COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER, CONSUMER ACTION, THE CONSUMER FEDERATION OF AMERICA, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

On Proposed Rulemaking Under the California Privacy Rights Act of 2020

(Proceeding No. 01-21)

November 8, 2021

The Electronic Privacy Information Center, Consumer Action, the Consumer Federation of America, and New America's Open Technology Institute submit these comments in response to the California Privacy Protection Agency (CPPA)'s September 2021 invitation for public input concerning the agency's development of regulations under the California Privacy Rights Act of 2020 (CPRA) and the California Consumer Protection Act of 2018 (CCPA). We support the efforts of the CPPA to establish robust data privacy protections for Californians. As the agency formulates regulations under the CPRA and CCPA, we urge you to continue "protect[ing] consumers' rights" and "strengthening consumer privacy" at every opportunity, consistent with the expressed will of California voters.[1] In particular, we urge you to impose rigorous risk assessment obligations on businesses whose data processing activities could reasonably harm individuals' privacy or security; to maximize the transparency of automated decisionmaking systems and minimize the burdens on individuals who wish to opt out of such systems; and to prevent any exceptions to user-directed limits on the use and disclosure of sensitive personal information from swallowing the rule.

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

I. Our organizations

The Electronic Privacy Information Center (EPIC) is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has long supported the establishment of a comprehensive federal privacy law while arguing that federal law should not preempt stronger state laws. EPIC has previously provided comments on the CCPA[2] and published a detailed analysis of the CPRA before its approval by California voters.[3]

Consumer Action[4] has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and utilities.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators. OTI sits within New America, a think tank based in Washington, DC.

---

[2] Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf.
[3] EPIC, *California's Proposition 24* (2020), https://epic.org/californias-proposition-24/.
[4] https://www.consumer-action.org/.

II. The agency should adopt an expansive definition of 'significant risk' and impose robust risk assessment obligations on covered businesses.

We urge the CPPA to adopt regulations that will (1) ensure a wide range of hazardous data practices meet the CPRA's "significant risk" standard; and (2) require businesses engaged in those hazardous data practices to conduct and publish meaningful and timely privacy risk assessments.

a. The meaning of 'significant risk'

Establishing a strong and effective definition of the term "significant risk" in the CPRA is vital.[5] Under section 1798.185(a)(15), the agency must issue regulations requiring "businesses whose processing of consumers' personal information presents *significant risk* to consumers' privacy or security" to conduct regular cybersecurity audits and risk assessments.[6] The CPRA does not define "significant risk,"[7] but the agency should interpret this term broadly to maximize the privacy protection afforded to California residents and to ensure that businesses routinely evaluate the hazards of processing and storing personal information. A "significant risk" must be understood to mean a *material* or *nontrivial* risk rather than an exceptional or unusual one. Establishing too high a threshold for audits and risk assessments would unduly limit the businesses from which a careful analysis of privacy and cybersecurity risks is required and undermine the express data protection purposes of the CPRA.

Not only is a broad reading of "significant risk" consistent with the aims of the CPRA; it also aligns with the meaning of the term in a related provision of the Civil Code concerning personal data. Section 1798.81.6 imposes various obligations on credit reporting agencies whose computer systems are "subject to a security vulnerability that poses a *significant risk* . . . to the security of

[5] Civ. Code § 1798.185(a)(15).
[6] *Id*. (emphasis added).
[7] However, it identifies "the size and complexity of the business and the nature and scope of processing activities" as factors to consider in the context of cybersecurity audits. Civ. Code § 1798.185(a)(15)(A).

computerized data that contains personal information[.]"[8] The term "significant risk" is defined in the same section as a risk that "*could reasonably result* in a breach of the security of the system . . . of personal information[.]"[9] Carrying this definition forward to the CPRA, the agency should construe the phrase "presents significant risk to consumers' privacy or security" as referring to data processing that *could reasonably result* in harm to consumers' privacy or security, not merely processing that is likely or certain to cause such harm. This also follows from the categories of information that the CPRA requires businesses to include in a risk assessment. Such assessments must specify "*whether* [their] processing involves sensitive personal information,"[10] which indicates that risk assessments are required even when a business does not process special categories of personal data that qualify as "sensitive."[11]

Although it is impossible to develop an exhaustive compilation of data processing activities that "present[] significant risk to consumers' privacy or security"—and therefore trigger a business's cybersecurity and risk assessment obligations—there are some forms of processing that definitively fit this description.[12] Senator Kirsten Gillibrand's Data Protection Act[13] offers a particularly useful compilation of hazardous data processing activities (defined there as "high-risk data practice[s]"),[14] many of which align with the CPRA's enumerated categories of sensitive personal information:

a. [T]he use of an automated decision system;
b. the processing of data in a manner that involves an individual's protected class, familial status, lawful source of income, financial status such as the individual's income or assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, or any other factor used as a proxy for identifying any of these characteristics;
c. a systematic processing of publicly accessible data on a large scale;

[8] Civ. Code § 1798.81.6(a) (emphasis added).
[9] Civ. Code § 1798.81.6(c) (emphasis added).
[10] Civ. Code § 1798.185(a)(15)(A) (emphasis added).
[11] Civ. Code § 1798.140(ae).
[12] Civ. Code § 1798.185(a)(15).
[13] S. 2134, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/2134/text.
[14] Civ. Code § 1798.140(ae).

d. processing involving the use of new technologies, or combinations of technologies, that causes or materially contributes to privacy harm;
e. decisions about an individual's access to a product, service, opportunity, or benefit which is based to any extent on automated decision system processing;
f. any profiling of individuals on a large scale;
g. any processing of biometric information for the purpose of uniquely identifying an individual, with the exception of one-to-one biometric authentication;
h. combining, comparing, or matching personal data obtained from multiple sources;
i. processing which involves an individual's precise geolocation;
j. the processing of personal data of children and teens under 17 or other vulnerable individuals such as the elderly, people with disabilities, and other groups known to be susceptible for exploitation for marketing purposes, profiling, or automated processing; or
k. consumer scoring or other business practices that pertain to the eligibility of an individual, and related terms, rights, benefits, and privileges, for employment (including hiring, firing, promotion, demotion, and compensation), credit, insurance, housing, education, professional certification, or the provision of health care and related services.[15]

As the agency develops regulations construing section 1798.185(a)(15), we urge you to include these forms of data processing in a non-exhaustive list of activities that "present[] significant risk to consumers' privacy or security[.]"[16]

b. The scope of risk assessments

As Professor Gary T. Marx writes, the object of a privacy risk assessment is to "anticipate[] problems, seeking to prevent, rather than to put out fires."[17] We urge the agency to implement the risk assessment provisions of the CPRA with this purpose in mind.

Under section 1798.185(a)(15)(A), when a business is engaged in "activities that "present[] significant risk to consumers' privacy or security," it must submit "on a regular basis a risk assessment with respect to [its] processing of personal information[.]" The CPRA specifies two categories of information that the assessment must contain: (1) "whether the processing involves sensitive personal information," and (2) an analysis "identifying and weighing the benefits resulting

[15] *Id.*
[16] Civ. Code § 1798.185(a)(15).
[17] *Privacy Impact Assessment* at v (David Wright & Paul de Hert, eds., 2012).

from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing[.]"[18] The goal of a risk assessment is to "restrict[] or prohibit[] the 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."[19]

First, although the categories of information set out by section 1798.185(a)(15)(A) are both essential, a risk assessment (also known as a privacy impact assessment or data protection impact assessment) must go further.[20] The E-Government Act of 2002 offers a useful starting point for setting the parameters of a risk assessment. Before initiating a new collection of personal information or procuring information technology that will process personal information, a federal agency must conduct, review, and publish a privacy impact assessment that explains:

> (I) what information is to be collected;
> (II) why the information is being collected;
> (III) the intended use of the agency of the information;
> (IV) with whom the information will be shared;
> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and]
> (VI) how the information will be secured[.][21]

The Office of Management and Budget (OMB) adds that privacy impact assessments under the E-Government Act:

> 1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
> 2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the

[18] Civ. Code § 1798.185(a)(15)(A) (emphasis added).
[19] Civ. Code § 1798.185(a)(15)(A).
[20] *See* EPIC, *Privacy Impact Assessments* (2021), https://epic.org/issues/open-government/privacy-impact-assessments/.
[21] E-Government Act, Pub. L. No. 107-347, § 208(b)(2)(B)(ii), 116 Stat. 2899, 2901 (Dec. 17, 2002).

elements identified in section II.C.1.a.(i)-(vii) [of the OMB Guidance], to the extent these elements are known at the initial stages of development;
3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.[22]

The OMB also requires privacy impact assessments concerning "major information systems" to "reflect more extensive analyses of":

1. the consequences of collection and flow of information,
2. the alternatives to collection and handling as designed,
3. the appropriate measures to mitigate risks identified for each alternative and,
4. the rationale for the final design choice or business process.[23]

And Article 35 of the European Union's General Data Protection Regulation (GDPR), which requires data protection impact assessments for all high-risk data processing activities, specifies that an assessment must include:

a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c. an assessment of the risks to the rights and freedoms of data subjects . . . ; and
d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[24]

At a minimum, we recommend that the risk assessments required of businesses under the CPRA include the categories of information set out in the E-Government Act and the GDPR.

Second, in assessing the "risks to the rights of the consumer associated with . . . processing," businesses should be required to evaluate the full range of privacy harms and civil rights violations

[22] OMB, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10 [hereinafter *OMB Circular*].
[23] *Id.* at 34.
[24] Commission Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119).

that may result from processing and disclosure of personal data.[25] Too often, risk assessments focus on the narrow question of whether personal data collected by the institution is secure from breaches. Although this is an essential element of data protection—one built into the CPRA's requirement for annual cybersecurity audits—it is only the beginning of a more fulsome analysis that institutions must undertake when processing personal data. Businesses must consider not only the harms of unintended or unauthorized uses of data, but also the harms of *intended* uses of the data, including screening, scoring, and other forms of algorithmic decisionmaking.[26] Businesses must also account for the full range of harms that can result from the processing and misuse of personal information. Professors Danielle Keats Citron and Daniel Solove have recently mapped out this spectrum, which includes numerous physical, economic, reputational, psychological, autonomy, discrimination, and relationship harms.[27] And businesses must take special account of the uneven impact of data processing, which disproportionately harms people of color, low-income individuals, and other marginalized populations.[28]

Third, ensuring the right timing and frequency of risk assessments is critical. As the CPRA's requirement of "regular" privacy risk assessments reflects,[29] an assessment cannot be treated as a static, one-off undertaking. Rather, "it is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project. It is a process that should

[25] Civ. Code § 1798.185(a)(15)(A).
[26] *See* EPIC, *Screening and Scoring* (2021), https://epic.org/issues/ai/screening-scoring/.
[27] Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, GW Law Faculty Publications & Other Works (2021), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2790&context=faculty_publications.
[28] *See, e.g.*, Fed. Trade Comm'n, *Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color* at 40 (Oct. 2021), https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf.
[29] Civ. Code § 1798.185(a)(15)(A).

continue until and even after the project has been deployed."[30] Or, as the OMB warns federal agencies, a risk assessment

> is not a time-restricted activity that is limited to a particular milestone or stage of the information system or [personally identifiable information] life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles. Accordingly, a PIA shall be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology."[31]

We urge the agency to require the completion of a risk assessment as soon as a business takes material steps toward data processing that will "present[] significant risk to consumers' privacy or security" so that the risks to individuals can be prevented or mitigated *before* any processing begins. Allowing risk assessments to be postponed until the last minute (or even until after data processing has begun) would turn the assessments into a simple box-checking exercise and facilitate the whitewashing of harmful data practices.[32] We also urge the agency to require covered businesses to review, update, and resubmit privacy risk assessments (1) well in advance of any change to a business's data processing activities that might alter the resulting risks to individuals' privacy, and (2) in any event, no less than once per six month period.

Finally, it is important that both the CPPA and the business submitting a risk assessment publish the full results of the assessment promptly, conspicuously, and by means that are readily accessible to interested members of the public. In addition to forcing an institution to evaluate and

---

[30] *Privacy Impact Assessment*, *supra* note 17, at 5–6.
[31] *OMB Circular*, *supra* note 22, app. II at 10.
[32] *See, e.g.*, EPIC, *EPIC v. U.S. Postal Service* (2021), https://epic.org/documents/epic-v-u-s-postal-service/ (detailing the U.S. Postal Service's failure to complete a privacy impact assessment before deploying facial recognition and social media surveillance tools); EPIC, *EPIC v. Commerce* (2020), https://epic.org/documents/epic-v-commerce-census-privacy/ (detailing the Census Bureau's failure to complete a privacy impact assessment before attempting to add the citizenship question to the 2020 Census); EPIC, *EPIC v. Presidential Election Commission* (2019), https://epic.org/documents/epic-v-presidential-election-commission/ (detailing the failure of the Presidential Advisory Commission on Election Integrity to complete a privacy impact assessment before initiating a nationwide collection of state voter data).

mitigate the harms of data processing, a risk assessment "also serves to inform the public of a data collection or system that poses a threat to privacy."[33] Although the CPRA already requires the agency to "provide a public report summarizing the risk assessments filed with the agency,"[34] we believe the underlying assessments should be presumptively public, subject only to the narrow redactions necessary to protect data security and trade secrets. This added degree of transparency will significantly enhance the data protection benefits of the CPRA without imposing significant additional burdens on the businesses that are already required to produce risk assessments.

III. The agency should embrace a broad definition of automated decisionmaking technology, maximize the disclosure of information about such systems, and minimize the burden on individuals to opt out.

We urge the CPPA to adopt regulations that will (1) include broad, rights-enhancing definitions of "automated decisionmaking technology" and "profiling"; (2) ensure easy access to information about the use and logic of automated decisionmaking systems; and (3) make it as easy as possible for individuals to opt out of such systems.

a. The meaning of 'automated decisionmaking technology' and 'profiling'

The agency should construe the terms "automated decisionmaking technology" and "profiling" broadly given the range of systems that can cause algorithmic harm. In defining automated decisionmaking technology, the agency should clarify that this term not only includes systems that *make* decisions unilaterally, but also systems that provide recommendations, support a decision, or contextualize information. We particularly recommend Rashida Richardson's definition of automated decision systems, which encompasses "any tool, software, system, process, function,

[33] EPIC, *supra* note 20.
[34] Civ. Code § 1798.199.40(d)

program, method, model, and/or formula designed with or using computation to automated, analyze, aid, augment, and/or replace [] decisions, judgments, and/or policy implementation."[35]

One of the most dangerous functions of automated decisionmaking is profiling. Profiling includes any form of automated processing of personal information used "to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[36] In applying this definition, the agency must be sensitive to the increasing prevalence of profiling and the special impacts of this practice in hiring, criminal justice, credit, and the provision of public benefits.

The following is a non-exhaustive list of systems and tools that qualify as automated decisionmaking technology in commercial settings, many of which also constitute profiling:

- Analysis of voice or facial expressions during a job interview for traits like "dependability," "emotional intelligence," and "cognitive ability";[37]
- Mortality risk predictions that inform COVID-19 care, kidney transplants, and other health care determinations;[38]
- Education services that monitor the internet activity of K-12 students;[39]

[35] Rashida Richardson, *Defining and Demystifying Automated Decision Systems,* 81 Md. L. Rev. 19 (forthcoming 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811708.
[36] Civ. Code § 1798.3.85(a)(16).
[37] Alex Engler, *Auditing Employment Algorithms for Discrimination*, Brookings Inst. (Mar. 12, 2021), https://www.brookings.edu/research/auditing-employment-algorithms-for-discrimination/.
[38] Mohammed Pourhomayoun & Mahdi Shakbi, *Predicting Mortality Risk In Patients With COVID-19 Using Machine Learning To Help Medical Decision-Making*, 20 Smart Health 100178 (2021).
[39] Benjamin Herold, *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming.*, Educ. Week (May 30, 2019), https://www.edweek.org/leadership/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05; Mark Keierleber, *'Don't Get Gaggled': Minneapolis School District Spends Big On Student Surveillance Tool, Raising Ire After Terminating Its Police Contract*, The74 (Oct. 18, 2020), https://www.the74million.org/article/dont-get-gaggled-minneapolis-school-district-spends-big-on-student-surveillance-tool-raising-ire-after-terminating-its-police-contract/.

- Exam proctoring tools using facial recognition and automated processing to identify potential instances of cheating;[40]
- The calculation of credit scores based on thousands of opaque data sources;[41]
- Recommendation algorithms on services like YouTube and Facebook;[42]
- "Fit scores," which yield a simplistic analysis a person's diet, exercise, and habits that may be computed by or delivered to insurance companies; and[43]
- Systems that purport to detect moods and emotions.[44]

Some of the most dangerous applications of profiling are facilitated by private companies but used in government settings such as law enforcement and the provision of public benefits. These include:

- Predictions of where a crime might occur next or the likelihood that an individual may commit a crime, which inform police resource allocation;[45]
- "Gang databases" that collect and combine sensitive information, subjective inputs, and social media information to categorize individuals as potentially gang-affiliated;[46]

---

[40] *Privacy Center*, Respondus (2021) https://web.respondus.com/privacy/privacy-additional-monitor/.
[41] *See* Aaron Klein, *Reducing Bias In AI-BASED Financial Services*, Brookings Inst. (July 10, 2020), https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/; Kevin Peachey, *Sexist And Biased? How Credit Firms Make Decisions*, BBC (Nov. 18, 2019), https://www.bbc.com/news/business-50432634.
[42] Debashis Das, Laxman Sahoo & Sujoy Datta, *A Survey Recommendation System*, 160 Int'l J. Comput. Applications 0975-8887 (2017).
[43] *See generally* Stewart Rogers, *Data science, machine learning, and AI in fitness – now and next*, Neoteric (Aug. 19, 2021), https://neoteric.eu/blog/data-science-machine-learning-and-ai-in-fitness-now-next/.
[44] Alexa Hagerty & Alexandra Albert, *AI Is Increasingly Being Used To Identify Emotions—Here's What's At Stake*, The Conversation (Apr. 15, 2021), https://theconversation.com/ai-is-increasingly-being-used-to-identify-emotions-heres-whats-at-stake-158809.
[45] *See* Caroline Haskins, *Academics Confirm Major Predictive Policing Algorithm Is Fundamentally Flawed*, Vice (Feb. 14, 2019), https://www.vice.com/en/article/xwbag4/academics-confirm-major-predictive-policing-algorithm-is-fundamentally-flawed.
[46] *See* Rashida Richardson & Amba Kak, I*t's Time For A Reckoning About This Foundation Piece Of Police Technology*, Slate (Sept. 11, 2020), https://slate.com/technology/2020/09/its-time-for-a-reckoning-about-criminal-intelligence-databases.html.

- Fraud detection and prevention services, which monitor activities of benefit recipients and score the likelihood that they are committing unemployment or other type of benefit fraud;[47]
- The use of facial recognition systems to confirm public benefit eligibility; and[48]
- The application of connected prescription drug monitoring programs.[49]

We encourage the CPPA to incorporate these examples when construing the terms "automated decisionmaking technology" and "profiling."

b. Consumer access to information about automated decisionmaking systems

The CPRA instructs the agency to create regulations that will govern how access and opt-out rights operate. To operationalize these rights, we urge the agency to focus on ensuring access to "meaningful information about the logic involved in . . . decision-making processes," as the CPRA requires.[50]

There are two primary barriers to meaningful access to information about automated decisionmaking and profiling: (1) a lack of awareness that a system is being used at all, and (2) a lack of detail about the system sufficient to allow an individual to opt out. Accordingly, the agency must ensure that the use of automated decisionmaking tools is conspicuously disclosed and that accurate information about those systems is made available to individuals in a timely and user-friendly fashion.

---

[47] *See* Ashesh Anad, *How Is AI Used In Fraud Detection?*, Analytic Steps (Sept. 21, 2021), https://www.analyticssteps.com/blogs/how-ai-used-fraud-detection.
[48] Mia Sato, *The Pandemic Is Testing The Limits of Facial Recognition*, MIT Tech. Rev. (Sept. 28, 2021), https://www.technologyreview.com/2021/09/28/1036279/pandemic-unemployment-government-face-recognition/.
[49] *See generally* Daniel B. Neill & William Herlands, *Machine Learning For Drug Overdose Surveillance*, 36 J. Tech in Hum. Servs. 8-14 (2018).
[50] Civ. Code § 1798.185(a)(16).

The CPPA must decide (1) what information must be made available to provide meaningful access and provide individuals with a real opportunity to opt out; (2) the process of how companies should report this information and ensure its availability to consumers; (3) whether the developer of a system and/or the user of that system should be responsible for disclosure; (4) how the consumer should be given access to this information; and (5) methods for enforcement and consequences for insufficient or misleading information. We urge the agency to mandate, at minimum, that a business disclose the purpose of an automated decisionmaking system; how the system is being used; the factors the system relies on; a plain-language explanation of the logic of the system;[51] the sources and life cycle of the data processed by the system, including any brokers or other third-party sources; and how the system has been evaluated for accuracy and fairness, including links to any audits, validation studies, or impact assessments.

In a growing number of countries, automated decisionmaking systems are required to undergo algorithmic impact assessments. In Canada, for example, businesses input information about automated decisionmaking systems into a standardized survey, which allows for the evaluation of system based on design attributes, the sensitivity of data processed, and the system's connection to areas requiring additional considerations and protections.[52] This type of form is something the CPPA could use to collect and ensure uniform reporting of key information about automated decisionmaking systems. The Canadian assessment asks each business to evaluate the stakes of the decisions that a system makes, the vulnerability of subjects, and whether the system is a predictive tool.[53] The tool also allows for multiple answer options and detailed explanations of responses. In some cases, the Canadian tool requires a business to identify the downstream processes of a system.

[51] For example, in a predictive profiling system or automated decisionmaking system, the explanation should include data sources and how particular inputs affect determinations (*e.g.*, if a criminal arrest in the last three years increases a "risk" classification by two points).
[52] Canada Digit. Servs., *Algorithmic Impact Assessment* (2021) https://open.canada.ca/aia-eia-js/?lang=en.
[53] *Id*.

This includes asking (1) whether the system will only be used to assist a decision-maker; (2) whether the system will be making a decision that would otherwise be made by a human; (3) whether the system will be replacing human judgment; (4) whether the system will be used by the same entity that developed it; and (5) for details about the system's economic and environmental impacts.[54] The CPPA should consider requiring similar reporting from businesses that deploy or sell automated decisionmaking systems.

Finally, meaningful access requires *actual* notice that automated decisionmaking is being used and easy retrieval of information about the system prior to, during, and after its use. Depending on the context, this could take the form of icon, banner, pop-up, or other type of conspicuous warning. We urge the agency to set clear minimum baselines and methods of disclosure in order to secure meaningful information for California residents about each automated decisionmaking or profiling system.

c. The right to opt out of automated decisionmaking systems

The right to opt out of automated decisionmaking systems under the CPRA is groundbreaking, but that right cannot be fully realized without key disclosures and protections. Individuals must be given complete information about the use and operation of automated decisionmaking systems, a user-friendly method to exercise opt-outs, a clear explanation about the scope of each opt-out they exercise, and confidence that their decisions to opt out will be honored.

The agency should pay special attention to the implementation of opt-outs by companies that process personal data across multiple platforms or websites. For example, Facebook/Meta Platforms' operations include Facebook, Instagram, WhatsApp, Oculus, and Facebook Login on third-party sites. Without strong regulations, a conglomerate like Facebook may make it difficult to opt out of

[54] *Id*.

automated decisionmaking systems across all its platforms (or even to determine how broadly a given opt-out extends in the first place).[55] We urge the agency to establish an easy method of opting out of automated decisionmaking systems across all of a company's properties.

For an opt-out mechanism to be effective, it must be simple and accessible. The CCPA already imposes certain consumer control mechanisms on covered entities, including the requirement to provide a "do not sell or share my personal information' link. Companies must also recognize Global Privacy Control as a valid consumer request to opt out of the sale of an individual's personal information.[56] Universal "do not track" regimes make opting out more accessible and should be implemented whenever possible. In order to streamline the CPRA opt-out process and maximize individual control over personal data, the agency should consider requiring covered entities to respect a universal opt-out signal for automated decisionmaking systems, as well.

IV. Any exceptions to consumer-directed limits on the use and disclosure of sensitive personal information should be narrowly drawn.

The agency should construe any exceptions to the CPRA's consumer-directed limits on use and disclosure of sensitive personal information narrowly to ensure that Californians' privacy rights are fully respected. While rare circumstances may justify nonconsensual disclosure of a resident's sensitive personal information, the CPPA must not allow exceptions to swallow the rule. In drafting its regulations, the agency should avoid the pitfalls of the Privacy Act of 1974 (Privacy Act)'s "routine-use" exception.[57] Any exceptions should be narrow, rare, and enumerated, and the CPPA should take an active role in enforcing that narrow language.

[55] *See* Steven Melendez, *Ready To Quit Facebook? It's Harder To Opt-Out Than You Think*, Fast Company (Oct. 6, 2021), https://www.fastcompany.com/90683647/facebook-whistleblower-quitting-data-collection.
[56] Cal. Dep't of Justice, *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa.
[57] 5 U.S.C. § 552a.

The Privacy Act provides a cautionary tale about the danger of vague and ill-enforced exceptions to data protection laws. The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the consent of the "individual to whom the record pertains."[58] However, the routine use exception permits an agency to disclose private data without consent if the agency determines that disclosure is "compatible with the purpose for which [the information] was collected."[59] The agency needs only to publish a proposed routine use in the Federal Register for that use to become a presumptively valid exception.[60]

The routine use exception has significantly diminished the Privacy Act's efficacy, giving agencies excessive power to define which of their activities are exempt from the statute. Agencies regularly claim extremely broad routine uses, taking advantage of the "compatibility" standard's vagueness. For example, the National Security Agency (NSA) declared that the purpose of its Operations Records database is to "maintain records" related to the NSA's mission.[61] What use or disclosure of data would not be compatible with "maintaining records"? Very few: the NSA claims it may disclose or use private data without consent whenever it is "compatible with" providing or obtaining intelligence or other information related to national security.[62] Similarly, the Department of Defense proposed creating a database of tens of millions of Americans for recruiting purposes but claimed as "routine uses" seemingly non-related activities, including providing data to law enforcement agencies for investigation and national security uses.[63] These wide-ranging "routine

[58] *Id.* § 552a(b).
[59] *Id.* § 552a(a)(7).
[60] *Id.* § 552a(e)(4) (agencies "publish in the Federal Register . . . each routine use of the records contained in the system, including the categories of users and the purpose of such use.").
[61] System of Records, 80 Fed. Reg. 63,749 (Oct. 21, 2015); *see also* Comments of EPIC to the Nat'l Sec. Agency, GNSA 18 Operations Records System of Records Notice, Docket ID: DoD-2015-OS-0100 (Nov. 20, 2015), https://www.epic.org/privacy/nsa/EPIC-NSA-SORN-Comments-2015.pdf.
[62] *Id.*
[63] Notice to Add a System of Records, DHRA 04--Joint Advertising and Market Research Recruiting Database., 70 Fed. Reg. 29,486; *see also* Comments of EPIC on the DHRA 04 Joint Advertising and

uses" stretch the definition of "compatible" and have contributed to a gradual erosion of the Privacy Act's protections.

Moreover, the federal agency charged with Privacy Act oversight, the OMB, has also failed to constrain agencies' overbroad application of the routine use exception.[64] The Privacy Act delegates enforcement powers to the OMB director, but the agency has issued guidance only sporadically,[65] has failed to keep up with changes in case law, and has given its blessing to practices that are arguably inconsistent with the Privacy Act.[66]

The CPPA can ensure that any exceptions to the CPRA's user-directed limits do not swallow the rule by drawing carve-outs narrowly and carefully policing their use by businesses. For example, the Electronic Communications Privacy Act (ECPA) has an exception for data uses or disclosures "necessary incident to the rendition of [the] service."[67] By instituting a more searching review of stated uses, ECPA's "necessary" standard has proven more privacy protective than the Privacy Act's "compatib[ility]" language.[68] The CPPA should also regulate businesses' reliance on use and disclosure exceptions more aggressively than OMB has regulated federal agencies' assertions of the routine use exception.

If any specific exceptions to consumer-directed use and disclosure limitations are proposed in response to the CPPA's current invitation for comments, we would be happy to respond to such proposals through supplemental comments or at a later stage of the regulatory process.

Marketing Research Recruiting Database to Dep't of Def. (June 22, 2005), https://epic.org/privacy/profiling/dodrecruiting.html.

[64] *See* Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exception*, 40 Am. U. L. Rev. 957, 983–98 (1991).

[65] *See* The White House, *Privacy* (2021), https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/ (listing two OMB memoranda on the Privacy Act in the past 20 years).

[66] *Id.* at 984.

[67] 18 U.S.C. § 2511(2)(a)(i).

[68] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417, 1482–83 (2009).

V. Conclusion

We thank the CPPA for the opportunity to comment on the forthcoming CPRA regulations and look forward to working with the agency in the future to protect the privacy of all Californians.

Respectfully submitted,

Electronic Privacy Information Center
Consumer Action
Consumer Federation of America
New America's Open Technology Institute