CENTER FOR DEMOCRACY & TECHNOLOGY

March 27, 2023

To: Kevin Sabo
California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Re: Invitation for Preliminary Comments on Proposed Rulemaking Regarding Cybersecurity Audits, Risk Assessments, and Automated Decision-making, PR 02-2023

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the California Privacy Protection Agency's (Agency) invitation for preliminary comments on its proposed rulemaking regarding cybersecurity audits, risk assessments, and automated decision-making.[1] CDT is a nonprofit 501(c)(3) organization dedicated to advancing privacy, consumer, and civil rights for all in the digital age. CDT's work includes a focus on automated decision-making and effective safeguards for its use.[2]

The bulk of our comments address automated decision-making. We also include a section that addresses risk assessments, incorporating previously answered questions along the way.

Automated decision-making

Question 1: Laws requiring access and/or opt-out rights for automated decision-making

At least two other laws require access or opt-out rights in the context of automated decision-making: the federal Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA). However, both require only *access*, and only in a limited and indirect way. The FCRA

[1] California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking: Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, Feb. 10, 2023, https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf.

[2] CDT has continuously engaged in the Agency's proposed rulemaking pursuant to the California Privacy RIghts Act. *See* Center for Democracy & Technology, *CDT Provides Testimony for California Privacy Protection Agency on Automated Decisionmaking, Limited Sensitive Uses of Data + More* (May 12, 2022), https://cdt.org/insights/cdt-provides-testimony-for-california-privacy-protection-agency-on-automated-decisionmaking-limited-sensitive-uses-of-data-more/; Center for Democracy & Technology, *Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, Nov. 8, 2021, https://cdt.org/wp-content/uploads/2021/11/CDT-Comments-to-Cal-Privacy-Protection-Agency-on-CPRA-Rulemaking.pdf.

allows consumers to receive a free copy of their credit report once per year from each of the three major consumer credit reporting agencies.[3] This requirement allows the consumer to review credit-related information that informs credit decisions. The ECOA gives consumers who are denied credit the right to be told the specific reasons for the adverse credit decision.[4] Because most credit decisions today involve at least some automated decision-making, the effect of these laws is that the consumers can access *some* information about the automated decision-making process or an automated decision. However, these are limited access rights, and California should go beyond them, as recommended in response to Questions 3f and 9.

Question 2: Other requirements, frameworks, and/or best practices currently in use.

At this time, there are not widely accepted industry standards or frameworks for automated decision-making. We also cannot speak to the degree to which companies actually use, implement, or adhere to their own published standards or best practices in the context of automated decision-making, because companies are not required to disclose their decision-making practices to regulators or the public. Consequently, we would urge the Agency to exercise caution to the extent industry actors hold up their own published (or unpublished) standards and practices as potential regulatory models. The Agency should also consider how companies may refer to the National Institute of Standards and Technology's AI Risk Management Framework to inform their decision-making practices.[5]

Question 3f: Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations?

We would not recommend that the Agency consider these other requirements discussed in the previous sections.

We would instead urge the Agency to look to the European Union's General Data Protection Regulation (GDPR) as a model for access and opt-out rights. Under the GDPR, individuals have the right:

- To information on "the existence of automated decision-making . . . and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[,]"[6] and

[3] 15 U.S.C. §1681j(a)(1)(A).
[4] 15 U.S.C. §1691(d).
[5] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[6] General Data Protection Regulation, Art. 15.1(h).

- "[N]ot to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[7]

The Agency should also recognize that "automated decision-making" encompasses both (1) a system's design, training data, and logic and (2) the greater contexts in which the system is embedded and uses of its outputs.[8] Therefore, when developing regulations governing access and opt-out, we urge the Agency to allow consumers to opt out of companies' use of the consumers' data to train automated decision-making systems. This would ensure that consumers have true agency with respect to how companies use their data.

Questions 4: How companies are using automated decision-making
Question 5: Consumers' experiences and concerns regarding automated decision-making technology

Today, automated decision-making systems influence decisions in multiple critical areas, including housing, credit, employment, and education. People have little to no choice in being subjected to these systems to access the opportunities about which the systems make decisions, and people may not be able to anticipate these systems' harms. Unregulated and inappropriate data use can result in biased training data for AI systems, compound historical discrimination, and yield incorrect assumptions. Unfortunately, all too often, these risks are disproportionately borne by historically marginalized groups, including people of color, immigrants, Indigenous populations, women, people with disabilities, and the LGBTQ+ community.[9]

The resulting harms can take a number of different forms, and can occur for a number of reasons:

- Companies train these systems on data sets that do not accurately represent all people on which the systems are used – or conversely, the training data may incorporate substantial data that over-represents a particular protected class.

---

[7] General Data Protection Regulation, Art. 22.1.
[8] *See Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, *supra* note 2 (citing Hannah Quay-De La Vallee and Natasha Duarte, Center for Democracy & Technology, *Algorithmic Systems In Education: Incorporating Equity and Fairness When Using Student Data* 6-8 (2019), https://cdt.org/wpcontent/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf).
[9] *See generally* Andrew Crawford, Center for Democracy & Technology, *Placing Equity at the Center of Health Care & Technology* 13 (2022), https://cdt.org/wp-content/uploads/2022/03/2022-03-22-CDT-Placing-Equity-at-the-Center-of-Health- Care-Technology-final.pdf.

- Companies may design these systems to evaluate consumer data from which protected characteristics could be inferred, which could enable or result in discrimination.
- Companies may not design these systems to ensure that all people subject to the systems can successfully navigate and use them.
- Companies may fail to establish processes for auditing the systems for inaccuracies or biases sufficiently to address and correct all harms.

Note that these factors are not always intentional. System design often executes the priorities and policies of the companies developing and using these systems, as well as societal biases regarding which people are entitled to have their fundamental needs met. In particular, people with a range of different disabilities, including chronic illnesses and mental health disabilities, face significant discrimination by algorithm-driven decision-making systems in a wide swath of areas, both because of exclusionary design and because of discriminatory targeting or profiling. Companies are neglecting disability-specific considerations when their decision-making systems rely on training data and operations parameters that under-represent disabled people, and companies can enable targeting of disabled people when training data and parameters overrepresent disabled people. Yet, the lack of transparency in how these decision-making systems work makes it difficult for people to demonstrate that a data practice has violated current federal civil rights laws.

Below, we discuss how companies are misusing data-driven systems in ways that make it difficult for people to challenge the data practice responsible for discriminatory housing, credit, employment, education, and public benefits decisions.

i. Housing and credit

To inform mortgage and other lending decisions and to screen rental applicants, "fintech" companies deploy systems that evaluate credit history, employment and income data, banking and purchase activity, rental payment history, eviction records, arrest and court records, education history, and other data.[10] These data points are supposed to predict whether applicants will fulfill the obligations that come with the housing or loan opportunities for which

[10] Jung Choi, Karan Kaul, & Laurie Goodman, *FinTech Innovation in the Home Purchase and Financing Market*, Urban Inst. 9 (2019), https://www.urban.org/sites/default/files/publication/100533/fintech_innovation_in_the_home_purchase_and_financing_market_2.pdf; Karen Hao, *The Coming War on The Hidden Algorithms That Trap People in Poverty*, MIT Tech. Rev. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back/.

they are applying. However, many fintech companies' systems have been shown to charge higher interest rates to low-income and Black borrowers, and the systems are not designed to account for the context in which this data is generated.[11]

For instance, data about past arrest records, eviction proceedings, and financial, employment, and education history may not reflect people's *current* ability to make regular rental payments or loan repayments.[12] Meanwhile, data that would more reliably indicate current ability to make regular payments, such as recent history of on-time utility payments, is not considered.[13] As a result, people can remain trapped in a cycle of poor access to credit because they are punished for past records despite changes in their circumstances or qualifications. In addition, tenant screening companies like CoreLogic use algorithms that consider data such as arrest and eviction records, which are unreliable predictors for how applicants will treat other tenants or property.[14] Higher volumes of arrest data are generated in overpoliced neighborhoods, disproportionately affecting Black, Indigenous, and Latinx communities, disabled people, and transgender people. Landlords often evict tenants after calls to police related to domestic violence – as CDT has written, this occurs even more frequently for disabled people and people of color, and contributes to unreliable eviction data.[15]

Biometric data can also contribute to housing decisions. Besides tenant screening and other functions, property technology companies also provide video surveillance and facial recognition to monitor properties for any unpermitted activity or unauthorized presence, and biometric entry systems to prevent such situations.[16] In these cases, biometric data can also trigger

---

[11] Choi et al., *supra* note 6, at 10-11.
[12] Christopher K. Odinet, *The New Data of Student Debt*, 92 Southern Cal. L. Rev 1617, 1667 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349478; Center for Democracy & Technology, Comments to Financial Regulators on Financial Institutions' Use of Artificial Intelligence, Jul. 1, 2021, https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf.
[13] *Id.* at 1663; Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage Approval Algorithms*, The Markup (Aug. 25, 2021, 6:50 AM), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.
[14] Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Center for Democracy & Technology (July 7, 2021), https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/ [hereinafter Brown, *Tenant Screening Algorithms*].
[15] Am. Civ. Liberties Union, *Calling 911 Shouldn't Lead to an Eviction* (Mar. 15, 2022, 1:45 PM), https://www.aclu-wi.org/en/news/calling-911-shouldnt-lead-eviction.
[16] Avi-Asher Schapiro, *Good Business or Digital Bias? The Divisive Rise of 'Proptech',* Thomson Reuters (July 15, 2020, 5:14 PM), https://news.trust.org/item/20200715162819-bngcy; Anti-Eviction Mapping Project, Landlord Tech Watch, https://antievictionmappingproject.github.io/landlordtech/.

evictions or arrests, further criminalizing people who are already disproportionately surveilled, and for whom facial analysis has been shown to produce unreliable matches.[17] Disabled people are currently at extraordinary risk of compounded discriminatory effects of rapidly expanding surveillance technologies. For instance, studies estimate up to 85% of incarcerated youth have learning or behavioral disabilities.[18] Use of tenant screening software, employment background checks, and predictive policing tools that inappropriately and sometimes illegally use arrest or conviction records thus has an outsized impact on disabled people, creating further inequities down the line in access to housing, employment, and social services.

Housing discrimination also occurs through targeted advertising, which has been shown to direct advertisements for critical opportunities and services to, or away from, certain categories of people who would be interested in acting on the advertisements. In such cases, targeted advertising can either deny these people access to information that could help them access opportunities and services, or relegate them to receiving advertisements for more unfavorable opportunities or products.[19] For example, a Department of Justice (DOJ) lawsuit alleged that Meta's advertising system enabled advertisers to use categories created based on race, color, religion, sex, disability, familial status, and national origin, and proxies for these characteristics, to designate eligible audiences for delivery of housing advertisements.[20]

While the companies responsible for data-driven discrimination in lending and housing should be subject to liability under federal civil rights laws, the lack of transparency from companies erects barriers for people to vindicate their civil rights even against entities that are subject to civil rights laws. The Fair Housing Act (FHA) prohibits discrimination in advertisements, offers, and sale or rental of housing on the basis of race, color, religion, sex, disability, familial status, or

---

[17] *See generally* Sophia Maalsen, Peta Wolifson, Dallas Rogers, Jacqueline Nelson, and Caitlin Buckle, AHURI, *Understanding Discrimination Effects in Private Rental Housing* (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916655. *See also* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings Of Machine Learning Research 2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[18] Daja E. Henry & Kimberly Rapanut, *How Schools and the Criminal Justice System Both Fail Students with Disabilities*, Slate (Oct. 21, 2020, 9:00 AM), https://slate.com/news-and-politics/2020/10/students-disabilities-criminal-justice-system.html.

[19] *See e.g.*, Julia Angwin & Terry Parris, Jr., *Facebook Says It Will Stop Allowing Some Advertisers to Exclude Users by Race*, ProPublica (Nov. 11, 2016, 10:00 AM), https://www.propublica.org/article/facebook-to-stop-allowing-some-advertisers-to-exclude-users-by-race.

[20] Department of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

national origin.[21] The Department of Housing and Urban Development (HUD) has warned that the use of criminal arrest records can violate the FHA because it can have a disparate impact based on race and national origin.[22] HUD has also advised that evictions following domestic violence-related calls to police can indicate disability or gender discrimination,[23] which can make housing decisions relying on eviction records more likely discriminatory as well. This has not deterred the use of tenant screening algorithms that include these records, though.[24]

HUD and other agencies have initiated efforts to address the ongoing harms of tenant screening algorithms. The CFPB published reports last fall examining the prevalence of tenant screening platforms and their impacts on housing access for marginalized renters, observing that while these tools can violate fair housing and consumer protection laws, renters are unable to dispute adverse outcomes arising from these tools.[25] HUD recently announced that it will issue guidance regarding how tenant screening algorithms can violate the FHA, and will work with the FTC, CFPB, and other agencies to release best practices for using tenant screening reports.[26] And the FTC and CFPB have since issued a request for information on tenant screening issues affecting the public, including the role of algorithm-based systems on these issues.[27]

The ECOA prohibits discrimination against applicants in any aspect of a credit transaction on the basis of race, color, religion, national origin, sex, marital status, age, or income derived from a public assistance program.[28] The CFPB issued guidance in 2022 stating that the ECOA requires creditors to provide people with a specific and accurate statement of principal reasons for

---

[21] 42 U.S.C. §3604 *et seq*.
[22] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions* (2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.
[23] Office of General Counsel, Department of Housing and Urban Development, *Guidance on Application of Fair Housing Act Standards to the Enforcement of Local Nuisance and Crime-Free Housing Ordinances Against Victims of Domestic Violence, Other Crime Victims, and Others Who Require Police or Emergency Services* (2016) https://www.hud.gov/sites/documents/FINALNUISANCEORDGDNCE.PDF.
[24] Brown, *Tenant Screening Algorithms*, *supra* note 10.
[25] *CFPB Reports Highlight Problems with Tenant Background Checks*, Nov. 15, 2022, https://www.consumerfinance.gov/about-us/newsroom/cfpb-reports-highlight-problems-with-tenant-background-checks/.
[26] The White House Blueprint for a Renters Bill of Rights (2023), https://www.whitehouse.gov/wp-content/uploads/2023/01/White-House-Blueprint-for-a-Renters-Bill-of-Rights.pdf.
[27] Federal Trade Commission, *FTC and CFPB Seek Public Comment on How Background Screening May Shut Renters Out of Housing* (Feb. 28, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-cfpb-seek-public-comment-how-background-screening-may-shut-renters-out-housing.
[28] 15 U.S.C. §1691(a).

adverse actions resulting from an algorithmic system.[29] Data practices that make or inform decisions regarding the extension of credit can violate the ECOA by using data that functions as proxies for these protected characteristics, but this does not extend to disability discrimination.

The ECOA requires creditors to inform credit applicants in writing about the reasons for an adverse credit decision or about the applicants' right to receive such a notice upon request, including for adverse actions resulting from algorithmic systems.[30] CDT has raised concerns about this form of notice to financial regulators, observing that it does not give applicants an opportunity to verify the accuracy of the data being evaluated during the approval process, or to provide additional information to supplement that data.[31] The ECOA also requires correction of inaccuracies in credit records upon request, which places responsibility on people to detect such errors, without clarity about which data contributed to the ultimate decision. Further, the ECOA offers limited recourse for targeted advertising – it protects people who actually apply for credit, extending to prospective applicants only insofar as it prohibits creditors from stating discriminatory preferences in advertising.[32]

ii. Employment

Algorithmic tools play a driving role in decisions including hiring, promotion, and termination. Vendors develop hiring technologies that aim to distinguish candidates in an applicant pool based on attributes they appear to have in common with other successful candidates and employees – in other words, attributes of people who have historically been hired more often.[33] Vendors market many of these tools as bias audited or less biased, without showing how (or even whether) the tools have been examined for disability bias.[34] Meanwhile, the tools collect and analyze data about candidates that is not relevant to candidates' ability to perform job

[29] Consumer Financial Protection Bureau, *Circular 2022-03: Adverse Action Notification Requirements in Connection With Credit Decisions Based on Complex Algorithms*, https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.
[30] *Id.*; 15 U.S.C. §1691(d)(2).
[31] Samir Jain & Ridhi Shetty, *Taking a Hard Line on AI Bias in Consumer Finance*, Center for Democracy & Technology, https://cdt.org/insights/taking-a-hard-line-on-ai-bias-in-consumer-finance/.
[32] 12 C.F.R. Supplement I to Part 1002, Paragraph 4(b).
[33] Miranda Bogen & Aaron Rieke, Upturn, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.
[34] *See* Manish Raghavan, Solon Barocas, Jon Kleinberg, & Karen Levy, *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 469 (2020), https://arxiv.org/pdf/1906.09208.pdf.

functions, causing workers to be rejected over irrelevant data related to marginalized identities.[35]

One such algorithm-driven hiring tool is resume screening. Ideal's resume screening software analyzes language and details in resumes, from candidates' names to affiliations to employment gaps, to identify whether the resumes reflect qualities the tools are designed to look for.[36] Taleo assigns bonus points for keywords in resumes that reflect attributes that are desired but not required.[37] As Amazon's now-discontinued resume screening tool demonstrated, resume screening tools can observe patterns in resumes that are moved forward in the hiring process and learn to filter out resumes with terms associated with women, such as women-oriented affiliation groups.[38] Such tools could similarly learn to exclude candidates based on data related to racial or ethnic identity.[39] Additionally, marginalized people who have previously experienced discrimination in their education, employment, or access to healthcare (especially if they face multiple forms of discrimination) might not get past screening tools that downgrade or screen out resumes before human reviewers can consider them. For instance, a disabled person may previously have had difficulty getting full-time employment, thus leading to gaps in their resume that will be flagged by such systems.[40]

Research by CDT and fellow advocates has raised concerns about other tools that purport to measure "soft skills" through gamified personality and aptitude assessments, or through

---

[35] *See* Hilke Schellmann, *Finding it Hard to Get a New Job? Robot Recruiters Might Be to Blame*, The Guardian (May 11, 2022, 4:30 PM), https://www.theguardian.com/us-news/2022/may/11/artitifical-intelligence-job-applications-screen-robot-recruiters (discussing how automated hiring technologies exhibit gender biases and use criteria such as names and data about non-professional activities).

[36] Ideal, *Screening*, https://ideal.com/product/screening/. *See also* Avi-Asher Schapiro, *AI is Taking Over Job Hiring, But Can it Be Racist?*, Thomson Reuters (Jun. 7, 2021, 7:04 AM), https://www.reuters.com/article/global-tech-ai-hiring/analysis-ai-is-taking-over-job-hiring-but-can-it-be-racist-idUSL5N2NF5ZC.

[37] James Hu, *Taleo: 4 Ways the Most Popular ATS Ranks Your Job Application*, Jobscan (Mar. 8, 2018), https://www.jobscan.co/blog/taleo-popular-ats-ranks-job-applications/.

[38] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women,* Thomson Reuters (Oct. 10, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[39] Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated Against Women*, American Civil Liberties Union (Oct. 12, 2018), https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against.

[40] Jim Fruchterman & Joan Mellea, Benetech, *Expanding Employment Success for People With Disabilities* (2018), https://benetech.org/about/resources/expanding-employment-success-for-people-with-disabilities-2/.

analysis of video interviews.[41] The use of such tools presumes that everyone demonstrates the traits employers look for – such as empathy, optimism, or adaptability – the same way. Paradox Traitify provides candidates with a series of images, requiring them to indicate whether they identify with what is depicted in each image to determine their alignment with a pseudoscientific personality model.[42] Pymetrics analyzes data collected while candidates complete a set of games to predict "cognitive and emotional attributes," which it claims to be "fairness-optimized" but has not been examined for disability bias.[43] Pymetrics was recently acquired by Harver, which implements "behavioral-based AI methodology" in soft skills assessments and automates matching of "high-potential" candidates.[44] Cappfinity's Koru uses a survey that requires candidates to select the responses with which they feel they align most, to assess soft skills.[45] Blind people and people with mobility impairments might not be able to adequately interface with a gamified assessment, while people with mental health disabilities or cognitive disabilities might have difficulty processing the information quickly enough to score well. Similarly, autistic and other neurodivergent people may be unable to answer correctly on personality tests that score candidates on characteristics unrelated to core competencies or essential functions of the job at hand.

HireVue has used video interview assessments that process data about how candidates physically appear, move, emote, and sound as they respond to interview questions. This treats candidates' eye contact, facial expressions, fidgeting, tics, vocabulary, and speech patterns as data points to infer personality traits such as confidence and trustworthiness.[46] HireVue has stated that it does not use video analysis or audio characteristics, but it analyzes personality

---

[41] Center for Democracy & Technology, *Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?* 11-12 (2020), https://cdt.org/wp-content/uploads/2020/12/Full-Text-Algorithm-driven-Hiring-Tools-Innovative-Recruitment-or-Expedited-Disability-Discrimination.pdf; Aaron Rieke, Urmila Janardan, Mingwei Hsu, and Natasha Duarte, Upturn, *Essential Work* (2021), https://www.upturn.org/work/essential-work/.

[42] Paradox, *Assessments*, https://www.paradox.ai/products/assessments; Olivia Goldhill, *We Took the World's Most Scientific Personality Test – and Discovered Unexpectedly Sexist Results* (Feb. 11, 2018), https://qz.com/1201773/we-took-the-worlds-most-scientific-personality-test-and-discovered-unexpectedly-sexist-results/.

[43] Pymetrics, *Assessments*, https://www.pymetrics.ai/assessments; Christo Wilson, Avijit Ghosh, Shan Jiang, Alan Mislove, Lewis Baker, Janelle Szary, Kelly Trindel, and Frida Polli, *Building and Auditing Fair Algorithms: a Case Study in Candidate Screening* (2021), https://evijit.github.io/docs/pymetrics_audit_FAccT.pdf.

[44] Harver, *Harver Acquires Pymetrics, Further Enhancing Talent Decision Capabilities Across the Employee Lifecycle* (Aug. 11, 2022), https://harver.com/press/harver-acquires-pymetrics/; Harver, *Assessments*, https://harver.com/software/assessments/; Harver, *Hiring Process Optimization*, https://harver.com/software/hiring-process-optimization/.

[45] Cappfinity, *Skills Identification*, https://www.cappfinity.com/cappfinity-product-page/assessment-cognitive-3/.

[46] Drew Harwell, *A Face-Scanning Algorithm Increasing Decides Whether You Deserve the Job*, Wash. Post (Nov. 6, 2019, 12:21 PM), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

traits and aptitudes by applying natural language processing to a transcription developed through an AI-driven speech-to-text service.[47] Disabled candidates who possess the traits that are necessary for successful job performance can nonetheless be scored unfairly by this type of tool, because their disabilities can cause them to demonstrate examined traits in ways that cannot be accurately captured through the analyzed data points.[48] This type of tool could also produce unfair scores for candidates of color or candidates who have been socialized to follow certain gender norms, as cultural norms can also affect speech patterns and eye contact.[49] HireVue also claims its product has been audited for fairness, but does not make its audit report available unless one provides their name, email address, and professional affiliation and agrees not to use any part of the audit report without HireVue's written authorization.[50] HireVue is now facing a class action lawsuit over its collection and use of biometric data.[51]

Companies are also increasingly developing and deploying sophisticated electronic surveillance to automate the monitoring and management of workers, whether they are in a warehouse, out making deliveries, at an office, or working remotely from home. CDT's report, *Warning: Bossware May Be Hazardous to Your Health*, examines companies' use of such automated systems, commonly referred to as "bossware," to perform a wide variety of monitoring tasks, such as tracking workers' location and movements, productivity and downtime, computer use, facial expressions, biometric markers, and frequency and length of bathroom and other breaks.[52] One system, Crossover's WorkSmart productivity tool, takes periodic screenshots and images of workstations to monitor what workers are doing.[53] Another company, Time Doctor,

---

[47] HireVue, *Explainability Statement* (2022), https://webapi.hirevue.com/wp-content/uploads/2022/03/HV_AI_Short-Form_Explainability_3152022.pdf.
[48] Matthew Scherer, *HireVue "AI Explainability Statement" Mostly Fails to Explain what it Does*, Center for Democracy & Technology (Sept. 8, 2022), https://cdt.org/insights/hirevue-ai-explainability-statement-mostly-fails-to-explain-what-it-does/.
[49] Goodman, *supra* note 35.
[50] HireVue, *Download IO Psychology Audit Description by Landers Workforce Science LLC*, https://www.hirevue.com/resources/template/hirevue-io-psychology-audit-report.
[51] Samantha Hawkins, *HireVue Attempts to Escape Biometrics Suit Over AI Interviews*, Bloomberg (June 22, 2022, 1:16 PM), https://news.bloomberglaw.com/privacy-and-data-security/hirevue-attempts-to-escape-biometrics-suit-over-ai-interviews.
[52] Jodi Kantor, Arya Sundaram, Aliza Aufrichtig, & Rumsey Taylor, *Workplace Productivity: Are You Being Tracked?*, N.Y. Times (Aug. 16, 2022, 10:03 AM), https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html; Spencer Soper, *Fired by Bot at Amazon: 'It's You Against the Machine'*, Bloomberg (June 28, 2021, 6:00 AM), https://www.bloomberg.com/news/features/2021-06-28/fired-by-bot-amazon-turns-to-machine-managers-and-workers-are-losing-out.
[53] Sean Captain, *In 20 Years, Your Boss May Track Your Every Glance, Keystroke, and HeartBeat*, Fast Company (Jan. 27, 2020), https://www.fastcompany.com/90450122/in-20-years-your-boss-may-track-your-every-glance-keystroke-and-heartbeat.

prevents workers from deleting screenshots to protect their privacy by deducting time worked during the period when screenshots were taken.[54] Some programs use workers' phones or computers to listen, watch, or monitor other sensors in their device, and can penalize workers for moving away from their workstation or slowing productivity.

Companies often use these technologies to optimize tasks for their own profit, but they put workers' health and safety at risk and threaten their privacy, autonomy, and dignity.[55] For example, Amazon has used productivity monitoring to monitor "time off task," which triggers warnings to workers for resting even when needed, putting them at risk of termination if they do not work at a pace that is dangerously fast.[56] Productivity monitoring also fails to capture work that is being performed offline or that cannot be accurately quantified through surveillance measures, and can punish and deter worker organizing.[57]

Many low-wage and hourly workers endure constant surveillance, often combined with algorithmic management systems that can discipline or even terminate them.[58] This exacerbates the already-wide gaps in information and bargaining power that low-wage workers face. Algorithmic tools further diminish gig workers' bargaining power, as they determine compensation and availability and termination of jobs.[59]

Low-wage workers marginalized on the basis of disability, race, ethnicity, and gender identity are at an even greater disadvantage. As many as 100,000 disabled workers are paid subminimum wages due to a provision in the Fair Labor Standards Act that allows employers to pay disabled workers commensurate with wages paid to non-disabled workers for "the same type, quality, and quantity of work" – effectively limiting disabled workers' wages based on their

---

[54] Matt Scherer, Center for Democracy & Technology, *Warning: Bossware May Be Hazardous to Your Health* 9 (2021), https://cdt.org/insights/report-warning-bossware-may-be-hazardous-to-your-health/ [hereinafter *Bossware*].
[55] *Id.* at 36.
[56] Deborah Berkowitz, *Packaging Pain: Workplace Injuries in Amazon's Empire*, Nat'l Emp. Law Project, https://www.nelp.org/publication/packaging-pain-workplace-injuries-amazons-empire/; Colin Lecher, *How Amazon Automatically Tracks and Fires Warehouse Workers for 'Productivity'*, The Verge (Apr. 25, 2019, 12:06 PM), https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.
[57] Kantor et al., *supra* note 48.
[58] Aiha Nguyen, *The Constant Boss: Labor Under Digital Surveillance*, Data & Society (2021), https://datasociety.net/library/the-constant-boss/.
[59] Federal Trade Commission, Policy Statement on Enforcement Related to Gig Work (Sept. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Matter%20No.%20P227600%20Gig%20Policy%20Statement.pdf.

challenges in meeting productivity expectations.[60] In other words, this provision allows an employer to pay a disabled worker only for the hours a non-disabled worker would take to complete the same work rather than the hours of labor the disabled worker has actually put in. Productivity monitoring systems can discriminate against disabled workers, pregnant or breastfeeding workers, older workers, and workers requiring religious prayer breaks by flagging breaks or slower pace of work, increasing the risk of injury to physical or mental health.[61] These effects are especially worse for people with physical, mental health, developmental, or cognitive disabilities.

Relatedly, more employers are relying on workplace wellness programs to increase worker productivity while reducing the cost of benefits claims for employers, even turning to gamified approaches to influence employees' behavior and personal health decisions.[62] Studies have shown that these programs do not deliver the intended positive effects on healthcare expenses or productivity.[63] Meanwhile, the programs impose expectations for physical exercise and diet that disabled workers may not be able to meet, and reinforce the higher societal value assigned to being "healthy."[64] To make matters worse, these programs pressure employees to provide health data that might make its way to third parties.[65]

While the discriminatory outcomes of hiring and algorithmic management technologies run afoul of federal employment discrimination laws, enforcement has not kept up with these technologies. For instance, Title I of the ADA prohibits adverse employment decisions based on

[60] Rebecca Vallas, Kim Knackstedt, Hayley Brown, Julie Cai, Shawn Fremstad, & Andrew Stettner, The Century Fdn. and Disability Econ. Just. Collaborative, *Economic Justice is Disability Justice* (2022), https://tcf.org/content/report/economic-justice-disability-justice/. Section 14(c) of the Fair Labor Standards Act allows employers to apply for special certificates to employ disabled workers at subminimum wages. 29 U.S.C. §214(c).

[61] *The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before House Comm. on Ed. & Labor, Civil & Human Serv. Subcomm.* (2020) (testimony of Jenny Yang, Senior Fellow, Urban Institute), https://edlabor.house.gov/imo/media/doc/YangTestimony02052020.pdf.

[62] *See* Joseph Sanford & Kevin Sexton, *Opinion: Improve Employee Health Using Behavioral Economics*, CFO (Feb. 3, 2022), https://www.cfo.com/human-capital/health-benefits/2022/02/employee-health-wellness-medical-claims-behavorial-economics/.

[63] Sally Wadyka, *Are Workplace Wellness Programs a Privacy Problem?*, Consumer Reports (Jan. 16, 2020), https://www.consumerreports.org/health-privacy/are-workplace-wellness-programs-a-privacy-problem-a2586134220/.

[64] *See* Lydia X. Z. Brown, Ridhi Shetty, Matthew U. Scherer, & Andrew Crawford, Center for Democracy & Technology, *Ableism And Disability Discrimination in New Surveillance Technologies* 54-55 (2022), https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/; Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 129-30, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211.

[65] *Id.*

workers' disability, and it requires employers to provide reasonable accommodations when doing so would not pose an undue hardship on employers.[66] Hiring and algorithmic management technologies provided by private companies can make or influence adverse decisions using disability-related data, without informing workers about how the technologies are collecting and analyzing their data, how this will influence employment decisions, and how workers might access accommodations that enable fairer evaluation.[67] Thus, workers may not have enough detail to pursue disability discrimination claims arising from these technologies' use. Similar issues plague enforcement of Title VII of the Civil Rights Act. The Equal Employment Opportunity Commission's draft Strategic Enforcement Plan for Fiscal Years 2023-2027 recognizes these issues, and the agency plans to dedicate resources to addressing employment discrimination related to the use of algorithm-driven hiring technologies.[68]

Beyond civil rights protections, there are few other laws or rules governing employers' use of surveillance technologies or safeguarding workers from their harmful effects. Workers have no concrete privacy rights under either federal law or the laws of most states. The Occupational Safety and Health Act prohibits practices that pose a risk of death or serious injury to workers, but the Occupational Safety and Health Administration's regulations do not cover many of the harms to workers' health that these technologies can impose, such as repetitive motion injuries and threats to workers' mental health. Gig workers are also not adequately protected under existing civil rights laws and the Occupational Health and Safety Act, which do not classify all workers as covered "employees."[69]

In addition, a new fact sheet from the Department of Labor regarding reporting requirements under the Labor-Management Reporting and Disclosure Act states that employers must report expenditures made for surveillance of employees and unfair labor practices, but only when the surveillance is used to obtain information connected to a labor dispute or the labor practices are intended to undermine the right to organize.[70]

---

[66] 42 U.S.C. §12112.
[67] *Algorithm-Driven Hiring Tools*, *supra* note 37.
[68] Center for Democracy & Technology, *CDT Comments Supporting EEOC's Recognition of Discriminatory Tech as an Enforcement Priority*, Feb. 9, 2023, https://cdt.org/insights/cdt-comments-supporting-eeocs-recognition-of-discriminatory-tech-as-an-enforcement-priority/.
[69] Scherer, *Bossware*, *supra* note 50, at 16.
[70] Jeffrey Freund, *How We're Ramping Up Enforcement of Surveillance Reporting*, Department of Labor Blog (Sept. 15, 2022), https://blog.dol.gov/2022/09/15/how-were-ramping-up-our-enforcement-of-surveillance-reporting; Office of Labor-Management Standards, U.S. Department of Labor, *OLMS Fact Sheet on Form LM-10 Employer Reporting: Transparency Concerning Persuader, Surveillance, and Unfair Labor Practices Expenditures*, https://www.dol.gov/sites/dolgov/files/OLMS/regs/compliance/LM10_FactSheet.pdf.

iii. Education

Public sector services, from education to governmental benefits, regularly involve the collection of personal data. Students and families may be subjected to data practices that worsen inequity throughout the education context, from the use of cameras equipped with computer vision on campus, to algorithms that make critical decisions about students' lives, to software that monitors everything students do online — often through technology sold by private contractors. Those uses of data and technology surveil students often without meaningful consent or opportunity to opt out because they are a condition for students' ability to access a fundamental service — their education.

CDT has researched student activity monitoring software, a type of school surveillance technology that allows schools to view students' screens, record their browsing and search histories, and scan their messages and documents stored online or on school devices.[71] The results showed that surveillance is pervasive: 89 percent of teachers report that their school uses student activity monitoring software,[72] and monitoring often occurs even outside of school hours. Although vendors claim that student activity monitoring and other forms of commercial surveillance benefit students, those claims are largely unsubstantiated.[73]
Instead, monitoring violates rights traditionally protected by civil rights laws.[74] Further, students experiencing poverty and students of color rely more heavily on school-issued devices, which are more likely to be subject to monitoring than personal devices.[75] As a result, these groups of

[71] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: The Misleading Promise of Monitoring Students Online* (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of- monitoring-students-online [hereinafter *Hidden Harms*].
[72] *Id.* at 8.
[73] Center for Democracy & Technology & Brennan Center for Justice, Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns (2019), https://cdt.org/insights/social-media-monitoring-in-k-12-schools-civil-and-human-rights-concerns; *see also* Rebecca Heilweil, *The Problem with Schools Turning to Surveillance After Mass Shootings*, Vox (June 2, 2022, 7:30 AM), https://www.vox.com/recode/23150863/school-surveillance-mass-shooting- texas-uvalde; Lucas Ropek, *Surveillance Tech Didn't Stop the Uvalde Massacre*, Gizmodo (May 27, 2022), https://gizmodo.com/surveillance-tech-uvalde-robb-elementary-school-shootin-1848977283; Jolie McCollough & Kate McGee, *Texas Already "Hardened" Schools. It Didn't Save Uvalde.*, Texas Tribune (May 26, 2022), https://www.texastribune.org/2022/05/26/texas-uvalde-shooting-harden-schools;
[74] *Hidden Harms*, *supra* note 67, at 19-24.
[75] DeVan L. Hankerson Madrigal, Cody Venzke, Elizabeth Laird, Hugh Grant-Chapman, & Dhanaraj Thakur, Center for Democracy & Technology, *Online and Observed: Student Privacy Implications of School-Issued Devices and Student Activity Monitoring Software* 10 (Sept. 21, 2021), https://cdt.org/insights/report-online-and-observed-student-privacy-implications-of-school-issued-devices-and-student-activity-monitoring-software/; Hugh Grant-Chapman & Elizabeth Laird, Center for Democracy & Technology, *Research Slides: Key Views Toward Ed Tech, School Data, and Student Privacy* 48 (Nov. 15, 2021), https://cdt.org/insights/report-navigating-the-new-normal-ensuring-equitable-and-trustworthy-edtech-for-the-future.

students are similarly subject to increased risks of discrimination. These incursions on students' fundamental rights are a betrayal of schools' role as "the nurseries of democracy."[76]

National reporting has also underscored the harms caused by commercial surveillance in education. Students with disabilities are at higher risk of generating false positives and false negatives when surveilled by student monitoring tools that are designed to identify atypical sounds, text, speech, or movements as potential indicators that students may be engaging in violent or prohibited conduct, making threats, or cheating on tests. For instance, a ProPublica investigation found that aggression-detection microphones were so unreliable that they flagged loud laughter and locker doors slamming as indicators of violence.[77] Those false positives raise concerns for students whose disabilities affect their speech and movement, such as students with cerebral palsy who might not be able to modulate voice volume or students with Tourette's who have loud vocal tics.

Meanwhile, student advocacy organizations such as the National Disabled Law Students Association have documented the discriminatory barriers that students with a wide range of disabilities, including ADD, blindness, and Crohn's disease, experience when required to use automated proctoring software.[78] Students reported not being permitted to take enough bathroom breaks, worrying about false positives from needing to move or pace, or not moving their eyes or hands the right way. For disabled students of color or LGBTQ+ students with disabilities, who also face additional discrimination and prejudice, the risks of student monitoring and commercial surveillance programs are further compounded.

Although existing laws address many of the impacts of the uses of data and technology on civil rights, they do not cover all harms to historically marginalized groups of people who are not recognized as a legally protected class, such as unhoused students, low-income students, foster care students, and rural students. Title VI[79] and Title IX[80] of the Civil Rights Act prohibit discrimination on the basis of race, sex, and related classes by entities receiving certain federal funds, including in the education sector. However, when discrimination is caused by technology

[76] Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2046 (2021).
[77] Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.
[78] National Disabled Law Students Association, *Report on Concerns Regarding Online Administration of Bar Exams* (2020), https://ndlsa.org/wp-content/uploads/2020/08/NDLSA_Online-Exam-Concerns-Report1.pdf.
[79] 42 U.S. Code § 2000d.
[80] 20 U.S.C. §§ 1681–1688.

distributed by private contractors for schools, students and families may not be aware of the discriminatory impact, due to a lack of transparency around the implementation and utilization of technological systems. Schools have very little ability to gain insight into contractors' data practices, no matter how reasonable their precautions, and this prevents them from providing parents with adequate notice. Schools, families, and students are consequently dependent on contractors' representations regarding data use, and need transparency regarding contractors' collection and use of student data.

Students and families do not have a meaningful choice in whether to consent to the surveillance. Students are often required or encouraged to use school-issued devices that are subject to monitoring,[81] or they may rely on school-issued devices because of their families' socioeconomic status.[82] Further, students and families are often not provided accurate, complete disclosures around commercial surveillance in education. For example, in recent CDT research, 47 percent of parents reported they were not informed about how their schools' contractors collect data about students' activity online; only 39% reported they were asked for input on those practices.[83] Even if students and families are provided adequate disclosures, they are typically not given a choice (whether opt-in or opt-out) with respect to whether and how schools or their contractors monitor student online activity. Moreover, it may be impractical or even impossible for students and families to switch schools to avoid their commercial surveillance practices.

For example, an algorithmic system used to assign students to schools may rely on a variety of factors, not all of which may be known to students and families.[84] This information asymmetry may make it difficult or impossible to challenge discriminatory practices caused by data or technology use. In interviews, school IT leaders stated they took strides through contractual measures to hold contractors accountable for their uses of student data, and expressed frustration with "what they describe as a lack of distinguishable options for privacy-forward

[81] Hankerson Madrigal et al., *supra* note 71, at 10.
[82] *Id.*
[83] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, & Hannah Quay-de la Vallee, Center for Democracy & Technology, *Hidden Harms: Research Slide Deck* 30–32 (2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online.
[84] Hannah Quay-de la Vallee & Natasha Duarte, Center for Democracy & Technology, *Algorithmic Systems in Education* 8-9 (2019), https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/.

devices."[85] Similarly, 94 percent of parents and 88 percent of students stated it was "important" for schools to engage them on the uses of student data.[86]

Title VI[87] and Title IX[88] prohibit entities receiving certain federal funds from acquiring discriminatory technology, but would not preclude private vendors from selling it in the first place. Further, certain uses of data and technology may not intentionally discriminate against people based on race, sex, disability status, or other protected classes, but nonetheless cause disparate impact. Courts, however, have curtailed people's ability to challenge disparate impact under critical civil rights laws in court,[89] limiting their ability to seek redress. CDT has called on the Office for Civil Rights in the U.S. Department of Education to address harms from some uses of data and technology on students of color, students with disabilities, and LGBTQ+ students.[90]

Lax data security practices by private contractors in the education sector also cause harm by undermining students' and families' trust in schools and contractors, and putting their financial and physical wellbeing at risk. Lax data security practices can result in breaches and other data security incidents, which have substantially increased in both number and scope since 2016 and strained schools' resources.[91] For example, one recent incident involved a contractor serving schools in six states, affecting over three million current and former students.[92] Similarly, a

---

[85] Hankerson Madrigal et al., *supra* note 71, at 17.
[86] *Hidden Harms*, *supra* note 67, at 18.
[87] 42 U.S. Code § 2000d.
[88] 20 U.S.C. §§ 1681–1688.
[89] *E.g.*, Jackson v. Birmingham Bd. of Educ., 544 U.S. 167, 178, 178 n.2 (2005) (Title IX); Alexander v. Sandoval, 532 U.S. 275 (2001) (Title VI); Doe v. BlueCross BlueShield of Tenn., Inc., 926 F.3d 235, 240-42 (6th Cir. 2019).
[90] Center for Democracy & Technology, *Comment on Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance*, Docket No. ED-2021-OCR-0166 (filed Sept. 12, 2022), https://cdt.org/insights/cdt-urges-us-department-of-education-to-protect-lgbtqi-students-from-discrimination-in-proposed-title-ix-rules; Letter to Catherine Lhamon, Assistant Secretary for Civil Rights, U.S. Department of Education, from Coalition of Civil, Digital, and Education Rights Organizations (filed Aug. 2, 2022), https://cdt.org/insights/letter-to-ed-office-for-civil-rights-on-discriminatory-effects-of-online-monitoring-of-students/; Center for Democracy & Technology, *Comments on Request for Information Regarding the Nondiscriminatory Administration of School Discipline*, Docket No. ED-2021-OCR-0068 (filed July 23, 2022), https://cdt.org/insights/cdt-comments-to-us-dept-of-ed-urging-the-protection-of-students-of-color-and-students-with-disabilities-and-their-data; Center for Democracy & Technology, *Comments on Announcement of Public Hearing; Title IX of the Education Amendments of 1972*, 86 Fed. Reg. 27429 (filed June 11, 2021), https://cdt.org/insights/cdt-comments-on-protecting-privacy-rights-and-ensuring-equitable-algorithmic-systems-for-transgender-and-gender-non-conforming-students/.
[91] K12 SIX, State of K-12 Cybersecurity 3 (2022), https://www.k12six.org/the-report.
[92] Mark Keierleber, *After Huge Illuminate Data Breach, Ed Tech's 'Student Privacy Pledge' Under Fire*, The 74 (July 24, 2022), https://www.the74million.org/article/after-huge-illuminate-data-breach-ed-techs-student-privacy-pledge-under-fire/.

recent ransomware attack on Los Angeles Unified School District resulted in the release of students' personal information, and parents and students have questioned the district's preparation and transparency.[93] A ransomware attack on a Texas school district cost more than a half million dollars to mitigate, and attacks in Baltimore and Buffalo cost in excess of $9 million each.[94]

As the Government Accountability Office has described, student data "can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood."[95] One breach included the personal information of students who completed surveys on bullying, and another included students' phone numbers, which "were used to send text messages that threatened physical violence."[96] In light of these harms, "COPPA-covered companies, including ed tech providers, must have procedures to maintain the confidentiality, security, and integrity of children's personal information. For example, even absent a breach, COPPA-covered ed tech providers violate COPPA if they lack reasonable security."[97]

Policymakers should note that public sector services are provided in part or entirely by private contractors or vendors, so new regulations should protect the privacy-forward provision of governmental services by such contractors.[98] Governments regularly contract out services to private companies, and many of those services involve data collection and use. Schools and school districts may contract with private contractors to provide systems for online lessons, communications services, or managing students' personal information. Other governmental

---

[93] Howard Blume & Alejandra Reyes-Velarde, *Student Information Remains at Risk After Massive Cyberattack on Los Angeles Unified*, Los Angeles Times (Sept. 7, 2022), https://www.latimes.com/california/story/2022-09-07/los-angeles-unified- schools-cyberattack; Joshua Bay, *LA Parents Sound Off After Cyberattack Leaves Students Vulnerable*, The 74 (Oct. 7, 2022), *https://www.the74million.org/article/la-parents-sound-off-after-cyberattack-leaves-students-vulnerable*.

[94] K12 SIX, *supra* note 176, at 8; *see also* McKenna Oxenden, *Baltimore County Schools Suffered a Ransomware Attack. Here's What You Need to Know*, Baltimore Sun (Nov. 30, 2020, 8:33 PM), https://www.baltimoresun.com/maryland/baltimore-county/bs-md-co-what-to-know-schools-ransomware-attack-20201130-2j3ws6yffzcrrkfzzf3m43zxma-story.html.

[95] Government Accountability Office, Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm 13 (2021), https://www.gao.gov/products/gao-20-644.

[96] *Id.*

[97] Federal Trade Commission, Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act 3 (2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online.

[98] *See Comments on California Privacy Protection Agency's Proposed Rulemaking Under the California Privacy Rights Act of 2020*, *supra* note 2, at 12-14 (explaining the importance of scoping rules to protect student privacy without creating unintended consequences for service provision).

entities may contract with private entities for a variety of services such as identity verification. A broadly applicable data-related rule may not apply as easily to entities providing government services and may even interfere with those services.[99]

iv. ID verification for government services

Both recipients of government services and victims of identity theft face risks from the use of private vendors by state and federal agencies providing benefits and services.[100] However, regulation of private vendors assisting with government service delivery presents a further challenge: just as with private providers of educational services, improperly considered rules may hamper the ability of government agencies to effectively deliver essential services. On the other hand, rules are clearly needed: the use and collection of citizen data by private companies poses risks to privacy that could result in material harm, such as identity theft; and government outsourcing of key benefits determinations to private companies can result in preventing some individuals from getting essential benefits.

The starting point for delivery of governmental services is identity verification, where the government agency checks that an applicant is who they say they are. As public agencies seek to modernize identity verification through data and technology use, they are increasingly considering incorporating assistance from private companies. Examples of vendor assistance include: attribute validation, where the vendor confirms that the information provided by an applicant matches that in other identity databases (such as driver's license data, health records, or financial records); and biometric verification, where the vendor confirms through the use of physical or biological information that the applicant matches any submitted identity documents (1:1 matching) or other biometric information in the vendor's database (1:many matching).[101] Most recently, the use of facial recognition as a kind of biometric verification has garnered widespread scrutiny.[102]

---

[99] For an analysis of how rules affecting private companies should be scoped to avoid unintended consequences for government service providers, *see* Center for Democracy & Technology, *Comments on FTC's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*, at 48-51, https://cdt.org/wp-content/uploads/2022/11/CDT-Comments-to-FTC-on-ANPR-R111004.pdf.

[100] Here, we focus on practices that involve passing data to private technology vendors and exclude services that are provided solely by governmental entities or primarily involve in-person verification.

[101] *See* Michael Yang, Center for Democracy & Technology, *Digital Identity Verification: Best Practices for Public Agencies* (2022), https://cdt.org/insights/digital-identity-verification-best-practices-for-public-agencies/.

[102] Brian Naylor, *IRS Has Second Thoughts About Selfie Requirement*, NPR (Feb. 7, 2022, 3:29 PM), https://www.npr.org/2022/02/07/1078024597/want-information-from-the-irs-for-some-the-agency-wants-a-selfie.

The two main risks in the provision and use of such identification verification services are data breaches and biased algorithms.[103] First, when sensitive information is processed by a third party for purposes of identity verification, this data sharing increases the potential for data breaches. For example, ID.me, a facial recognition identity verification company, allowed employees to bring home devices that carried U.S. citizens' identity data and retained biometric data longer than necessary.[104] Such practices increase the chances of data being leaked onto the internet and later used for identity theft. Similar risks came to fruition when Equifax, a credit agency that also provides attribute validation for identity verification, exposed personal information of 147 million people in a 2017 data leak, allowing both domestic and foreign criminals to defraud state governments of pandemic unemployment assistance by using false or stolen identities.[105] Victims of identity theft face significant obstacles in re-asserting their identity and regaining access to government services.

Second, biometric analysis for identity verification may be less accurate for individuals from some racial backgrounds.[106] That bias harms members of those groups because they face increased barriers in accessing government services that require biometrics as part of identity verification. For this reason, the General Services Administration (GSA) committed in January 2022 not to use facial recognition, from private companies or otherwise, for identity verification in government service delivery until facial recognition is sufficiently free of biases.[107] However, the GSA's new rule is limited to the products that it deploys (namely, Login.gov, the single sign-on authentication solution it provides to other federal, state, and local agencies), and does

---

[103] Hannah Quay-de la Vallee, *Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives*, Center for Democracy & Technology (Jun. 7, 2022), https://cdt.org/insights/public-agencies-use-of-biometrics-to-prevent-fraud-and-abuse-risks-and-alternatives/.

[104] Caroline Haskins, *Inside ID.me's Torrid Pandemic Growth Spurt, Which Led to Frantic Hiring, Ill-Equipped Staff, and Data-Security Lapses as Tte Company Closed Lucrative Deals With Unemployment Agencies and the IRS*, Bus. Insider (Jun. 7, 2022, 5:00 AM), https://www.businessinsider.com/id-me-customer-service-workers-hiring-secuirty-privacy-stress-data-2022-6. Jessy Edwards, *ID.me Lawsuit Claims Company Violates Data Storage Requirements*, Top Class Actions (Aug. 22, 2022), https://topclassactions.com/lawsuit-settlements/privacy/bipa/id-me-lawsuit-claims-company-violates-data-storage-requirements/.

[105] Cezary Podkul, *How Unemployment Insurance Fraud Exploded During the Pandemic*, ProPublica (July 26, 2021, 5:00 AM), https://www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.

[106] Nicol Turner Lee, *Mitigating Bias and Equity in Use of Facial Recognition Technology by the U.S. Customs and Border Protection*, Brookings Institution (July 27, 2022), https://www.brookings.edu/testimonies/mitigating-bias-and-equity-in-use-of-facial-recognition-technology-by-the-u-s-customs-and-border-protection/.

[107] *Executive Order 13985 – Equity Action Plan*, General Services Administration (Jan. 20, 2022), https://www.gsa.gov/cdnstatic/GSAEquityPlan_EO13985_2022.pdf.

not address bias in other forms of biometrics, like voice recognition.[108] Other government agencies at every level may still use biometrics from private vendors, regardless of levels of bias, for identity verification. Thus, other agencies should consider the appropriate level of accuracy and fairness for biometrics to be used safely, and establish that as the standard all private vendors must meet when providing biometric verification to government services on the ground.

v. Eligibility determination and allocation of benefits

Government agencies also use private vendors' algorithm-driven systems to determine eligibility for, allocate, and verify legitimate provision of benefits. Private contractors develop many of these systems, some of which are off-the-shelf products while others are developed for specific populations in the jurisdictions where they are used. People with disabilities who are not able to work, or who can work only limited hours, may be reliant on public benefits – including Medicaid coverage for basic health care and long-term supports and services, housing assistance, food stamps, and cash assistance – that are subject to algorithm-driven decisions generated by private companies.

For instance, algorithmic systems are used in determinations about home- and community-based services to assess hours of care a beneficiary will need or the budget for providing necessary care.[109] Advocates have documented that in many cases, states' implementation of these systems has caused sudden, drastic, and arbitrary reductions or terminations of benefits that were previously granted. This has had devastating and terrifying effects on the lives of disabled and low-income people because it deprives recipients of care that supports independent living at home. Recipients cannot reasonably avoid such outcomes because reductions or terminations to their benefits often take effect before they are properly informed. For instance, one health services technology company, Optum, developed a needs assessment tool for Arkansas that cut approved care hours for some people with developmental disabilities in Arkansas nearly in half without explanation, putting them at imminent risk of serious injury and potential institutionalization, and preventing them from completing basic

[108] Claudia Lopez Lloreda, *Speech Recognition Tech Is Yet Another Example of Bias*, Scientific American (July 5, 2020), https://www.scientificamerican.com/article/speech-recognition-tech-is-yet-another-example-of-bias/.
[109] Lydia X.Z. Brown et al, Ctr. for Democracy & Tech., *Challenging the Use of Algorithm-Driven Decision-Making in Benefits Determinations Affecting People With Disabilities* (2020), https://cdt.org/insights/report-challenging-the-use-of-algorithm-driven-decision-making-in-benefits-determinations-affecting-people-with-disabilities/ [hereinafter *Benefits Determinations*].

daily functions like eating and using a bathroom.[110] Similarly, in Indiana, IBM's algorithm-driven system for processing welfare applications caused sudden termination of benefits for huge numbers of low-income people, who received confusing and delayed notices about noncompliance or fraud.[111]

While state agencies violate civil rights and constitutional protections when adopting systems that impose these harms, people currently have little to no recourse against the private companies that develop and sell these tools to arbitrarily and drastically cut people's benefits. Under Title II of the ADA, a person may not be excluded from participation in or denied benefits of the services of any "public entity" on the basis of disability.[112] Public benefits determinations that deprive recipients of benefits that allow them to live independently can force recipients to be institutionalized. This violates the ADA's community integration mandate that the Supreme Court affirmed in 1999, which requires government entities to administer government services and programs in a manner that enables disabled people to interact with non-disabled people in the most integrated setting possible.[113] Although government agencies should avoid procuring systems from private vendors that would interfere with disabled people's ability to continue living in their own homes, vendors are not precluded from selling tools that have this outcome.

Even when a benefits recipient is granted these services in the correct amount, the use of electronic visit verification (EVV) systems can interfere with the provision of personal care services. Similar to algorithmic systems used for benefits determination, EVV mobile apps and software are often provided by private home health tech companies.[114] With these systems, companies like Sandata and Direct Care Innovations require care workers to confirm that they are providing services as approved by interacting with facial recognition, voice verification, and

---

[110] *Id.* at 21. *See also* Upturn, Benefits Tech Advocacy Hub, *Arkansas Medicaid Home and Community Based Services Hours Cuts*, https://www.btah.org/case-study/arkansas-medicaid-home-and-community-based-services-hours-cuts.html; Ryan Calo & Danielle Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 Emory L.J. 797, 799 (2021), https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1418&context=elj.

[111] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, at 39-54 (2018); Rick Callahan & Tom Davies, *Judge: IBM Owes Indiana $78M for Failed Welfare Automation*, APNews (Aug. 7, 2017), https://apnews.com/article/8eb53eb9bdf94adb92e5b8b09559d8d0.

[112] 42. U.S.C. 12132.

[113] Brown, *Benefits Determinations*, *supra* note 105, at 17.

[114] Alexandra Mateescu, Data & Society, Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care 14 (2021), https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf. For a non-exhaustive list of private EVV vendors, *see* Applied Self-Direction, *Directory of EVV Vendors Interested in Serving Self-Direction Programs* (last updated Oct. 5, 2022), https://www.appliedselfdirection.com/resources/directory-evv-vendors-interested-serving-self-direction-programs.

GPS location tracking features during home visits.[115] Companies require workers to verify their service provision through their designated EVV systems frequently, with precision, and within narrow windows of time during their home visits to prove that benefits are not being abused.[116]

When a system incorrectly flags that workers did not provide services at the approved time and location, this delays payments until this flag is resolved, costing workers their wages.[117] This can also obligate recipients to pay for workers' lost wages out of pocket and to stay within the confines of their homes due to geofencing limits that cause their care workers to be flagged for fraud, and it reduces the home care workforce.[118] One company, CareBridge, plans to combine EVV technology with a predictive model to assess care needs, creating new risks for unreliable data practices to undercut provision of care.[119] This interferes with the care disabled people are supposed to receive as well as the wages that care workers (who are disproportionately women of color, and often disabled and from immigrant communities) can lose over minor errors or delays.[120]

Question 6: Prevalence of algorithmic discrimination and sectors of concern

Unfortunately, there is no good data on the prevalence of algorithmic discrimination--either across the economy or in particular sectors--because companies generally are not required to publicly disclose the existence (much less the impact) of automated decision-making in their

[115] Sandata, *Ensure EVV Compliance with Multiple Verification Methods*, https://www.sandata.com/multiple-verification-methods-help-ensure-evv-compliance/; Direct Care Innovations, *High Tech and Low Tech Options for EVV* (Mar. 24, 2019), https://www.dcisoftware.com/blog/dci-evv-options/.
[116] Mateescu, *supra* note 110, at 30. *See also* Public Partnerships, *Time4Care Electronic Visit Verification (EVV) Mobile App*, https://www.publicpartnerships.com/tools/time4care-evv/.
[117] Virginia Eubanks & Alexandra Mateescu, *'We Don't Deserve This': New App Places US Caregivers Under Digital Surveillance*, The Guardian (July 28, 2021, 6:00 AM), https://www.theguardian.com/us-news/2021/jul/28/digital-surveillance-caregivers-artificial-intelligence; Jacqueline Miller et al., University of California San Francisco Health Workforce Research Center on Long-Term Care, *Impact of Electronic Visit Verification (EVV) on Personal Care Services Workers and Consumers in the United States* 12, 15-16 (2021), https://healthworkforce.ucsf.edu/sites/healthworkforce.ucsf.edu/files/EVV_Report_210722.pdf.
[118] Eubanks, *supra* note 113; Naomi Gallopyn & Liza I. Iezzoni, *Views of Electronic Visit Verification (EVV) Among Home-Based Personal Assistance Services Consumers and Workers*, Disability and Health Journal (2020), https://www.ancor.org/wp-content/uploads/2022/08/disability_and_health_journal_article_on_views_of_evv.pdf.
[119] *CareBridge Launches to Improve Care for Individuals Receiving Long-Term Support Services*, Business Wire (Jan. 12, 2020, 4:58 PM), https://www.businesswire.com/news/home/20200113005935/en/CareBridge-Launches-Improve-Care-Individuals-Receiving-Long-Term.
[120] Id at 45-46. See also Lydia X.Z. Brown, *EVV Threatens Disabled People's Privacy and Dignity – Whether We Need Care, or Work as Professional Caregivers*, Ctr. for Democracy & Tech (Mar. 24, 2022), https://cdt.org/insights/evv-threatens-disabled-peoples-privacy-and-dignity-whether-we-need-care-or-work-as-professional-caregivers/.

operations. There are some limited exceptions to this general rule. For example, federal contractors are usually required to maintain records on all personnel actions[121] and may be subjected to compliance reviews by the federal Department of Labor's Office of Federal Contractor Compliance Programs (OFCCP) that require them to reveal information about particular practices.[122] But such information is not collected from a sufficient number of employers to reliably estimate the prevalence of automated decision-making in any particular sector.

Question 7: How access and opt-out rights can address algorithmic discrimination

Lack of transparency regarding automated decision-making is a recurring theme in our responses to the preceding questions, and that opacity is one of the key areas that the Agency can help address through regulations ensuring access and accountability, in particular. Additionally, opt-out rights could help reduce the risk of discrimination, such as by giving disabled consumers and workers the right to opt out of decision-making processes for which they cannot obtain adequate accommodation, or where they otherwise believe the automated system will not make a fair and accurate decision due to their disability.

Question 8: Whether access/opt-out rights should vary depending on certain factors

Access and opt-out rights for automated decision-making should depend, as under the GDPR, on whether the decision affects the consumer's legal rights or would have significant effects on the consumer's life (such as housing, employment, education, and credit). When such decisions are left to automated systems, the consumer should have the right to access the information upon which the decision was based, to obtain an explanation as to the reasons for the decision itself, and to opt-out of purely automated decision-making and request human review. This approach will allow the consumer an opportunity to raise concerns, request accommodation, and make an informed decision about whether, when, and how to proceed with the automated decision-making process. Those rights should not be reduced or otherwise changed in particular settings and sectors.

[121] 41 C.F.R. 60-1.12.

[122] *See generally* Federal Contract Compliance Manual, Chapter 1A00 (Types of Compliance Evaluations), https://www.dol.gov/agencies/ofccp/manual/fccm/1a-introduction/1a00-types-compliance-evaluations.

Question 9: Information that should be included in response to access requests

We recommend that the Agency examine Standard 4 of the *Civil Rights Standards for 21st Century Employment Selection Procedures*,[123] which CDT and a coalition of other national civil rights organizations published in December 2022. Standard 4 would require all companies that sell or use automated employment decision technologies (or other employment selection procedures) to publish a short-form disclosure on their website and provide the disclosure to each candidate about whom the tool will make an employment decision. The required disclosure must include the following:

- What types of employment decisions will be made or informed by the tool,
- The positions for which the selection procedure will be used; the knowledge, skills, abilities, and other characteristics that the tool will assess; how those characteristics relate to the position's essential functions; and how the tool measures those characteristics,
- How to interpret the results or other outputs of the tool,
- Any reasonably foreseeable accommodations that candidates may require,
- How candidates can access accommodations, communicate concerns, or file a complaint relating to the tool, and
- How a candidate can opt out of the automated decision-making process.

We believe that this approach should be applied to automated decisions made in other contexts as well. One way to adapt those requirements for the CPPA, which would cover automated decision-making systems in a broad range of additional settings beyond employment would be to require brief, accessible disclosures that inform consumers subjected to automated decision-making of the following information:

- The types of automated decisions to which the consumer may be subjected,
- How the automated system makes those decisions, including the information it is relying upon and how that information is relevant to the decision being made,
- How the consumer can interpret the system's output,
- What accommodations the consumer may require,
- How the consumer can request accommodation, raise concerns, or file a complaint, and
- How the consumer can opt out of the automated decision process altogether.

[123] *Civil Rights Standards for 21st Century Employment Selection Procedures* (2022), https://cdt.org/insights/civil-rights-standards-for-21st-century-employment-selection-procedures/.

Risk Assessments

Question 1: Existing risk assessment requirements for processing personal information

To our knowledge, there are no laws requiring California[124] businesses to conduct risk assessments for "processing . . . personal information" as a general matter. There are, however, laws requiring companies to conduct analyses regarding certain *decisions* that may be based on the processing of personal data, perhaps most notably in the context of employment discrimination laws. Title VII of the federal Civil Rights Act of 1964, for example, generally prohibits companies from employment practices that have an adverse impact on a protected group. Where such adverse impacts exist, Title VII requires companies to establish that the employment practice causing the adverse impact is "job related for the position in question and consistent with business necessity."[125] However, federal law does not affirmatively require companies to conduct adverse impact analyses or job-relatedness (or validation) studies; companies simply have an incentive to do so to avoid liability for discrimination should adverse impacts arise as a result of using a selection procedure.

The absence of effective risk assessment requirements for the processing of personal information is a major weakness in the current legal regime governing the processing of personal information, particularly when decisions significantly impacting the consumer are made through such processing. Companies should be required to conduct detailed impact assessments to identify potential harms that might result from the processing of personal information *before* deploying systems relying on such processing.

Question 2: Harms that can result from processing personal information

For this question, we incorporate by reference our response to questions 4 and 5 from the Automated Decision-making section.

Question 3: GDPR and other potential models for risk assessment requirements

We would consider the GDPR's data protection impact assessment provisions to be a solid, if imperfect, model for risk assessment requirements. Substantively, the GDPR requires the impact assessment to describe the data processing operations, state the purposes of the processing,

[124] In our response to Question 3, below, we discuss laws applicable elsewhere--specifically the EU's GDPR and the Colorado Privacy Act.
[125] 42 U.S.C. 2000e-2(k)(1)(A)(i).

and assess the necessity and proportionality of the processing in relation to those purposes, the risks to the "rights and freedoms" of data subjects, and the measures envisaged to address those risks.[126] These are sound principles, although merely assessing potential threats to data subjects' "rights and freedoms" does not address the full scope of potential risk that consumers face when subjected to data processing that affects major aspects of the data subject's life or livelihood, such as decisions relating to housing, employment, or education.

To provide a more thorough and meaningful disclosure, we recommend an approach akin to that suggested by the Berkeley Labor Center in its Framework for Worker Technology Rights (hereafter, "BLC Framework").[127] Specifically, Section 8 of the BLC Framework covers impact assessments, and it states companies "should evaluate the full range of potential harms to workers," including "discrimination, harms to mental and physical health and safety, loss of privacy, and negative economic impacts."[128]

The GDPR's approach is also limited in other respects. It requires impact assessments only when a "new" technology "is likely to result in a high risk to the rights and freedoms of natural persons."[129] The impact assessment requirement should not be limited to new technologies; on the contrary, companies should be required to reexamine their data processing operations regularly to ensure that new risks are identified and mitigated when they arise in the course of a processing system's operations. Moreover, the GDPR's "likely to result in a high risk" limitation on which systems must be assessed is too ambiguous, potentially leaving companies with the ability to avoid the requirements by claiming that they did not subjectively perceive the risk of harm to be "high." The Colorado Privacy Act's (CoPA) data protection assessment requirements suffer from a similar deficiency, requiring assessments to be conducted only if the data processing creates a "reasonably foreseeable risk of" certain harms.[130]

The scope of the Agency's risk assessment requirements should instead be based on concrete factors such as the nature of the processing (e.g., those relating to employment, education,

[126] General Data Protection Regulation, art. 35.7.
[127] Annette Bernhardt, et al., Berkeley Labor Center, *Data and Algorithms at Work: The Case for Worker Technology Rights*, Part II: A Framework for Worker Technology Rights, Nov. 3, 2021, https://laborcenter.berkeley.edu/data-algorithms-at-work/.
[128] *Id.*
[129] General Data Protection Regulation, art. 35.1.
[130] Colo. Rev. Stat. § 6-1-1309(2)(a).

housing, credit, etc, or that process sensitive personal information) and the number of consumers potentially affected.[131]

Question 4: Minimum content of impact assessments
Question 5: Benefits and drawbacks of adopting GDPR or CoPA approaches
Question 6: Format of risk assessments submitted to the Agency

For the reasons stated in response to Question 3, we believe that the impact assessment requirements of the GDPR are a good starting point for the Agency, with the caveats stated in that response regarding the scope of what types of data processing should be subject to risk assessment requirements.

We do not believe that the requirements of the CoPA serve as a suitable model for the content of risk assessment requirements because they are not specific as to what details should be included in such assessments. The CoPA requires companies to "identify and weigh" the data processing's potential "benefits" and "risks to the rights of the consumer," factoring in circumstances such as "the use of de-identified data and the reasonable expectations of consumers."[132] These requirements are too vague and, on their face, could allow companies to satisfy the statute with very cursory impact assessments that would provide neither the company, consumers, nor the Agency with the information needed to determine the degree of risk a data processing practice might pose.

We believe that the Agency should require risk assessments that, at a minimum:

- Identify the purposes of the data processing
- Describe the nature of the data processing
- Assess the necessity and proportionality of the data processing in relation to the purposes
- Evaluate the full range of potential harms to consumers and workers that the data processing may pose, including potential harms relating to consumers' and workers':
    - Rights and freedoms, including the right to be free from discrimination
    - Health and safety
    - Finances and economic situation

[131] The National Institute of Standards and Technology's AI Risk Management Framework proposes additional factors to consider when measuring risk. *See Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, *supra* note 5.
[132] Colo. Rev. Stat. § 6-1-1309(3).

- State what safeguards, mitigation measures, or other efforts to address these potential harms the data processor has taken, and what additional steps could or should be taken to reduce the risk of harm
- Are conducted prior to the deployment of the data processing system or practice, and repeated at least annually for as long as the system or practice remains in place
- Are conducted by a third party with no conflict of interest with respect to the data processor or the data at issue
- Are:
    - Submitted to the Agency; and
    - Published in an accessible format on the website of the data processor and any company from whom the data was obtained or with whom the data is sold or shared

Conclusion

We thank the Agency for its thoughtful questions on these important topics and for providing us with the opportunity to comment in advance of the formal rulemaking process. We look forward to engaging with the Agency and supporting its efforts to protect the rights and dignity of California's consumers and workers.