February 19, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Re: Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations

Sent via email to regulations@cppa.ca.gov

Dear Board Members, Executive Director, and Agency Staff,

We write in response to the California Privacy Protection Agency's ("CPPA" or "the Agency") request for comment on the Agency's proposed Risk Assessment and Automated Decisionmaking Technology ("ADMT") Regulations ("Proposed Regulations") under the California Consumer Protection Act ("CCPA").[1]

Technology can make life better for Californians if it is built carefully and used thoughtfully to empower people and address systemic challenges to access, equity, and justice that have disproportionately harmed marginalized Californians. But technology broadly, and algorithmic systems specifically, can also magnify and expand threats to rights, health, and safety if robust protections are not properly put into place throughout the ADMT ecosystem.

As algorithmic systems become increasingly ubiquitous in the life of Californians, those systems need to meet a high standard of respecting people's rights and ensuring that they can be used safely, without harming people already pushed to

[1] ACLU California Action would like to thank the Juelsgaard Intellectual Property and Innovation Clinic at Stanford Law School, including law students Caitlin Burke, Mark Cantu, Alex Cohen, Timothy Fellows, and Lane Miles for their assistance researching and writing these comments. The ACLU also acknowledges the support of Clinical Supervising Attorney and Lecturer in Law Nina Srejovic and Clinic Director and Professor of Law Phil Malone for their assistance supervising the clinic and the law students.

the margins of our society. Among the core rights implicated by AI systems is our state constitutional right to privacy in Article I, Section 1 of the California Constitution. Enacted in 1972, this right guarantees an inalienable right to privacy to all Californians and protects against invasions by both government and private parties. Article I, Section 1 is intended to impose "effective restraints" on the "accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."[2] This fundamental right to privacy for Californians should inform the Proposed Regulations.

These comments focus on how the draft regulations can best protect people's privacy, safety, and civil rights. Section I explains how the regulations are within the agency's statutory authority, which extends to fulfilling the purposes of the CCPA and the underlying constitutional privacy framework on which it builds. Section II provides recommendations for strengthening and clarifying the ADMT regulations to ensure that people's rights are protected against technology that could cause them harm. In particular, Section II argues that strong opt-out rights should be preserved for the most harmful ADMT applications (if they are not banned outright), and the exceptions in the Proposed Regulations that hamstring people's ability to control how their personal information is used should be clarified or eliminated. Section III provides recommendations for the proposed Risk Assessment regulations to ensure that the law's intent—that processing of personal information which is not beneficial should not be used—is properly reflected in the regulations. Section IV offers recommendations for how the Proposed Regulations should take the law's trade-secret exception into account to avoid trade-secret law inappropriately undermining the public and the agency's ability to understand how Californians' personal information is being used by businesses.

I. The Proposed Regulations Are Comfortably Within the Agency's Statutory Authority.

The statutory framework of the CCPA, and the constitutional rights on which it was based, offer a firm foundation for the draft regulations. Section 1798(a)(15) empowers the Agency to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform annual cybersecurity audits and submit risk assessments to the Agency. When the risks to privacy outweigh the purported benefits, the goal of the regulations is to "restrict or prohibit" the processing. *Id.* And Section 1798(a)(16) gives the Agency the authority to issue regulations "governing access

[2] *White v. Davis*, 13 Cal. 3d 760, 774 (Cal. 1975).

and opt-out rights with respect to businesses' use of automated decision-making technology."

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).

The CCPA's focus on use of personal information should also be understood in the proper historical context. Controlling the *use* of personal information (as compared with the collection or disclosure) is not a marginal aspect of legal privacy rights; it is one of the cornerstones of privacy protections that has been present in California law for over half a century. The California constitutional right to privacy was passed by the legislature and the voters in 1972, in a time when many Californians had developed a personal and visceral understanding about how the government and private actors could weaponize information about their lives to try to harm them.[3] The constitutional privacy rights protect against intrusion by both government and private actors. *See Hill*, 7 Cal. 4th at 20 ("In summary, the Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities."). A foundational aspect of the right to privacy is the right to control what personal information is collected and, importantly, how that information is used. The voter guide for the constitutional amendment explained that the right to privacy was targeted at addressing four "principal mischiefs," among them being "the improper *use* of information properly

[3] *See generally* Nicole A. Ozer, *Golden State Sword: The History and Future of California's Constitutional Right To Privacy To Defend and Promote Rights, Justice, And Democracy in The Modern Digital Age*, 39 BERKELEY TECH. L. J. 963 (2024).

obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party." *White v. Davis*, 13 Cal.3d at 775 (citing ballot argument).

The foundational protection in the California Constitution against misuse of information are all the more prescient today, as the ways in which private parties use people's personal information have expanded through the use of algorithmic systems including "artificial intelligence." The collection, sharing, and use of personal information can cause people to be incarcerated,[4] to suffer bodily injury,[5] to lose their homes[6] or their jobs,[7] and to be blocked from accessing new opportunities[8] and credit[9]. Misuse of personal information can expose people to hacking,[10] scams,[11] higher prices and lower quality goods,[12] intimate-partner violence,[13] and

[4] Will D. Heaven, *Predictive Policing Algorithms are racist. They need to be dismantled.* MIT TECHNOLOGY REVIEW (July 17, 2020), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

[5] Will Evans, *Amazon's Warehouse Quotas have been injuring workers for years now. Now, officials are taking action,* REVEAL NEWS (May 16, 2022), https://revealnews.org/article/amazons-warehouse-quotas-have-been-injuring-workers-for-years-now-officials-are-taking-action/.

[6] Wendy Fry, *Landlords are Using AI to Raise Rents- and cities are starting to push back,* GIZMODO (December 7, 2024), https://gizmodo.com/landlords-are-using-ai-to-raise-rents-and-cities-are-starting-to-push-back-2000535519.

[7] Tim De Chant, *Amazon is using algorithms with little human intervention*, ARSTECHNICA (Jun 28, 2021), https://arstechnica.com/tech-policy/2021/06/amazon-is-firing-flex-workers-using-algorithms-with-little-human-intervention/.

[8] Olga Akselrod and Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Fired,* ACLU: NEWS & COMMENTARY (August 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired.

[9] Edmund L. Andrews, *How Flawed Data Aggravates Inequity Credit,* STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE (August 6, 2021), https://hai.stanford.edu/news/how-flawed-data-aggravates-inequality-credit.

[10] Thomas Germain, *The FBI Says You Need to Use an Ad Blocker,* GIZMODO (December 22, 2022), https://gizmodo.com/google-bing-fbi-ad-blocker-scam-ads-1849923478.

[11] Craig Silverman & Ryan Mac, *Facebook Gets Rich Off Of Ads That Rip Off Its Users*, BUZZFEED NEWS (Dec. 1, 2020), https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam; Andrew Chow, *Facebook Shopping Scams Have Skyrocketed During the Pandemic*, TIME, Dec. 8, 2020, https://time.com/5921820/facebook-shopping-scams-holidays-covid-19; Jason Koebler, *Most of My Instagram Ads Are for Drugs, Stolen Credit Cards, Hacked Accounts, Counterfeit Money, and Weapons*, 404 MEDIA (Aug. 23, 2023), https://www.404media.co/instagram-ads-illegal-content-drugs-guns-hackers/.

[12] Julia Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why.*, N.Y. TIMES (April 6, 2023), https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html (summarizing Schnadower Mustri, Eduardo and Adjerid, Idris and Acquisti, Alessandro, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation* (Mar. 23, 2023), available at SSRN: https://ssrn.com/abstract=4398428).

[13] Becca Downes, *Data Broker Harms: Domestic Violence Survivors, EPIC (ELECTRONIC PRIVACY INFORMATION CENTER) (November 25, 2024),* https://epic.org/documents/data-broker-harms-domestic-violence-survivors/.

deportation.[14] Because collection, sharing, and use of personal information is at the root of these varied harms, they are *exactly* the kind of social ills a privacy law can and should address. Indeed, they are just the kinds of harms that the draft regulations seek to address.[15]

II. The ADMT Regulations Should Be Clarified to Give People True Opt-Out Rights When Their Rights and Safety Are Threatened.

A. Definitions.

1. The definition of ADMT should properly protect people.

The final regulations should ensure that covered businesses cannot exploit ambiguity to avoid regulation. Under the December 2023 Proposed Regulations, the term ADMT was defined to include systems that were a "whole or part of a system to make or execute a decision or facilitate human decisionmaking."[16] But the current Proposed Regulations revise this definition to only cover systems that "execute a decision, replace human decisionmaking, or *substantially facilitate* human decisionmaking."[17] (Italics added). These changes raise two concerns.

First, consumers may be deprived of these important protections because businesses may inaccurately report that their technology merely "facilitates" rather than "substantially facilitates" human decisionmaking. As written, the regulations state that a system substantially facilitates human decisionmaking when the "output of the technology [is] a key factor in a human's decisionmaking."[18] But this language could easily be manipulated by businesses. Companies will have a strong incentive to characterize their systems as providing only one input of many to a human—thus making it arguably not a "key factor" in the decision—but nevertheless create implicit policies that make clear to the human decision-makers that the automated factor is the one to be trusted. As one Board Member emphasized during the March

[14] Corin Faife, *ICE uses data brokers to bypass surveillance restrictions, report finds,* THE VERGE (May 10, 2022), https://www.theverge.com/2022/5/10/23065080/ice-surveillance-dragnet-data-brokers-georgetown-law; Jake Weiner, *New ICE Privacy Impact Assessment Shows All the Ways the Agency Fails to Protect Immigrants' Privacy,* EPIC (April 20, 2023), https://epic.org/new-ice-privacy-impact-assessment-shows-all-the-way-the-agency-fails-to-protect-immigrants-privacy/.

[15] See *Benefits Anticipated From Regulatory Action*, Draft Initial Statement of Reasons, pp. 2–8, California Privacy Protection Agency, https://cppa.ca.gov/meetings/materials/20241004_item6_draft_initial_statement_of_reasons

[16] December 2023 Draft Risk Assessment Regulations, Section 7001.

[17] Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, Section 7001 (November 22, 2024).

[18] § 7001(2).

2024 meeting, the “substantially facilitates” language could become a “loophole … you can drive a truck through.”[19]

Second, even if businesses claim that the algorithmic input is not a “key factor” for human decisionmaking, it is likely that such inputs will nevertheless, in practice, become the primary determinant in the decision. Research consistently shows that humans are inclined to “attribute a great deal of authority and trustworthiness to machines.”[20] Moreover, there is “a bias towards leaning more heavily on algorithms as a task gets harder.”[21]

Decisions targeted for automation—such as who to hire, fire, prosecute, or release on parole—are exactly the “hard[] … task[s]” in which people are likely to defer to the judgment of an automated system. Thus, even when automatically generated information is not supposed to be a “key factor” in a human’s decisionmaking, it will likely take on such importance in practice. But senior leadership at these businesses—removed from the actual decisionmaking system itself—will nevertheless determine that the system is not a providing a “key factor.” As a result, consumers will be denied the notice and opt-out protections they need and deserve.

We therefore recommend that the Agency align with other areas of state policy and adopt the State Administrative Manual’s (SAM) definition of Automated Decision System:

> **Automated Decision System: 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. An “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.**

[19] *See* Comment from Board Member Alastair Mactaggart, Transcript of Mar. 8, 2024 Meeting of California Privacy Protection Agency Board, https://cppa.ca.gov/meetings/materials/20240308_transcript.pdf at 70. (“[A]s we've seen time and again a small loophole ends up being something you can drive a truck through.”).

[20] Lauren Leffer, *Too Much Trust in AI Poses Unexpected Threats to the Scientific Process*, SCIENTIFIC AMERICAN (Mar. 18, 2024), https://www.scientificamerican.com/article/trust-ai-science-risks/.

[21] David Nield, *This is the Point When People Start Trusting Algorithms More Than Other Humans*, SCIENCE ALERT (Apr. 17, 2021), https://www.sciencealert.com/this-is-when-people-start-to-trust-algorithms-more-than-humans.

1. *The regulations should provide additional context-specific examples of "significant decisions concerning a consumer."*

The Proposed Regulations reflect a valid concern that ADMTs can harm people in a wide variety of ways, reaching almost every corner of the modern digital world, from housing to insurance to criminal justice. But the regulations fail to specify adequately the nature of the decisions that are "significant" under the law.

Under Section 7200(a)(1), the regulations apply to any business that uses an ADMT "for a significant decision regarding a consumer." The regulations should be updated to provide additional examples of what qualifies as a significant decision so there is no confusion and people are properly protected under the definition. Currently, the regulations define significant decisions as those that:

> [R]esult[] 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).[22]

For several of these contexts, the regulations provide specific examples of significant decisions.[23] For example, Section 7200(a)(1)(A)(i) provides a non-exhaustive list of significant decisions relating to "education enrollment or opportunity"—namely, admission or acceptance into academic or vocational programs; educational credentials (e.g., a degree, diploma, or certificate); and suspension and expulsion.

The regulations should be updated to provide examples of significant decisions in the other contexts listed in Section 7200(a)(1)(A). In its recent letter regarding Executive Order N-12-23 (focused on the State's use of Generative Artificial Intelligence), ACLU California Action ("ACLU") provided clear examples of these important decisions in these other contexts.[24] Drawing from that letter, we propose the following additions:

> § 7200. Uses of Automated Decisionmaking Technology.
>
> (a)(1)(A) For purposes of this Article, "significant decision" means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4),

[22] § 7200(a)(1).

[23] *See* § 7200(a)(1)(A)(i), *et seq.*

[24] *See* ACLU California Action Comment on Executive Order N-12-23, https://www.aclunc.org/sites/default/files/ACLU%20Comment%20on%20GenAI%20Executive%20Order.pdf

and (5), 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).

(iii) Criminal justice includes:

1. Risk assessments for pretrial decisionmaking, including, but not limited to, decisions related to pretrial detention, release on one's own recognizance, the granting or setting of monetary bail, and the conditions of pretrial release;
2. Sentencing;
3. Parole;
4. Probation and any other form of supervised release;
5. Deployment of law enforcement resources;
6. Decisions related to conditions of confinement, including, but not limited to, housing, classification, and programming.

(iv) Housing includes[25]:

1. Screening or monitoring tenants;
2. Providing valuations for homes or underwriting mortgages; and
3. Determining access to or terms of home insurance; and
4. Determining the rate or conditions of housing.

(v) Healthcare services includes[26]:

7. Carrying out the medically relevant functions of medical devices;
8. Providing medical diagnoses or determining medical treatments;
9. Providing medical or insurance health-risk assessments;
10. Providing drug-addiction risk assessments or determining access to medication;
11. Conducting risk assessments for suicide or other violence;
12. Detecting or preventing mental-health issues;
13. Detecting or preventing mental-health issues or flagging patients for interventions;
14. Allocating care in the context of public insurance; and
15. Controlling health-insurance costs and underwriting.

[25] *Id.* at 12.
[26] *Id.*

B. Categorical Opt-Out Rights Should be Maintained.

The Proposed Regulations provide people with a categorical opt-out right for consumers against being profiled "for behavioral advertising."[27] This right is stronger than the opt-out protections against behavioral advertising in the statute, because those rules allow people only to opt out of behavioral advertising that is "cross-context," meaning that the advertising is based on the consumer's personal information "across businesses, distinctly-branded websites, applications, or services . . . ." Cal. Civ. Code § 1798.140(k). The limit to cross context behavioral advertising is significant because it allows large consumer-facing platforms—like Meta, Google, Microsoft, and Amazon—to continue serving behavioral advertising even when people don't want them. A stronger opt-out rule is warranted because, as the CPRA states, "[r]ather than diluting privacy rights, California should strengthen them over time." Section 2(E), California Privacy Rights Act. Since voters passed the CPRA in November of 2020, governments, scholars, researchers, activists, companies, and the public have continued to gain understanding of how behavioral advertising affects people's lives, both in positive and negative ways.

Advertising platforms that rely on detailed profiles of people's online and offline behavior to target advertisements are the source of significant public concern, and rightly so. It is invasive and unnerving to be bombarded with targeted advertisements based on your online or offline activity.[28] Companies may target their advertisements in a discriminatory way, based on age, sex, race, or ethnicity, resulting in certain groups receiving information about opportunities that others do not.[29] The products in behaviorally-targeted ads are also often lower quality and higher priced.[30] Targeted ads also enable outright scammers to proliferate and financially harm people.[31] Examples abound of predatory advertisements

[27] §§ 7200(a)(2)(iii), 7221(b)(6).

[28] Brian X. Chen, *Are Targeted Ads Stalking You? Here's How to Make them Stop*, N.Y. TIMES (Aug. 15, 2018) https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targetedstalker-ads.html ("Even if you end up ordering the watch, the ads continue trailing you everywhere. They're stalker ads.").

[29] For example, in 2019 the Department of Housing and Urban Development charged Meta with housing discrimination based on its targeted advertising. Charge of Discrimination available at https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

[30] Julia Angwin, *If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why.*, N.Y. TIMES (Apr. 6, 2023) https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-datasurveillance-consumer-quality.html (summarizing Schnadower Mustri, Eduardo and Adjerid, Idris and Acquisti, Alessandro, Behavioral Advertising and Consumer Welfare: An Empirical Investigation (Mar. 23, 2023) available at SSRN: https://ssrn.com/abstract=4398428).

[31] Craig Silverman & Ryan Mac, Facebook Gets Paid, BUZZFEED NEWS (Dec. 10, 2020) https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scamsrevenue-china-tiktok-vietnam; Andrew Chow, Facebook Shopping Scams Have Skyrocketed During the Pandemic, TIME (Dec. 18, 2020) https://time.com/5921820/facebook-shopping-scams-holidays-covid-19/; Jason Koebler,

deliberately targeting vulnerable people, such as subprime lenders targeting financially vulnerable consumers[32] (which often target victims based on their race[33]) or seniors targeted with direct investment scams.[34] The Federal Trade Commission has gone so far as to recommend that people opt out of targeted advertising to protect themselves from scammers.[35] The Federal Bureau of Investigation has similarly recommended the use of an ad blocker.[36]

This litany of harms offers strong support for the opt-out right for behavioral advertising in the Proposed Regulations.

C. The Exceptions to Opt-Out Rights Should Be Narrowed and Clarified.

The regulations recognize the importance of opt-out rights for ADMTs (in certain circumstances) by providing a general opt-out right to consumers in Section 7221(a). However, Section 7221(b) permits businesses to avoid providing an opt-out right if they meet one of several exceptions. These exceptions need to be further clarified and narrowed to properly protect people's rights.

First, when an opt-out is not categorically required, businesses can avoid offering an opt-out by providing a "method to appeal the decision to a qualified human reviewer who has the authority to overturn the decision."[37] Next, in addition to the "human appeal exception," a business may avoid providing an opt-out for certain uses of ADMT where the use of ADMT is 1) necessary and 2) used solely for that purpose,

Most of My Instagram Ads Are for Drugs, Stolen Credit Cards, Hacked Accounts, Counterfeit Money, and Weapons, 404 MEDIA (Aug. 23, 2023) https://www.404media.co/instagram-ads-illegal-content-drugs-guns-hackers/.

[32] John Paul Strong, Target Subprime Credit Using Facebook and Paid Search, STRONG AUTOMOTIVE MERCHANDISING (Apr. 14, 2019) https://strongautomotive.com/target-subprime-credit-facebook-paid-search/.

[33] Jacob Rugh & Douglas Masset, Racial Segregation and the American Foreclosure Crisis, 75(5) AMERICAN SOCIOLOGICAL REVIEW 629, 630 (Oct. 2010), available at http://www.asanet.org/wpcontent/uploads/savvy/images/journals/docs/pdf/asr/Oct10ASRFeature.pdf; *see also* Editorial, Fair Lending and Accountability, N.Y. TIMES (Sep. 7, 2011) https://www.nytimes.com/2011/09/08/opinion/fair-lending-and-accountability.html ("Studies by consumer advocates found that large numbers of minority borrowers who were eligible for affordable, traditional loans were routinely steered toward ruinously priced subprime loans that they would never be able to repay.")

[34] Jeremy B. Merrill & Kozlowska Hanna, How Facebook Fueled a PreciousMetal Scheme Targeting Older Conservatives, QUARTZ (Nov. 19, 2019) https://qz.com/1751030/facebook-ads-lured-seniors-into-giving-savings-to-metalscom.

[35] Emma Fletcher, *Social media a gold mine for scammers in 2021*, FEDERAL TRADE COMMISSION (Jan. 25, 2022), https://www.ftc.gov/news-events/datavisualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021 ("Here are some ways to help you and your family stay safe on social media: . . .Check if you can opt out of targeted advertising.").

[36] Thomas Germain, *The FBI Says You Need to Use an Ad Blocker,* GIZMODO (December 22, 2022), https://gizmodo.com/google-bing-fbi-ad-blocker-scam-ads-1849923478.

[37] § 7221(b)(2).

and where the system has been demonstrated to 3) work as intended and 4) not discriminate on the basis of a protected class.[38]

Those exceptions are limited by Section 7221(b)(6), which requires an opt-out be provided for certain uses of ADMT in all circumstances.[39] To better protect consumers, three changes are necessary to the opt-out regime in the Proposed Regulations.

1. *The set of ADMT uses that categorically require an opt-out should be expanded.*

As outlined below, the regulations should be updated to prohibit ADMT systems that rely on emotion detection technology, that involve government use of facial recognition technology, or that for predictive policing or in child-welfare proceedings.[40] However, if those prohibitions are not added, then the regulations should at least categorically require that an opt-out be provided to consumers.

These systems have too many well-documented problems to be forced on the public. For example, companies are increasingly using ADMT systems to evaluate job applicants during interviews. By analyzing the applicant's facial expression, among other things, these systems claim to determine "whether the candidate is tenacious, resilient, or good at working on a team."[41] But the link between facial expressions and emotions is neither reliable nor generalizable, and experts have warned that "the effects of different cultures and contexts has not been sufficiently documented."[42] In short, "these products are built on a bed of intellectual quicksand."[43]

Being denied a job because of faulty software can have significant consequences on a person's life. And when the government uses these kinds of systems, as they have in child-welfare proceedings and criminal investigations, the harms can be even more severe. But as written, the Proposed Regulations would not give the public the right to opt out of these inaccurate systems.

[38] *See* § 7221(b)(3) et seq.

[39] Currently, the regulations require that an opt out be provided "in all circumstances" when the ADMT is used for "behavior advertising" or to "train[] ... ADMT [systems]." § 7221(b)(6).

[40] *See* Section III.C below.

[41] Rachel Metz, *There's a New Obstacle to Landing a Job After College: Getting Approved by AI*, CNN (Jan. 15, 2020), https://www.cnn.com/2020/01/15/tech/ai-job-interview/index.html

[42] Jay Stanley, *Experts Say 'Emotion Recognition' Lacks Scientific Foundation*, ACLU (July 18, 2019), https://www.aclu.org/news/privacy-technology/experts-say-emotion-recognition-lacks-scientific.

[43] *Id.*

2. *The regulations should remove the "human appeal exception."*[44]

When an opt-out is not categorically required, businesses can avoid offering an opt-out for uses of ADMT that make a significant decision concerning a consumer so long as the business provides a "method to appeal the decision to a qualified human reviewer who has the authority to overturn the decision."[45] This exception is fundamentally flawed and should be removed.

Research indicates that humans are inherently trusting of algorithmic decisions. Even if reviewers "consider the relevant information provided by the consumer in their appeal"—as required by the regulations[46]—they are likely to be biased towards affirming the decision of the ADMT system.[47] If a human reviewer is often just a rubber stamp for the decisions made by the ADMT system, businesses may simply add a layer of human review to their ADMT systems, avoid offering an opt-out option for consumers, and have the automated decisions affirmed en masse by the human reviewers. The right to opt-out of ADMT systems would be effectively written out of the regulations.

3. *The Agency should clarify what qualifies as "necessary" in the regulations.*[48]

Businesses will have a strong incentive to classify their ADMT uses as "necessary" whenever those systems are good for their bottom line, rather than when they are *actually* necessary. The Agency should set clearer standards to prevent this gamesmanship.

For example, colleges and universities have for decades sorted through thousands (or even tens of thousands) of applications, without the use of ADMT systems, to determine who to accept.[49] However, it is easy to imagine universities today arguing that ADMT systems are needed in those situations given the large cost in both time and administrative staff salaries. This history makes it clear that those systems are not actually necessary, even though some universities might prefer to be able to reduce those kinds of expenses, even at the expense of students invisibly deprived of an opportunity for higher education by an algorithm.

[44] § 7221(b)(2).

[45] *Id.*

[46] § 7221(b)(2)(A).

[47] *See* David Nield, *This is the Point When People Start Trusting Algorithms More Than Other Humans*, SCIENCE ALERT (Apr. 17, 2021), https://www.sciencealert.com/this-is-when-people-start-to-trust-algorithms-more-than-humans.

[48] *See, e.g.*, § 7221(b)(3)(A) ("The automated decisionmaking technology is necessary to achieve, and is used solely for, the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them.")

[49] *See College Admission Is Easier, But Harvard Still 'Selective'*, HARVARD CRIMSON, (Jan. 8, 1981), https://www.thecrimson.com/article/1981/1/8/college-admission-is-easier-but-harvard/ (noting over 14,000 applications to Harvard University in 1981).

Similarly, businesses are increasingly using technology systems to track the "performance" of their warehouse employees.[50] For example, one large employer uses "radio-frequency handheld scanners" to "track[] and record[] every minute of 'time off task.'"[51] These systems pressure employees to prioritize speed above their own physical and mental well-being, including causing many of them to "skip water and bathroom breaks because they fear being disciplined and terminated."[52] It is clear these systems are not necessary—packages have been delivered, and delivered quickly, without punishing and harmful surveillance technologies. But because these systems allow businesses to improve their profit margins, they will argue they are "necessary" (for example, to enable one-day delivery).

"Necessary" cannot simply mean profit-maximizing. The regulations should set forth clear standards for what "necessary" requires.

4. *The regulations should include an objective standard for whether an AMDT system "works as intended."*

As written, the regulations do not outline any specific criteria that a business must use in determining whether their ADMT system works as it is intended. Thus, businesses will have every incentive to invest as little as possible in these systems, see how they perform, and then construct an argument as to why that's sufficient. For example, some emotion recognition systems claim to be ~75–80% accurate in identifying a person's emotional state based on the facial signals.[53] Under the regulations as written, it is unclear whether these systems are accurate enough to "work as intended." Given that uncertainty, businesses that develop and deploy these systems will be inclined to devote their energies to fighting a compliance battle about why that percentage is good enough, rather than allocating those resources to the difficult—but more societally useful—task of improving the technology itself.

5. *Evidentiary disclosure requirements should apply to all opt-out exceptions.*

The regulations already require that businesses provide supporting information as to the third and fourth requirements—that the ADMT systems work as intended and do not discriminate.[54] However, the regulations do not require similar documentation as to why the systems are necessary and proof that the systems are

[50] Lauren Kaori Gurley, *Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts*, VICE (June 2, 2022), https://www.vice.com/en/article/5dgn73/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts.
[51] *Id.*
[52] *Id.*
[53] Zi-Yu Huang et al., *A Study on Computer Vision for Facial Emotion Recognition*, SCIENTIFIC REPORTS (2023), https://www.nature.com/articles/s41598-023-35446-4.
[54] *See* §7152(a)(6)(B).

only used for those purposes. Requiring this information will not only reduce the incentive for businesses to improperly use one of the exceptions, but also empower the Agency to determine how often these exceptions are being used. This will allow the Agency to decide whether the exceptions need to be adjusted to avoid undermining the public's right to opt-out.

D. Actionable Post-Use Access Rights Should Be Mandatory, Not Optional.

The regulations require that after an ADMT system is used, the business allow the consumer to see "how the ADMT worked with respect to [that] consumer."[55] This description must include: (1) "How the logic, including its assumptions and limitations, was applied to the consumer;" and (2) "The key parameters that affected the output of the automated decisionmaking technology with respect to the consumer, and how those parameters applied to the consumer."[56] While these disclosures are important, the regulation should be strengthened.

The post-use notice is only valuable to consumers if it is actionable. And without understanding how they compare to other consumers, consumers faced with adverse ADMT decisions will not know whether they should pursue additional action. For example, if a person who knows they have a high credit score sees they were considered a "high risk" for missing payments, they may choose to follow up with the landlord to ensure the system had accurate information. Or if a Black applicant was in the 99th percentile for "rentability" but was still denied, they may choose to pursue legal action against the company under anti-discrimination laws. Thus, to empower consumers, the regulations should be changed so that a business must provide contextual information.

This requires only a small change to the existing regulations.

> § 7222. Requests to Access Information About the Business's Use of Automated Decisionmaking Technology.
>
> (b)(4)(C) A business also ~~may~~ **shall** provide the range of possible outputs ~~or~~ **and** aggregate output statistics to help a consumer understand how they compare to other consumers. For example, a business may provide the five most common outputs of the automated decisionmaking technology, and the percentage of consumers that received each of those outputs during the preceding calendar year.

[55] § 7222(b)(4).

[56] § 7222(b)(4)(A), (B).

III. The Risk Assessment Regulations Should Be Strengthened to Limit Harmful Applications.

A. Abridged assessments should include a plain-language explanation of the business's cost-benefit analysis.

The Proposed Regulations describe two versions of the statutorily required risk assessments: one "abridged" version that is provided annually to the Agency as a matter of course, and a second, more detailed assessment that is available to the agency upon request. *See* §§ 7157(b) (abridged risk assessments), 7152(a) (full risk assessments). The full assessments include a variety of information that businesses must compile about their processing of people's personal information, including the purpose, the categories of personal information, the operational elements, and the positive and negative impacts on people's privacy. § 7152(a)(1)–(5). The abridged assessments, by contrast, must only include an identification of the category of the processing, a statement of the purpose of the processing, and a list of the categories of personal information processed. § 7157(b)(2)(A)–(C).

The abridged risk assessment is insufficient to fulfill the purpose of risk assessments, both for businesses creating them and to the Agency as it does its work to protect consumers. Specifically, the requirement under Section 7157(b) that companies submit only abridged risk assessments every year (barring Agency action or a business voluntarily submitting a full risk assessment) creates problems for the Agency, consumers, and companies themselves.

The central problem is that abridged risk assessments need not contain any explicit or specific disclosure pertaining to the cost-benefit analysis of a given processing activity. Under Sections 7152 and 7154, businesses must conduct cost-benefit analysis as part of a full risk assessment *before* processing consumer data. But that cost-benefit analysis need not be included in the abridged assessment. As a result, the abridged risk assessment will not provide the Agency or the Attorney General with sufficient information to preliminarily assess baseline compliance with the Proposed Regulations. The Agency can, of course, request the full risk assessment, but adding the summary of the cost-benefit analysis will ease the burden on the Agency and the business by including important information in the submitted version.

Without the plain-language summary of the cost-benefit analysis the company has done, the Agency will be unable to assess preliminarily whether the business has complied with the law without seeking more information. Requiring that the Agency or the Attorney General take the additional step of requesting the full risk assessment in order to understand—even at a high level—the business's cost-benefit analysis will only waste resources, both of the Agency and the businesses processing personal information in ways that require risk assessments.

The Agency should restore the language in the December 2023 draft of the Proposed Regulations, which included a requirement that businesses include in abridged risk assessments a "plain-language explanation of why the negative impacts of the processing, as mitigated by safeguards, do or do not outweigh the benefits of the processing."[57]

B. The Agency has the power to substantively disagree with risk assessment submissions.

The risk assessment framework of the Proposed Regulations does not currently provide a clear mechanism for the Agency to disagree with a company's certification that the benefits of some processing activity outweigh the costs. This lack of an explicit delineated process risks hobbling the Agency's ability to prevent the most egregious privacy violations revealed by a risk assessment.

Risk assessments are required by the CCPA for a simple reason: when the risks to privacy of processing of consumers' personal information outweigh the benefits, the processing should be restricted or prohibited outright. As the statute makes explicit, risk assessments weigh the risks "with the goal of *restricting or prohibiting such processing* if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."[58]

Regulations that only require risk assessments to be prepared by businesses and maintained internally (and made available to the Agency upon request) are insufficient to protect the autonomy and dignity of the public from processing activities that do not meet the legal standard. Imagine a processing activity that risks significant harm to vulnerable consumers—like people searching for housing or employment—but which is marginally profitable for a business. When a business self-certifies that the processing's benefits outweigh the costs, it is the Agency's role under the statute to review that certification and the supporting analysis and determine independently whether the business has, under the law, properly performed the cost-benefit analysis. If the business's assessment is inconsistent with the law, then the processing, in the language of the statute, must be restricted or prohibited.

[57] December 2023 Draft Regulations, § 7158(b)(2)(E).

[58] Civil Code § 1798.185(a)(15)(B) (emphasis added).

We propose the following language, based on the statutory damages provisions in Section 1798.155(a), creating an explicit mechanism for the Agency to question and take action against deficient risk assessments:

> **Upon review of a business's Risk Assessment, if the Agency has any cause to conclude that the benefits of the processing do not outweigh the costs as required by statute, the Agency may require additional documentation or evidence from the business. If the Agency determines, after reviewing any further materials as necessary, that there is probable cause for believing that the benefits of the processing do not outweigh the costs in violation of the statute, the Agency may hold a hearing pursuant to Section 1798.199.55(a) to determine if a violation has occurred. If the Agency so determines that a violation has occurred, it may issue an order requiring the violator to restrict the processing to address such costs or prohibiting the business from such processing.**

C. The Agency should implement per se bans against certain types of processing activities.

The Agency should establish *per se* rules that categorically prohibit certain activities. While we commend the Agency for the steps already taken to subject certain processing activities—such as biologically identifying and profiling—to heightened risk-reporting requirements, *see* § 7201, such moves do not go far enough to protect consumers and workers. Under the current approach, these riskier activities merely trigger the need for more internal deliberation and paperwork. Pending the introduction of language granting the government the power to disagree with this paperwork or internal corporate judgment, however, the approach taken by the Proposed Regulations risks being an ineffective half-measure.

A more consumer-protective, simpler approach would be to set out *per se* rules banning companies from undertaking certain processing activities, punishable by the same penalties or noncompliance standards outlined above. These prohibited processing use-cases should at least include the following: predictive policing,[59]

[59] *See Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations*, ACLU (Aug. 31 2016).

emotional recognition,[60] facial and biometric surveillance for government actors,[61] and child-welfare proceedings.[62] Each of these applications, at present, pose an unduly high risk of discrimination against disadvantaged consumers.

These applications are within the scope of the Proposed Regulations. Private vendors often sell technology to the government, and those businesses fall within the Regulations' scope.[63] In the realm of predictive policing, for example, stories of third-party technology used by vendors at the government's behest to falsely accuse and arrest Black civilians are common.[64] Emotional-recognition technologies have already been used by businesses to track the expressions of migrants at the border,[65] and certain emotional-recognition A.I. intended for educational use[66] might also be deployed in public schools. The use of third-party private vendors to aggregate and process child welfare proceeding data—as well as make predictive judgments about this data—is also well-documented.[67]

Based on the available evidence of their potential harms, their penetration into the public sector through private vendors, and the potential difficulties in uncovering their use or misuse, the Proposed Regulations should prohibit the above processing activities.

[60] *See* Jay Stanley, *Experts Say 'Emotion Recognition' Lacks Scientific Foundation*, ACLU (July 18, 2019); *see also* Lisa Feldman Barret et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 ASS'N FOR PSYCH. SCI., 1, 46 (2019); Ifeoma Ajunwa, *Automated Video Interviewing as the New Phrenology*, 36 BERKELEY TECH. L. J. 1173, 1191 (2021).

[61] *See, e.g.*, *Keep Facial Recognition Off Police Body Cameras*, ACLU California Action; *Facial Recognition Technology Falsely Identifies 26 California Legislators with Mugshots*, ACLU NORCAL (Aug. 13, 2019); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1, 12 (2018).

[62] *See* Nat'l Indian Child Welfare Ass'n & Pew, *Time for Reform: A Matter of Justice for American Indian and Alaskan Native Children* (2007); Alan J. Dettlaff & Reiko Boyd, *Racial Disproportionality and Disparities in the Child Welfare System: Why Do They Exist, and What Can Be Done to Address Them?*, 692 ANNALS AM. ACAD. POL. & SOC. SCI. 253 (2020); Sally Ho & Garance Burke, *Here's how an AI tool may flag parents with disabilities*, AP NEWS (2023); Jerry Milner & David Kelly, *It's Time to Stop Confusing Poverty With Neglect*, THE IMPRINT (Jan. 17, 2020).

[63] *See* § 1798.140(d)(1), *et seq*.

[64] *See* Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N. Y. TIMES (Aug. 6, 2023); Kashmir Hill, *Wrongfully Accused by an Algorithm*, N. Y. TIMES (Jun. 24, 2020).

[65] *See* Daniel Boffey, *EU Border 'Lie Detector' System Criticised as Pseudoscience*, THE GUARDIAN (Nov. 2, 2018, 5:58 A.M.).

[66] See Peggy Keene, *The Privacy Implications of Intel's Classroom AI*, TEX. BAR J. (Sept. 2022).

[67] *See* Christopher Teixeira & Matthew Boyas, MITRE Corp., *Predictive Analytics in Child Welfare: An Assessment of Current Efforts, Challenges and Opportunities* 6-7 (2017); Anjana Samant, Aaron Horowitz, Kath Xu, and Sophie Beiers, *Family Surveillance by Algorithm: The Rapidly Spreading Tools Few Have Heard Of*, ACLU (Sept. 21, 2021).

IV. The Regulations Should Not Allow Trade-Secret Law To Be Weaponized for Improper Secrecy

Any regulations should also ensure that trade-secret law cannot be weaponized to undermine the ability for the public and the government to understand how systems affect people's livelihood and civil rights. While the CCPA has a trade-secret exception, that exception must hew to the proper contours of trade-secret law, and should not deprive Californians of access to information about the algorithms and practices that can affect their lives.

When trade-secret law can be weaponized against transparency to the government and the public, it is people's rights and safety that pay the price. For example, the 2018 crash of a Boeing 737 MAX passenger jet was caused by its automated flight control system.[68] But Boeing withheld crash information from the appropriate pilots and the public at large, purportedly because trade-secret law prohibited the disclosure of that proprietary information.[69] The same flight-control system then caused the 2019 crash, and a report by the House Committee on Transportation & Infrastructure concluded that "Boeing's and the FAA's secrecy after the first crash contributed to the second, by preventing pilots and the public from learning" of the system's design problems.[70]

People have also not been able to defend themselves properly against criminal charges because trade secret law has been used to deprive criminal defendants of access to information necessary for their defense.[71]

As algorithmic decisionmaking continues to expand, the risk that trade-secret law will be used to undermine the transparency necessary for the public and the government will only increase. The Agency should carefully scrutinize how to ensure that trade-secret law is not used in overbroad ways that trample on people's fundamental rights. If the Agency has probable cause to believe that the statute has been violated—including through an inappropriate or overbroad trade-secret claim—the law allows the Agency to hold a hearing to determine whether a violation has occurred and issue appropriate relief.[72] The trade secret exception should be carefully applied, and only in circumstances where it is statutorily required. And businesses should be prepared to substantiate to the Agency or the Attorney General any claims of trade-secret protection. Following the legal

[68] Christopher J. Morten, *Publicizing Corporate Secrets*, 171 U. PENN. L. R. 1319, 1322 (2023).

[69] *Id.*

[70] *Id.* at 1322–33.

[71] Vera Eidelman, *Secret Algorithms Are Deciding Criminal Trials and We're Not Even Allowed to Test Their Accuracy*, https://www.aclu.org/news/privacy-technology/secret-algorithms-are-deciding-criminal-trials-and

[72] CA Civil Code § 1798.199.60.

boundaries of trade secret law, the Agency and the Attorney General should ensure that the following limits exist:

Information that is publicly available or readily ascertainable should not be shielded by the trade secret exception. Public availability destroys trade secret protection.[73] As a result if information associated with an algorithm is available to the public, claims of trade secret protection for that information should be scrutinized carefully by the Agency and the Attorney General.

Information that has not been adequately protected should not be shielded by the trade secret exception. Trade secret owners must make "reasonable efforts" to safeguard information for it to be eligible for protection. Reasonable efforts may include "restricting access and physical segregation of the information, confidentiality agreements with employees, and marking documents with warnings or reminders of confidentiality."[74] The absence of these protections should call into question the applicability of a trade secret exception.

The "value" of the information must be properly determined. Civil trade secret law is codified in the California Uniform Trade Secrets Act[75] at the state level and the Defend Trade Secrets Act[76] at the federal level. Both acts generally protect information that derives independent economic value from the fact that it is not known to the public or persons who could derive economic value from it.[77] Trade secret information must be valuable at least in part *because* it is a secret, not merely valuable *and* a secret.[78] Courts have ruled that "the focus of the inquiry regarding the independent economic value element is on whether the information is generally known to or readily ascertainable by business competitors or others to whom the information would have some economic value."[79]

The organization claiming trade-secret protection must not have acquired the information improperly. Using the equitable doctrine of unclean hands, the Agency may refuse to recognize trade secret rights if an organization's directly related misconduct would make a finding in their favor unjust.[80] Crucially, the

[73] Cal. Civ. Code § 3426.1(d) (trade secret defined as "not being generally known to the public"); 18 U.S.C. § 1839(3) (trade secret defined as "not being generally known to, and not being readily ascertainable" by another who can obtain economic value from the information).
[74] *Id.*
[75] Cal. Civ. Code § 3426.
[76] 18 U.S.C. § 1836.
[77] Cal. Civ. Code § 3426; 18 U.S. Code § 1836.1
[78] *See Miranda v. Thiry*, 2021 U.S. Dist. LEXIS 231264 (C.D. Cal. Dec. 2, 2021).
[79] *Altavion, Inc. v. Konica Minolta Sys. Lab'y, Inc.*, 226 Cal.App.4th 26, 62 (2014) (quoting *Syngenta Crop Protection, Inc. v. Helliker*, 138 Cal.App.4th 1135, 1172 (2006)).
[80] *Keystone Driller Co. v. General Excavator Co.*, 290 U.S. 240, 245–56 (1933).

defense does not require the reporting organization to have acted illegally, only that their conduct related to the trade secret was "unconscientious."[81]

The unclean hands doctrine in particular allows the Agency to combat overly broad claiming of trade secrets when business misconduct is present (and it is often present). The Agency and the Attorney General's office should clarify that when the acts or practices of a business constitute unclean hands, that will eliminate businesses' authority to rely on trade secret protection in certain circumstances. As ADMT and other systems grow in popularity, so will opportunities for misuse of ADMT to harm consumers. In 2023 alone, one artificial intelligence, algorithm, and automation watchdog group recorded over 300 instances of potentially harmful and unethical use of ADMT.[82] Particularly egregious incidents include having Medicare benefits denied by ADMT,[83] collecting facial data without consent,[84] and faulty algorithms leading to wrongful arrests.[85] These harms should factor into the Agency's assessment of whether companies' trade secret protections are forfeited under the doctrine of unclean hands.

V. Conclusion

We commend the Agency on the Proposed Regulations and urge the Agency to take the steps recommended in these comments to ensure that consumers' privacy rights are protected.

Sincerely,

Jacob Snow
Senior Staff Attorney
Technology & Civil Liberties Program
ACLU of Northern California

Nicole Ozer
Technology & Civil Liberties Director
Technology & Civil Liberties Program
ACLU of Northern California

[81] *Kendall-Jackson Winery, Ltd. v. Superior Court*, 76 Cal. App. 4th 970, 980.

[82] *AI, algorithmic, and automation incidents*, AIAAIC (Feb. 14, 2024), https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents.

[83] *NaviHealth nH Predict used to deny Medicare Advantage benefits*, AIAAIC (Feb. 15, 2024), https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/navihealth-nh-predict-used-to-deny-medicare-advantage-benefits.

[84] *Prisma Labs sued for collecting facial biometrics without consent*, AIAAIC (Feb. 15, 2024), https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/prisma-labs-sued-for-collecting-facial-biometrics-without-consent.

[85] *Michael Williams gunshot detection wrongful arrest*, AIAAIC (Feb. 14, 2024), https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/michael-williams-gunshot-detection-wrongful-arrest.

Carmen-Nicole Cox
Director of Government Affairs
ACLU California Action

Emory Roane
Associate Director of Policy
Privacy Rights Clearinghouse

Sara Geoghegan
EPIC Senior Counsel
Electronic Privacy Information Center

Ben Winters
Director of AI and Data Privacy
Consumer Federation of America

Lee Tien
Legislative Director and Adams Chair
for Internet Rights
Electronic Frontier Foundation