https://www.pbs.org/wgbh/frontline/article/watch-inside-facebooks-early-days/.
[275] Courtney Radsch, *Meta and Mark Zuckerberg must not be allowed to shape the next era of humanity*, Guardian (Feb. 4, 2024), https://www.theguardian.com/commentis-free/2024/feb/04/mark-zuckerberg-meta-facebook-ai-future-accountability.
[276] Jennifer Sheridan, *California legislators challenge independence of CPPA rulemaking authority*, IAPP (Apr. 2, 2025), https://iapp.org/news/a/california-legislators-challenge-independence-of-cppa-rulemaking-authority; Tyler Katzenberger, *Echoing Big Tech, Newsom warns privacy watchdog on AI*, Politico (Apr. 24, 2025), https://www.politico.com/news/2025/04/24/newsom-california-privacy-cppa-ai-00307233; Jeremy B. White, *Newsom sends prepaid phones, aka 'burners,' to tech CEOs*, Politico (Mar. 18, 2025), https://www.politico.com/news/2025/03/18/newsom-ceos-burner-phones-00235044.
[277] Cal. Civ. Code § 1798.185(a)(14)(b).
[278] *Id*.
[279] *Id.* § 1798.185(a)(15).
[280] ACLU California Action, et al., *Re: Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations*, ACLU of Northern California (Feb. 19, 2025), https://www.aclunc.org/sites/default/files/2025-02-19%20ACLU%20CA%20Action%20EPIC%20EFF%20CFA%20PRC%20CPPA%20Comments.pdf.
[281] *White v. Davis*, 13 Cal.3d at 775 (citing ballot argument).
[282] Kara Williams, *Assessing the Assessments: Comparing Risk Assessment Requirements Around the World*, EPIC (Dec. 4, 2023), https://epic.org/impact-comparison/.
[283] Cal. Civ. Code § 1798.100(c).
[284] *Id*. § 1798.135.
[285] Standardized Regulatory Impact Assessment: California Privacy, 57 (Oct. 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.
[286] ISOR Appendix A, pp. 57-58, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.
[287] *Id*.
[288] *Id.* at 70.
[289] *Id.* at 77.
[290] *Id.* at 64.
[291] *Id.* at 81.
[292] *Id.* at 81.
[293] *Id.* at 82.
[294] Calli Schroeder, Ben Winters, & John Davisson, *We Can Work It Out: The False Conflict Between Data Protection and Innovation*, 20 Colo. Tech. L. J. 251, 259, citing *Most Innovative Companies Apple*, Fast Company, https://www.fastcompany.com/company/apple [https://perma.cc/DRG7-49XE].
[295] AB 1018 2025-2026 Leg. (CA 2025), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB1018.

[296] *Irish Data Protection Commission fines LinkedIn Ireland €310 million*, Data Protection Commission (Oct. 24, 2024), https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million; *Data Protection Commission announces decision in WhatsApp inquiry*, Data Protection Commission (Sept. 2, 2021), https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry; *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, European Data Protection Board (Jan 21, 2019), https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en; *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies*, Ken Paxton, Attorney General of Texas (Jan 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45; Press Release, FTC, *FTC Order Requires Workado to Back Up Artificial Intelligence Detection Claims* (April 28, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-order-requires-workado-back-artificial-intelligence-detection-claims; Press Release, FTC, *FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent* (Jan 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data; Press Release, FTC, *FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data* (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data; *Privacy Enforcement Actions*, State of California Dep't of Justice, https://oag.ca.gov/privacy/privacy-enforcement-actions.

epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER