Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Comment on
Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

By

Grace Gedye, Policy Analyst
Stacey Higginbotham, Policy Fellow
Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

February 19, 2025

Consumer Reports[1] appreciates the opportunity to provide feedback on the California Privacy Protection Agency's (CPPA) Invitation for Comments on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies. We thank the CPPA for initiating this proceeding and for its other efforts to protect consumer privacy.

Every day, Californians are subject to high-stakes decisions made with the help of automated systems about their access to employment opportunities, lending services, housing, insurance, and more. There is clear evidence that these systems–which rely on plumbing Californians' personal data–can be biased[2] and faulty,[3] causing a wide range of harms. The Agency's proposed rules are critical, and represent a reasonable, measured step to provide Californians with transparency and agency.

The Agency has clear statutory authority to pursue this rulemaking process. As is explained in greater detail by other commenters, including the American Civil Liberties Union of Northern California, section 1798(a)(15) of the CCPA enables the agency to regulate businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform annual cybersecurity audits and conduct risk assessments. Section 1798(a)(16) gives the Agency the authority to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology." Additionally, the CCPA empowers the agency to promulgate rules in all areas that would "further the purposes of this title, including, but not limited to, the following areas," in Section 185.

Our comment proceeds in three sections. In the first, we largely praise the Agency's efforts around cybersecurity audits. In the second, we argue that the Agency should strengthen requirements around risk assessments, including by recommendation that the Agency grant itself a formal mechanism to contest businesses' self-assessments of the tradeoffs between the risks and benefits of their processing activities. Finally, we discuss the proposed regulations around ADMTs, recommending the Agency improve the definition of 'automated decisionmaking technology', and add additional clarity to the opt-out right, right to appeal, and the post-decisions access right.

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-ziad_obermeyer.pdf

[3] https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/

Comments on Cybersecurity Audit Proposal

The cybersecurity audit proposal is a welcome tool to ensure that companies processing consumer data actually take the necessary steps to improve their overall cybersecurity. The 18 requirements covered by the audit are a fairly complete list of modern best practices acknowledged by agencies such as NIST[4] and CISA.[5] They are also elements in several federal and municipal[6] procurement contracts, which mean that companies have already found ways and processes that will help them meet these requirements.

The proposed regulations also recognize the fact that cybersecurity and compliance regulations are already extant and allows companies to submit proof that they have completed some of the audit requirements as part of a different compliance regime. This helps companies avoid conducting multiple audits, or doubling up on efforts to comply with the many different security frameworks associated with their industries.

The proposed regulations also require the auditor to actually assess the security practices using interviews, documentation, and sampling to ensure that the company cannot simply tell the auditor that they are following best practices without providing some proof. This also clarifies the process of auditing so companies cannot shop around for an audit firm that will simply rubber stamp their audit based on company assertions. While this level of granularity will likely frustrate some companies, it is a necessary safeguard to ensure that companies are actually putting real cybersecurity best practices into play.

Additionally by requiring someone at the board level or the highest ranking executive “with authority to certify on behalf of the business and who is responsible for the business’s cybersecurity program.” The audit requirements make it easier to establish some sense of personal accountability for cybersecurity. There is an emerging trend in enforcement

There was concern in earlier comments that requiring an annual audit only offers a snapshot “reflective of a point in time and cannot reflect a real-time measure of the state of an organization’s security practices.[7]” However, such concerns miss the fact that there are still many organizations that are blithely unaware of their overall cybersecurity hygiene or are actively avoiding addressing known issues. For example, the Change Healthcare breach from February 2024, that resulted in the disclosure of 190 million consumers’ private data was a

---

[4] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[5] Zero Trust Maturity Model 2.0. April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

[6] California Cybersecurity Task Force (2023) 2023 California Cybersecurity Plan https://www.caloes.ca.gov/wp-content/uploads/Homeland-Security/Documents/California_Cybersecurity_Plan_FINAL_v1.5.5_20230921.pdf

[7] Comments from Crowdstrike for California’s CCPA proposal PR 02-2023 *p. 2* submitted March 27, 2023 https://cppa.ca.gov/regulations/pdf/rm2_pre_comments_27_52.pdf#page=301

result of hackers gaining access to stolen credentials and then accessing a server that did not require multifactor authentication[8].

Requiring MFA for remote access has been a cybersecurity best practice for sensitive data for a decade. Consumer Reports cannot speculate as to why a multi-billion healthcare organization with hundreds of millions of consumers' sensitive personal information didn't take such basic precautions, but these sorts of oversights are exactly the types of things an audit can detect. And once implemented it is unlikely that a business would revert back to poorer cybersecurity practices, meaning the act of taking this snapshot in time would result in better cybersecurity hygiene.

Security is never foolproof. All one can do is try to harden infrastructure to make attacks more challenging and less rewarding. The continued monitoring implied by the annual audit is an excellent tool to prompt companies to evaluate and remediate their cybersecurity hygiene on a regular basis. Additionally, the audit also requires covered companies to have plans in place to respond to an incident and includes provisions for a disaster recovery plan. Having a high-quality disaster recovery plan means that ransomware attacks are less likely to result in service outages, which is of substantial benefit to consumers when companies providing essential services such as utilities or healthcare are hacked.

Taken together, the audit process and audit requirements are a tool that can push covered companies to implement and follow cybersecurity best practices that will harden their infrastructure against today's attacks. Looking forward, Consumer Reports would like to see provisions for adapting the audit process and requirements to meet the changing demands of the security landscape.

Comments on Risk Assessment Proposal

The proposed regulations seek to implement Section 1798.185(14)(B) of CCPA, which empowers the CPPA to issue regulations requiring businesses whose processing of personal information "presents significant risk to consumers' privacy or security" to "[s]ubmit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information." In general, we believe risk assessments, if appropriately scoped and backstopped by meaningful enforcement, can play an important role in prompting businesses to reckon with the dangers of their data processing activities at an early stage, helping them mitigate serious harms before consumers encounter them.[9] We are therefore pleased to see in the proposed regulations broad applicability of the risk assessment

[8] "Examining the Change Healthcare Cyberattack" Hearing Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations. 118th Congress (2024) testimony of Andrew Witty, CEO of United Healthcare https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

[9] Margot Kaminski, The Developing Law of AI: A Turn to Risk Regulation, The Digital Social Contract: A Lawfare Paper Series, U of Colorado Law Legal Studies Research Paper No. 24-5, (April 2023), available at: http://dx.doi.org/10.2139/ssrn.4692562

requirement, whereby businesses must prepare one whenever they meet one of several criteria, including selling personal data, processing sensitive data, and using automated decisionmaking for a significant decision concerning a consumer.[10] These criteria should be preserved in any future version of the rules.

However, we suggest several improvements to ensure that the proposed risk assessments benefit consumers to the fullest extent possible.

Align Requirements Around Disclosing the "Logic" Of Automated Decisionmaking Technology

The proposed rules require that businesses using ADMTs for a significant decision concerning a consumer or for extensive profiling must identify in the risk assessment "[t]he logic of the automated decisionmaking technology, including any assumptions or limitations of the logic."[11] This largely echoes language in Section 7220 (Pre-Use Notice) that requires businesses to share with consumers a plain language explanation of the "the logic used in the automated decisionmaking technology," except that in the Pre-Use Notice, businesses must also share "the key parameters that affect the output of the automated decisionmaking technology."

Presumably, the purpose of replicating this requirement in the risk assessment is to allow businesses to explain the logic of their ADMTs in further detail than they would in the plain language disclosure within the Pre-Use Notice. However, without the commensurate requirement that businesses share the "key parameters affecting automated decisionmaking technology" the proposal may allow businesses to provide vague or ambiguous information in the risk assessment. This may frustrate the Agency's goal of advancing their and consumers' understanding of these critical tools through the risk assessment beyond what is already known via the Pre-Use Notice. For example, a business utilizing tenant screening software may simply respond that the "logic" of the technology is to assess tenants' suitability for the property or ability to pay rent. They may further state that the assumption of such a tool is that the selected criteria are relevant to the landlord and will produce a higher quality of applicant.

In order to avoid this scenario, at a minimum, the Agency should clarify that businesses must identify in their risk assessment the key parameters that affect the output of a given ADMT, as well as any evidence that supports the relevance of those key parameters to the decision the business is ultimately attempting to make. The latter requirement will more ensure businesses more fully meet the requirement that they assess the "assumptions or limitations of the logic"[12] in the ADMTs they use. In addition, it will provide businesses with the opportunity to expand on their explanation of the logic used by the ADMT in their employ beyond the plain language explanation and allow the Agency to more closely scrutinize business' justifications for using an ADMT in a given context.

---

[10] Proposed Rules, Section 7150(b)
[11] Proposed Rules, Section 7152(a)(3)(G)(i)
[12] Proposed Rules, Section 7152 (a)(3)(G)(i)

CPPA Should Clarify its Authority to Contest Business' Assessments of Cost-Benefit Tradeoffs

The statutory text authorizing CPPA to create regulations around risk assessments differs from the 16 of the other states with comprehensive privacy laws containing similar requirements in one key way: CCPA explicitly states that the "goal" of the risk assessments is "restricting or prohibiting 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."[13] This seemingly addresses one of the major limitations inherent to other state risk assessment frameworks, which contain no legal mechanism to restrict processing activities even when businesses find serious or even unjustifiable harms associated with their processing activities.

We are therefore supportive of Section 7154's clear prohibition on processing activities when the identified risks to consumers' privacy outweigh the benefits. However, in order to fully depart from the weak standard set by other states, CPPA must do more to ensure that it has the formal ability to challenge businesses' assessments of the tradeoffs between the benefits of their processing activities and the harms. Otherwise, businesses will be incentivized to simply downplay the risks of processing in order to avoid the blanket prohibition.

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 a 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.*

Abridged Risk Assessments Should Include the Business' Plain Language Assessments of the Harms and Benefits of Processing

The CPPA contemplates a bifurcated risk assessment structure, where businesses would be required to annually submit to the Agency a streamlined "abridged" risk assessment, while a more fulsome unabridged risk assessment would be available to the Agency upon request.

Under previous versions of the draft rules, businesses were required in their abridged risk assessment to include a "plain-language explanation of why the negative impacts of the

[13] CCPA Section 1798.185(a)(14)(B), https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

processing, as mitigated by safeguards, do or do not outweigh the benefits of the processing."[14] However, that provision has since been removed, and the abridged risk assessment now only includes four simple components: identification of the activity that triggered the risk assessment, a plain language explanation of purpose of the processing, categories of information processed and whether that includes sensitive data, and a plain language explanation of the safeguards a business has implemented to mitigate any harms. Critically, this means that the abridged risk assessment will no longer allow the Agency (or any other stakeholder entitled to access it) to review a business' actual analysis of the tradeoffs between benefits and costs, the central component of the risk assessment, without asking for additional information.

We struggle to see the purpose of requiring an abridged risk assessment with such little information and urge the Agency to restore the aforementioned disclosure.

CPPA Should Require Public Disclosure of Abridged Risk Assessments

We believe it is crucial that the public have access to the risk assessments, so that interested consumers can use this information to weigh their engagement with businesses and that public interest researchers can serve as a secondary check against bad-faith compliance. A business' risk assessment (assuming it includes a plain language assessment of the cost-benefit tradeoffs) could very well be material to a consumer's decision to engage with that business, and therefore there should be a high bar for depriving them of that information. Indeed, the bifurcated structure seemingly lends itself to an approach that would include public consumption of the assessment; while companies, for legible competitive reasons, might be hesitant to publicly share every single element required in the unabridged risk assessment, it is unclear what justification there is for withholding the much more limited abridged risk assessment from the public (and to be clear, we'd continue to believe that is the case even if our above recommendation was adopted). Furthermore, in any case, businesses are already protected from being required to reveal trade secrets by statute.[15]

In addition, because the Agency is unlikely to have the resources necessary to deeply review even the abridged version of each covered business' risk assessments, interested consumers and researchers could play an important role as a force multiplier by relaying important information back to the Agency that it may not have uncovered on its own. Without this extra accountability mechanism, businesses may simply take their chances that the Agency is unlikely to review their risk assessment and potentially provide less than complete information.

We've seen a similar dynamic play out with privacy laws writ-large, where given the lack of private enforcement mechanisms and relatively minimal government enforcement efforts

[14] New Rules Subcommittee Revised Draft Risk Assessment Regulations, (December 2023), Section 7158(b)(2)(E), https://cppa.ca.gov/meetings/materials/20231208_item2_draft_clean.pdf
[15] CCPA Section 1798.185(a)(14)(B), https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

to-date, compliance gaps appear to be widespread well after these laws' effective dates.[16] CPPA should not replicate that mistake here.

Comments on Automated Decisionmaking Technology

We are pleased to see the agency promulgate rules on automated decisionmaking technology (ADMT). These systems have a hidden hand in some of the most important decisions made about consumers using their personal data—and consumers are uncomfortable with it.

In May of 2024, Consumer Reports conducted a nationally representative study of 2,022 U.S. adults focused on the use of AI and algorithms in consequential decisions.[17] When asked how they feel about the use of AI and algorithms in a variety of situations—such as banks using algorithms to make underwriting decisions, landlords using AI to screen potential tenants, hospitals using AI to help make diagnoses—a majority of Americans said they were uncomfortable with each scenario. Researchers also asked consumers to imagine an AI system or algorithm had been used to determine whether or not they would be interviewed for a job they applied for and asked if they would like to know specifically what information about them the program used to make the decision; 83% of Americans said they would want to know. Additionally, researchers asked a question about a similar scenario, and asked if the respondent would want the opportunity to correct incorrect information. An overwhelming 91% of Americans did. These results suggest that the Agency's proposal to provide consumers with explanations, referred to as the "access right," and with a right to correct, are in line with what the vast majority of Americans desire.

Currently, an informational asymmetry prevents Californian consumers from understanding what personal information ADMT draw on, how ADMT use that information to make decisions, and whether ADMT are effective and do not discriminate. With these rules, California will take an important step to rebalance that asymmetry.

However, some changes are needed to ensure these rules protect Californian consumers. These include:

- *Amend the definition of automated decisionmaking technology to meaningfully protect Californians*
- *Require that businesses explain to consumers what happens if they choose to opt-out when presenting them with the right to opt-out*
- *Ensure right of appeal is meaningful by detailing a rigorous appeal process*

---

[16] See, e.g., Data Grail, 2024 Data Privacy Trends Report, (finding that 75 percent of websites do not comply with GPC requests), https://www.datagrail.io/resources/pdfs/privacy-trends-2024/; Privado, The State of Website Privacy, (finding that 76 percent of the most visited websites in the U.S. do not honor CPRA opt-out signals), https://www.privado.ai/state-of-website-privacy-report-2024

[17] Consumer Reports Survey Group, A.I./Algorithmic Decision-making: Consumer Reports Nationally Representative Phone and Internet Survey, (July 9th, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/07/CR-AES-AI-Algorithms-Report-7.25.24.pdf

- *Send post-decision explanations to consumers by default; ensure explanations are sufficiently detailed and put in context*

Amend the definition of automated decisionmaking technology to meaningfully protect Californians

The definition of automated decisionmaking technology raises serious concerns; we fear the agency's move to narrow the definition may cause a considerable problem for compliance.

In the current draft, "automated decisionmaking technology" covers systems that "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." The rules in turn define "substantially facilitate" as "using the output of the technology as a key factor in a human's decisionmaking." The rules further clarify that this includes, for example, "using automated decisionmaking technology to generate a score about a consumer that the human reviewer uses as a primary factor to make a significant decision about them."

If the ADMT could ultimately alter the outcome of a decision, its use should be subject to these rules. Currently, however, if the recommendation or score generated by an ADMT is one of a handful of factors that leads to a decision to hire someone, or deny them a mortgage, or some other high-stakes decision, a company could plausibly argue the ADMT was not a "key" factor, and therefore it need not comply with these regulations. Companies are heavily incentivized to interpret this definition as narrowly as possible, since doing so releases them from many of the requirements in these regulations. Humans within a company may also, in practice, rely on the outputs of ADMT to different degrees; one HR manager may weigh the output of an ADMT against five other factors, while another HR manager at the same company may treat the output of the ADMT as the most important factor.

Research conducted by Cornell, Data & Society, and Consumer Reports has illustrated how minor phrasing issues in similar definitions can lead to low compliance. Researchers looked for markers of compliance with New York City's Local Law 144, which applies to the use of automated employment decision tools, and found extremely low levels of affirmative compliance.[18] The researchers attributed this in part to the fact that "employers can off-ramp from the regulatory decision tree by claiming (correctly or incorrectly) that their decision-making process does not 'substantially' rely upon the outputs of the AEDT."[19]

We recommend the Agency adopt the State Administrative Manual's (SAM) definition of Automated Decision System:[20]

---

[18] Wright, L., Muenster, R. M., Vecchione, B., Qu, T., Cai, P., Smith, A., … & Matias, J. N. (2024). Null Compliance: NYC Local Law 144 and the challenges of algorithm accountability. In The 2024 ACM Conference on Fairness, Accountability, and Transparency.

[19] Ibid, see page 1709

[20] California Department of General Services, State Administrative Manual, Definitions - 4819.2 (last revised March 2024). https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2.

> 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.

Require that businesses explain to consumers what happens if they choose to opt-out when presenting them with the right to opt-out

Currently, the regulations provide consumers with the right to opt-out of ADMT in Section 7221, but do not require businesses to explain to consumers what will happen if they choose to exercise that right. As a practical matter, ambiguity impedes consumers' ability to exercise their right to opt out. For example, if a renter sees they can opt out of automated AI renter screening, but she does not know whether this means the landlord will conduct a human review of her application or whether she will be out of the running entirely, she may be hesitant to exercise her opt-out right. To ensure the opt-out right is meaningful, we propose that the agency requires businesses, when providing the right to opt-out as required by the regulations, to also specify, in plain language, what happens next for consumers who choose to opt-out, what the alternative process is, and to reminding consumers that the law protects them from retaliation for exercising their rights.

We support the regulations exempting businesses from providing an opt-out of ADMT used for significant decisions if they provide an appeal process (the "human appeal exemption") in Section 7221(b)(2). In some cases, such as with credit scores, we do not believe consumers should have the right to opt-out. In other cases, offering a meaningful alternative process to consumers who opt-out seems impractical.

We believe that a right to appeal is a critical addition; there are documented cases of ADMT making errors with high stakes for consumers,[21] and ADMT making inferences about consumers on worryingly thin evidence.[22] Few ADMT are independently and rigorously audited. In light of this, consumers have no reason to be confident that any particular ADMT is drawing accurate conclusions, performs in a reliable manner, and does not discriminate. Therefore, it is critical that consumers receive information about how decisions are made about them, and have recourse to contest the decision, through a right of appeal, when appropriate.

Ensure right of appeal is meaningful by detailing a rigorous appeal process

---

[21] Cyrus Farivar, NBC News, 'Tenant screening software faces national reckoning', March 14, 2021, https://www.nbcnews.com/tech/tech-news/tenant-screening-software-faces-national-reckoning-n1260975

[22] Drew Harwell, Washington Post, 'Wanted: The 'perfect babysitter.' Must pass AI scan for respect and attitude,' November 23rd, 2018, https://www.washingtonpost.com/technology/2018/11/16/wanted-perfect-babysitter-must-pass-ai-scan-respect-attitude/

We believe the right to appeal can be a useful backstop for consumers when companies use flawed, unfair, or discriminatory ADMT to make decisions about them. Unfortunately, companies may put pressure on individuals reviewing appeals to move as quickly as possible, or overturn as few decisions as possible. When telling consumers they have upheld their original decision, companies may use vague language that does not make clear why new information provided by the consumer was insufficient to overturn the decision. Another factor working against meaningful, rigorous appeal review processes is the fact that humans tend to view automated systems as authoritative and trustworthy.[23]

To counter these human impulses and corporate incentives, the appeals process must require careful consideration. We recommend the Agency adopt the change suggested in a January 9 joint comment letter authored by 56 organizations and individuals,[24] including unions, privacy rights organizations, and public policy experts who recommend that Section 7221(b)(2) be revised as follows:

(2) For any significant decision concerning a consumer as set forth in Section 7200, subsection (a)(1), if the business provides the consumer with a method to appeal the decision to a qualified human reviewer who is required to objectively evaluate all relevant evidence and has the authority to overturn the decision ("human appeal exception"). To qualify for the human appeal exception, the business must do the following:

(A) The business must designate a human reviewer who:

(i) Is trained and qualified to understand the significant decision being appealed, ~~and~~ the consequences of the decision for the consumer, how to evaluate the decision, and how to serve impartially, including by avoiding prejudgment of the facts at issue, conflict of interest, and bias;

(ii) Does not have a conflict of interest or bias for or against the business or the consumer generally, or against the business or consumer specifically;

(iii) Was not involved in the initial decision being appealed;

(iv) Must enjoy protection from dismissal or its equivalent, disciplinary measures, or other adverse treatment for exercising their functions under this section; and

(v) Must be allocated sufficient human resources by the business to conduct an effective appeal of the decision.

(B) This human reviewer must consider the relevant information provided by the consumer in their appeal and may consider any other sources of information about the significant decision.

(C) The business must clearly describe to the consumer how to submit an appeal and enable the consumer to submit corrections or otherwise provide information.

---

[23] See, e.g., Danielle Keats Citron, Washington University Law Review, 'Technological Due Process,' 2008 supra note 3, at 1271–72; https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview

[24] 'Joint Comment Letter on Proposed Regulations for the California Consumer Privacy Act (CCPA)', Janruary 9, 2025, accessed at https://laborcenter.berkeley.edu/joint-letter-to-the-california-privacy-protection-agency-on-proposed-regulations/

evidence, and a written statement in support of or challenging the outcome, for the human reviewer to consider as part of the appeal.

(i) The method of the appeal must also be easy for the consumers to execute, require minimal steps, and comply with sections 7004 and 7020.

(ii) The business must permit the consumer to be represented by an authorized agent or advisor of their choice, who may be, but is not required to be an attorney.

(iii) In responding to the appeal, the business must provide the consumer with a sufficiently precise and adequately substantiated reply in the form of a written document, describing the result and explaining the reasons for its decision, which may be in electronic format.

(iv) In the event that the significant decision in paragraph (b)(2) of this section is found by the human reviewer to have infringed on the rights of the consumer, the business shall rectify that decision without delay and in any case within fourteen calendar days of the finding by the human reviewer. The business shall also take the necessary steps in order to avoid such decisions in the future, including, if appropriate, a modification of the ADMT or a discontinuance of its use.

Send post-decision explanations to consumers by default; ensure explanations are sufficiently detailed and put in context

The pre-use notice paired with a post-decision explanation ("right to access") are two of the most critical provisions of Article 11. The additional information consumers will receive as a result of these provisions will help consumers understand how their personal data is being used to make decisions that impact their lives, exercise their right to appeal if necessary, and in some cases, may enable them to exercise rights under existing laws, such as civil rights laws, consumer protection laws, and labor laws. For these disclosures to live up to their promise, they must be easy for consumers to access, detailed, and easy for them to understand.

Currently, in order for a consumer to receive information about how an adverse significant decision was made about them, the regulations require consumers to take a proactive step to exercise their right to "access." Many consumers will not take this step even when doing so may benefit them; they may not see the additional notice required under 7222(k); consumers may not understand the potential upside of receiving the information provided by their access right, and therefore may not choose to spend time requesting it. We recommend that instead of requiring consumers to take a proactive step when an adverse decision is made about them, businesses should instead be required to provide the information to consumers by default via their typical means of communicating with consumers.

Additionally, post-decision explanations must be detailed and put in relevant context in order to be useful to consumers. In addition to Section 7222's requirements under (b)(4), businesses should also be required to disclose what personal information was most relevant to the key factors articulated in Section 7222 (b)(4)(B), what the sources of that personal information were, and how that personal information interacted with the key factors.

Context is also important. Section 7222 (b)(2) requires businesses to disclose “the output of the automated decisionmaking technology with respect to the consumer.” A business could comply with this requirement by disclosing that an ADMT’s output for a given consumer is a risk score of three. That information will be meaningless to the consumer if she does not know if the ADMT’s scale is zero to five, or zero to one hundred. Therefore, businesses should be required to provide information specified under Section 7222 (b)(4)(C) (“A business also may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers”).

In order to increase the likelihood that the post-decision explanations businesses generate are both plain language and sufficiently detailed, we recommend the Agency provide an appendix with examples of hypothetical explanations that meet the Agency’s expectations.

****

We thank the California Privacy Protection Agency for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Justin Brookman (justin.brookman@consumer.org) for more information.