Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments On
Proposed Rulemaking for Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking

By

Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

March 27, 2023

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

We describe our views on each of the potential areas for rulemaking in the course of providing answers to the questions posed by the CPPA in its invitation.

I. Cybersecurity Audits

1. What laws that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require cybersecurity audits? For the laws identified:

a. To what degree are these laws' cybersecurity audit requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(A)?
b. What processes have businesses or organizations implemented to comply with these laws that could also assist with their compliance with CCPA's cybersecurity audit requirements?
c. What gaps or weaknesses exist in these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?
d. What gaps or weaknesses exist in businesses' compliance processes with these laws for cybersecurity audits? What is the impact of these gaps or weaknesses on consumers?
e. Would you recommend that the Agency consider the cybersecurity audit models created by these laws when drafting its regulations? Why, or why not?

Though cybersecurity audits are admittedly far from Consumer Reports' top priority in privacy law, we do believe they have a role to play and that fulsome outside evaluation of businesses' cybersecurity risk is likely to benefit consumers. In order to pass audits, businesses will be motivated to invest more resources into safeguards to protect personal data from unauthorized access that could result in a host of secondary harms that extend beyond the original collection, including, physical, reputational, psychological, discriminatory, and economic harms. Basic cybersecurity hygiene calls for consumer friendly behaviors such as encrypting data, reducing employee access, and simply minimizing the amount of consumer data the business collects and retains to begin with.

[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.

Extant state law focusing *specifically* on cybersecurity is minimal compared to state data security law, where at least 25 states have passed measures that address the data security practices of private entities.[2] The handful of state laws that specifically address cybersecurity, such as those in Massachusetts, New York, and Oregon, typically require businesses to "assess" the safeguards they have implemented to mitigate cyber risks, rather than accede to a formal audit.[3] Similarly, state data security laws typically require that businesses adopt "reasonable" safeguards, but do not require businesses to submit to formal third-party audits. Since many existing state data security and cybersecurity laws only require businesses to *internally* assess their relevant safeguards, whereas CPRA clearly contemplates independent audits (which, in our view, means those conducted by a dispassionate third-party), CPRA seems to raise the bar above existing law.

Other strong state cybersecurity provisions include those instituted by the New York Department of Financial Services (NYDFS), which recently adopted new requirements for financial institutions, including annual penetration testing and bi-annual vulnerability assessments, limits on access privileges, and a requirement to designate a chief information security officer who is responsible for the company's security program.[4]

On the federal level, the FTC recently updated its Safeguards Rule with more specific security requirements, consistent with the NYDFS regulation, including placing limits on internal access to data, new encryption requirements, and a requirement to establish a chief security officer. The new rules also require covered businesses to conduct an assessment (internal *and* external) to determine foreseeable risks and threats to the security, confidentiality, and integrity of customer information.[5] Separately, the FTC has interpreted its Section 5 authority to mandate that companies take reasonable security measures to protect consumer information – though it is unclear when that may require auditing.[6] The Health Information Technology for Economic and Clinical Health Act also requires that the U.S. Department of Health and Human Services, through its Office of Civil Rights (OCR), periodically audit covered entities and business associates for their compliance with the Health Insurance Portability and Accountability Act privacy, security, and breach notification rules.[7]

---

[2] Data Security Laws | Private Sector, National Council of State Legislatures, (May 29. 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.
[3] See, e.g., Code of Massachusetts Regulations 201 Section 17.03 2(b), https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download
[4] 23 CRR-NY § 500.0 et seq., https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
[5] Federal Trade Commission, FTC Safeguards Rule: What Your Business Needs to Know, (May 2022) https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
[6] Federal Trade Commission, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers, (October 31, 2022) https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions
[7] Office of Civil Rights, HIPAA Privacy, Security, and Breach Notification Audit Programm, (December 17, 2020), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

Unfortunately, the lack of regulatory bandwidth to intervene when businesses fail to remedy shortcomings identified by self-assessments and audits often hampers their effectiveness as accountability mechanisms. According to its last available fiscal year report, OCR audited around 150 businesses.[8] OCR employs around 200 full time employees. Scaling down to an agency of CPPA's size, even assuming massive efficiency gains from the CPPA outsourcing audit responsibilities to third parties, it is clear that CPPA will not be able to review cybersecurity audits on a mass scale.

Absent the expectation of robust oversight, businesses are less likely to invest the resources necessary to protect consumer information above levels that the market may bear, which, for a variety of reasons – including many industries operating in non-competitive markets, can be an exceedingly low bar. The consistent drumbeat of news articles describing the increase in successful cyberattacks on companies of all sizes seems to bear this out.[9]

Consistent underfunding of key regulators has left them under-equipped to keep pace and police the market. Consumer Reports has consistently called for legislators to raise funding levels for key regulators; until more appropriate funding levels are reached, underenforcement of all business requirements, but especially laborious ones like cyber audits, will continue to be endemic.[10]

II. Risk-Assessments

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments? For the laws or other requirements identified:

a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?

Following the passage of the General Data Protection Regulation (GDPR) in the European Union, data protection risk-assessments have emerged as a consistent presence in comprehensive state privacy laws and proposals in the United States. Of the four other comprehensive state privacy laws, three, Virginia (VCDPA), Connecticut (CTDPA), and Colorado (CPA), include a requirement for covered entities to conduct data protection assessments regarding processing activities that pose a "heightened risk of harm" or other specific risks to consumers. Drawing from the text of GDPR, each of the risk-assessments requires that businesses weigh the benefits of processing to all relevant stakeholders against

---

[8] Office of Civil Rights, Health Information Privacy Division, 2016-2017 HIPAA Audits Industry Report (December 2020), https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf

[9] E.g., Joy LePree Anderson, Global Cyberattacks Increased 38 percent in 2022, Security Magazine, (January 20, 2023), https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

[10] Consumer Reports, Group Letter in Support of FTC Privacy Funding, (September 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf

the potential risks to the rights of the consumer associated with such processing. Through its rulemaking process, Colorado has gone furthest to outline the discrete elements and process required to complete a risk assessment.

Though the aforementioned requirements largely align with those articulated in CPRA, it is not a one-to-one match. Firstly, the risk assessment requirement under CPRA applies to businesses whose processing presents "significant risk to consumers' privacy or security," rather than a "heightened risk" as in the other laws.[11] The term "significant risk" is undefined in CPRA. CPRA also requires that businesses identify when their processing involves sensitive personal information, whereas that requirement lives elsewhere in the other state laws (though Colorado did include this in their regulations).[12] Finally CPRA attaches a normative goal to its risk-assessment requirement, which 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."

b. What processes have businesses or organizations implemented to comply with these laws, other requirements, or best practices that could also assist with compliance with CCPA's risk-assessments requirements (e.g., product reviews)?

Businesses with operations in Europe should be familiar with the broad framework and goals of a data protection risk-assessment through their compliance with GDPR. Risk assessments may be a newer undertaking for smaller U.S. based businesses, especially those that do not operate in other states with comprehensive privacy laws.

c. What gaps or weaknesses exist in these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?

One major weakness in the existing risk-assessment framework as set out in Virginia, Connecticut, and Colorado is that the assessment must only be produced if the controller is being investigated by a supervisory authority.[13] In fact, each of the laws completely exempts risk assessments from public inspection. Unless a company's behavior is suspicious enough to warrant an Attorney General investigation, nobody outside of the business will ever see the risk assessment.

Another weakness stems from the assumption that by forcing controllers to confront the risks inherent to their data processing activities, they will automatically change their behavior. The reality is that even when tech companies fully recognize the harms their services cause, they often do not act to countervail them; Frances Haugen's revelations regarding Facebook's lack of action in the face of multiple known harms created by the platform provide the most high-profile

---

[11] Civil Code § 1798.185(a)(15)(B)
[12] Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 8.04 A(2), (March 2023), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf
[13] Code of Virginia, Consumer Data Protection Act, Section 59.1-580(C), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

example.[14] The more intertwined a business' revenue model is with the harms they produce, as in the case of the surveillance advertising model, the less likely risk assessments are to change behavior voluntarily. If the goal of improving consumer outcomes through risk assessments is even achievable, stronger accountability mechanisms are required.

CPRA's risk assessment does differ somewhat from other states, since it explicitly states that the goal is "restricting or prohibiting" processing if the risks outweigh the benefits. However, without strict enforcement, businesses are likely to simply downplay the risks in order to avoid any affirmative requirement to change. At the very least, CPPA should require that businesses provide risk assessments to the agency on an ongoing basis – rather than only when the business is being investigated – so that they may review for systemic underreporting or other obvious noncompliance. In any case, proving a business outright lied on its risk assessment will likely be a difficult endeavor.

At the same time, we recognize that state Attorneys General or even dedicated supervisory authorities like the CPPA do not possess the resources to closely and continually monitor risk assessments. For this reason, we believe it is crucial that the public also be able to review risk assessments (with tightly scoped exemptions around revealing business trade secrets), so that interested consumers can use this information to weigh their engagement with businesses. Public inspection of risk assessments will also deputize the public by allowing it to relay important information back to the agency that it may not have uncovered on its own. While few people will likely read risk assessments and the business will still be incentivized to emphasize the public benefits of its processing and minimize the risks, more documentation is probably better than nothing at all. CPPA's forthcoming regulations should also require that businesses share any internal documentation they possess on the concrete harms caused by the service to avoid large-scale coverups like at Facebook.

Similar to cybersecurity audits, it all comes down to enforcement. If businesses fear the consequences of not being forthcoming, risk assessments could produce additional information that improves regulators' and the public's understanding of the processing harms caused by businesses. If left to their own devices, businesses will likely produce anodyne documents that serve few and the process will simply become a "check the box" exercise.

d. What gaps or weaknesses exist in businesses' or organizations' compliance processes with these laws, other requirements, or best practices for risk assessments? What is the impact of these gaps or weaknesses on consumers?

As previously mentioned, comprehensive state privacy laws that require risk assessments do not *allow* them to be publicly available, let alone require it. GDPR also does not mandate public disclosure. As such, our understanding of business' compliance processes with existing risk assessment frameworks is minimal.

---

[14] Wall Street Journal, The Facebook Files, (October 1, 2021), https://www.wsj.com/articles/the-facebook-files-11631713039

In the rare instances that businesses do make risk assessments publicly available, evidence of their efficacy is sketchy, if inconclusive. For example, Google recently reduced the results of its voluntary civil rights audit, which was roundly criticized by civil rights advocates for being performative and light on details.[15]

e. Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?

See above (*supra* Section 2, Question 1(c)) for our view on how existing models can be improved.

2. What harms, if any, are particular individuals or communities likely to experience from a business's processing of personal information? What processing of personal information is likely to be harmful to these individuals or communities, and why?

It is first important to note that unwanted observation, through excessive data collection and use, is harmful in and of itself. Intrusion upon seclusion has long been recognized as a privacy tort, and consumers will always have a legitimate interest in constraining unnecessary processing of their data. That applies both on the individual level, as well as collectively.

Consumers have no shortage of reasons to object to the collection and retention of their personal information per se even if a company has no immediate plans to do anything with that data. Some of those reasons include:[16]

- **Data breach**: The data could be breached and accessed by outside attackers, or inadvertently exposed to the world.
- **Internal misuse**: Bad actors within the company could access and misuse the data for their own purposes.[17]
- **Loss of economic power and future unwanted secondary use**: Even if the company today has no present plans to use the data, the company could change its mind in the future (privacy policies often reserve broad rights to use personal information for any number of reasons). Such usage could range from the merely annoying (say, retargeted advertising) to price discrimination to selling the information to data brokers who could then use the information to deny consumers credit or employment. Differential pricing is

[15] Cristiano Lima, Google's civil rights audit lacked teeth, advocates say, Washington Post (March 10, 2023), https://www.washingtonpost.com/politics/2023/03/10/googles-civil-rights-audit-lacked-teeth-advocates-say/

[16] These categories are derived from a paper for the Future of Privacy Forum and the Stanford Center for Internet & Society's "Big Data and Privacy: Making Ends Meet" workshop. For further elaboration on these categories, see Justin Brookman and G.S. Hans, Why Collection Matters: Surveillance as a De Facto Privacy Harm, (Sep. 30, 2013), https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.pdf

[17] Adrian Chen, GCreep: Google Engineer Stalked Teens, Spied on Chats, Gawker (Sep. 14, 2010) http://gawker.com/5637234/gcreep-googleengineer-stalked-teens-spied-on-chats

a special concern, as companies with more data about an individual will have a better sense of how much that person is willing to pay for a particular product. This in turn will empower the company to set personal prices closest to that equilibrium point, allowing the company to take relatively more of the consumer surplus from any transaction. This type of first-degree price discrimination is all the more of a concern to consumers as increasing corporate concentration means that consumers have fewer market alternatives.

- **Government access**: Consumers may be legitimately concerned about illegitimate government access to their personal information. TikTok, for example, has been dogged by fears of Chinese government access[18] — fears that appear to be justified.[19] Moreover, in the wake of the Dobbs Supreme Court decision, many Americans worry that fertility and health information generated and stored by tech companies may be accessed by states that criminalize abortion access.[20]
- **Chilling effect**: Finally, all these concerns together —along with others, and even with an irrational or inchoately realized dislike of being observed — has a chilling effect on public participation and free expression. People will feel constrained from experimenting with new ideas or adopting controversial positions. In fact, this constant threat of surveillance was the fundamental conceit behind the development of the Panopticon prison: if inmates had to worry all the time that they were being observed, they would be less likely to engage in problematic behaviors.[21] The United States was founded on a tradition of anonymous speech. In order to remain a vibrant and innovative society, citizens need room for the expression of controversial — and occasionally wrong — ideas without worry that the ideas will be attributable to them in perpetuity. In a world where increasingly every action is monitored, stored, and analyzed, people have a substantial interest in finding some way to preserve a zone of personal privacy that cannot be observed by others.

With that said, there are also many, many examples of *discrete* commercial surveillance and processing practices negatively impacting individuals and disproportionately harming vulnerable populations and communities historically subjected to discrimination. For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.[22] These targeting systems have also been used to interfere with elections and fuel voter suppression efforts and to carry

---

[18] Jack Sommers, Nearly half of Americans fear TikTok would give their data to the Chinese government, Business Insider, (Jul. 15, 2021), https://www.businessinsider.com/nearly-half-of-americans-fear-tiktok-would-give-china-data-2021-7

[19] Christianna Silva and Elizabeth de Luna, It looks like China does have access to U.S. TikTok user data, Mashable, (Nov. 3, 2022), https://mashable.com/article/tiktok-china-access-data-in-us.

[20] Naomi Nix and Elizabeth Dwoskin, Search warrants for abortion data leave tech companies few options, Washington Post, (Aug. 12, 2022), https://www.washingtonpost.com/technology/2022/08/12/nebraska-abortion-case-facebook/.

[21] Michel Foucault, Discipline and Punish: The Birth of the Prison (1977).

[22] Sec'y of Hous. & Urban Dev. v. Facebook, Inc., No 01-18-0323-8, 1, Charge of Discrimination, FHEO No. 01- 18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

out disinformation campaigns that undermine public trust.[23] Further, some data brokers provide this information to employers, landlords, and others, while evading the Fair Credit Reporting Act, giving consumers next to no control over these uses.[24] The increasing use of automated decision-making can further exacerbate these problems, as opaque algorithms, often trained on historical data, can perpetuate existing inequalities.[25]

In one recent example, Consumer Reports uncovered evidence that auto insurers were engaging in algorithmically-driven discriminatory pricing schemes based on educational attainment and employment data they had collected from consumers.[26] These factors disproportionately penalize drivers of color and working-class people, often costing them hundreds of dollars per year.

Consumer Reports has also written about the use of race as a variable in medical algorithms, which can determine eligibility for critical services, such as risky treatments or organ transplants.[27] One paper found that Black patients were assigned lower-risk scores than white patients, even when they were equally sick; the algorithm used data about patients' historical healthcare costs to make decisions, and Black patients were routinely spent less on, which the scientists speculated is due to systemic barriers to healthcare access.[28] While many hospitals have dropped race as a consideration in medical algorithms, citing a lack of evidence, many still use them, often without the patient knowing their race was a consideration in the clinical decisionmaking process.[29]

---

[23] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Fed. Trade Comm'n (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billionpenalty-sweeping-new-privacy-restrictions.

[24] Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA, Fed. Trade Comm'n (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-chargescompany-allegedly-marketed; Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 26 (Mar. 2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf

[25] See Erin Simpson & Adam Conner, How to Regulate Tech: A Technology Policy Framework for Online Services, Ctr. for Am. Progress (Nov. 16, 2021) (discussing the extensive literature on civil rights harms caused by automated decision-making systems, biometric surveillance, amplification of civil-rights suppressing content, and reification of prejudice), https://www.americanprogress.org/article/how-toregulate-tech-a-technology-policy-framework-for-online-services/.

[26] Chuck Bell, CR investigates how auto insurers are using drivers' education and occupation to set premiums, (January 28, 2021) https://advocacy.consumerreports.org/research/report-effects-of-varying-education-level-and-job-status-on-online-auto-insurance-price-quotes/

[27]Kaveh Waddell, Medical Algorithms Have a Race Problem, Consumer Reports, (September 18, 2020), https://www.consumerreports.org/medical-tests/medical-algorithms-have-a-race-problem/

[28] Heidi Ledford, "Millions Affected by Racial Bias in Health-Care Algorithm," Nature 574 (October 31, 2019): 608-609, https://media.nature.com/original/magazine-assets/d41586-019-03228-6/d41586-019-03228-6.pdf.

[29]Kaveh Waddell, Medical Algorithms Have a Race Problem, Consumer Reports, (September 18, 2020), https://www.consumerreports.org/medical-tests/medical-algorithms-have-a-race-problem/

In the employment context, some AI companies are developing algorithms that are intended to help human resources departments narrow down job applicants or monitor/encourage productivity in the workplace. Companies like HireVue have been criticized for incorporating facial and other analysis into their video interviewing software which monitors the applicant's expressions, their tone of voice, perceived traits like "enthusiasm," eye contact, and their word choice. After much pushback from civil rights groups including an official complaint to the FTC from the Electronic Privacy Information Center, the company discontinued their facial analysis component of their software. HireVue is not the only company using biometrics to assess job applicants; other companies like Interviewer.AI and MyInterview assess candidates' faces, body language, and/or voices and rank candidates perceived characteristics like "sociability," "humility," and "positive attitude." Consumers typically have little ability to revoke consent for such uses.

3. To determine what processing of personal information presents significant risk to consumers' privacy or security under Civil Code § 1798.185(a)(15):

a. What would the benefits and drawbacks be of the Agency following the approach outlined in the European Data Protection Board's Guidelines on Data Protection Impact Assessment?

It is unclear whether there is a truly meaningful distinction between risky and non-risky processing activities. While some activities might be risky no matter the context (facial recognition or automated decisionmaking with legal or similarly significant effects), almost any processing activity poses some degree of inherent risk. Even the most basic activity, such as collecting and processing a consumer's information to consummate a purchase, can entail high-risk depending on the category of item or contextual personal factors of the purchaser.

Plenty of so-called "non-sensitive" personal information, when combined in certain ways, can become sensitive, and companies can often use their vast stores of non-sensitive data to infer sensitive attributes about a person. The Federal Trade Commission has, for example, identified categories such as geolocation[30] and TV viewing[31] as "sensitive" and worthy of greater protection; however, other common categories of data collection — such as web browsing and shopping — can in many cases be at least as if not more revealing about personal behavior.

The boundaries of "risky" behavior are also highly dependent on the person and context, which brings to the fore important equity and civil rights considerations. Individuals with certain lived experiences may not want information about their lives revealed, whereas that same information may be entirely unobjectionable to another person. As such, there are immense challenges in scoping the definitions of risk and sensitive information. A common outcome, at least in the case

[30] FTC v Kochava, Inc., Complaint for Permanent Injunction and Other Relief, (August 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf
[31] FTC v Vizio and Vizio Inscape, Complaint for Permanent Injunction and Other Equitable and Monetary Relief, (February 2017) https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf

of state privacy laws and proposals, is that the sensitive data category (if such a category exists) is under-inclusive.[32]

For that reason, we support a broad definition of risky behavior, which is largely reflected in the European Data Protection Board's (EDPB) approach. The EDPB lists nine categories of processing activity that would meet its definition:

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organizational solutions
- Prevents data subjects from exercising a right or using a service or a contract

In addition to the factors included in the EDPB's analysis, we would add several criteria present in the Colorado Privacy Act rules, including information processed for the purposes of targeting advertising (insofar as that is not already covered by other factors), selling of personal information, and physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person.[33]

b. What other models or factors should the Agency consider? Why? How?
c. Should the models or factors be different, or assessed differently, for determining when processing requires a risk assessment versus a cybersecurity audit? Why, or why not? If so, how?

We do not believe there is a strong reason to differentiate the factors for determining when processing requires a risk assessment versus a cybersecurity audit.

d. What processing, if any, does not present significant risk to consumers' privacy or security? Why?

See above (*supra,* Section 2, Question 3(a)).

4. What minimum content should be required in businesses' risk assessments? In addition:

---

[32] For example, in relation to health information, Virginia's Consumer Data Protection Act only includes "mental or physical health diagnosis" in its definition of sensitive personal information, leaving reproductive health information uncovered. Code of Virginia, Chapter 53, § 59.1-575, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

[33] Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 8.04 (6), (March 2023), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf

a. What would the benefits and drawbacks be if the Agency considered the data protection impact assessment content requirements under GDPR and the Colorado Privacy Act?

See above (*supra* Section 2, Questions 1(c) and 3(a))

b. What, if any, additional content should be included in risk assessments for processing that involves automated decisionmaking, including profiling? Why?

Consumer Reports believes that in the case of automated decisionmaking, especially when those decisions involve legal or similarly significant effect, businesses should provide additional transparency, including an evaluation of how the algorithm works under various conditions and in what circumstances the model is intended to be used.

However, we do not believe that internal risk assessments should be the primary mechanisms to hold businesses accountable for their use of automated decisionmaking systems. Instead we recommend that algorithms that may have significant legal effects undergo third party audits before deployment, and regularly after deployment; we also recommend that these auditors are required to undergo an accreditation process to evaluate algorithms that can have significant legal effects. In order for these audits to be effective, companies should be required to disclose specific data to the auditors, such as training data used to develop the model, a standardized API to easily test the system, or even the code itself, depending on the case. We also recommend that specific issues be investigated by auditors such as discrimination against protected classes, etc. Finally, the results of the audit should be made public if the algorithm has already been deployed to the public. If not, the company must address the results of the audit in a timely manner, and before deployment.

5. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments? How would businesses demonstrate to the Agency that these assessments comply with CCPA's requirements?

See above (*supra* Section 2, Question 1(c)) for our view on the weaknesses of existing risk assessment models.

6. In what format should businesses submit risk assessments to the Agency? In particular:

a. If businesses were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business):

i. What should these summaries include?
ii. In what format should they be submitted?
iii. How often should they be submitted?

b. How would businesses demonstrate to the Agency that their summaries are complete and accurate reflections of their compliance with CCPA's risk assessment requirements (e.g., summaries signed under penalty of perjury)?
7. Should the compliance requirements for risk assessments or cybersecurity audits be different for businesses that have less than $25 million in annual gross revenues? If so, why, and how?
8. What else should the Agency consider in drafting its regulations for risk assessments?

It is worth keeping in mind that the primary motivation behind privacy law is to combat the excesses of big internet companies and a small number of niche companies whose primary business is trafficking in personal data. We do not necessarily want to subject smaller companies with far less sophisticated processing capabilities to the same requirements as the largest tech companies. That said, businesses that engage in certain types of behaviors, such as applying novel technologies, processing data of vulnerable individuals, engaging in systematic monitoring of individuals or deploying automated decisionmaking tools that produce legal or significantly similar effects should have to complete risk assessments no matter their size.

III. Automated Decisionmaking

The CCPA directs the Agency to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer." In determining the necessary scope of such regulations, the Agency is interested in learning more about existing state, federal, and international laws, other requirements, frameworks, and/or best practices applicable to some or all CCPA-covered businesses or organizations that presently utilize any form of automated decisionmaking technology in relation to consumers, as well as businesses' compliance processes with these laws, requirements, frameworks, and/or best practices. In addition, the Agency is interested in learning more about businesses' uses of and consumers' experiences with these technologies, including the prevalence of algorithmic discrimination. Lastly, the Agency is interested in the public's recommendations regarding whether access and opt-out rights should differ based on various factors, and how to ensure that access requests provide meaningful information about the logic involved in automated decisionmaking processes as well as a description of the likely outcome of the process with respect to the consumer. Accordingly, the Agency asks:

1. What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

A right to opt-out of automated decisionmaking is expressed in Article 22 of GDPR, which states that data subjects "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or

similarly significantly affects him or her."[34] Recent state privacy laws in Virginia, Connecticut, and Colorado have followed suit by allowing consumers to opt out of "profiling" in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.

In the financial sector, both the Equal Credit Opportunity Act (ECOA) and Fair Credit Reporting Act (FCRA) provide something resembling access and explainability rights.[35] When a consumer is denied credit, under ECOA creditors must provide consumers with the main reasons for that denial. The CFPB recently clarified that creditors that use complex algorithms or artificial intelligence to help generate credit decisions must still "provide a notice that discloses the specific, principal reasons for taking adverse actions."[36] Meanwhile, FCRA requires that when an adverse action, such as the denial of credit, is based on a credit score, the creditor must disclose the key factors that affected the score, among other information.

2. What other requirements, frameworks, and/or best practices that address access and/or opt out rights in the context of automated decisionmaking are being implemented or used by businesses or organizations (individually or as members of specific sectors)?

Some businesses that operate in Europe may also apply opt-out rights to consumers in the United States, but this practice is not widespread, to our knowledge. We are unaware of any self-regulatory frameworks to provide rights to access or explainability when it comes to automated decisionmaking.

3. With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:

a. How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?

The term "automated decisionmaking" is not defined in GDPR, VCDPA, CPA, or CTDPA. Instead, each of those laws defines a related concept, "profiling", which is automated processing to evaluate certain aspects of a person's life. Each of those laws allows consumers to opt out of profiling. Of course, while some automated decisionmaking may involve profiling, profiling does not always constitute automated decisionmaking.

In the CPA rules, the Attorney General defines the terms "Human Involved Automated Processing", "Human Reviewed Automated Processing", and "solely automated processing" to

---

[34] General Data Protection Regulation, Article 22 (1), https://gdpr-info.eu/art-22-gdpr/
[35] Patrice Alexander Ficklin, Tom Pahl, and Paul Watkins, Innovation spotlight: Providing adverse action notices when using AI/ML models, Consumer Financial Protection Bureau, (July 7, 2020), https://www.consumerfinance.gov/about-us/blog/innovation-spotlight-providing-adverse-action-notices-when-using-ai-ml-models/
[36] Consumer Financial Protection Bureau, CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms (May 26, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/

differentiate between different circumstances in which the right to opt out of profiling should apply.[37] This conception appears to have been drawn from the GDPR, which only grants opt-out rights when legal or similarly significant decisions are "solely" automated.

Though the CPA and GDPR relieve controllers of their opt out responsibilities when a human is involved with an automated process, we question at what level humans can be meaningfully involved in the outcome of more complicated algorithmic processes. In other words, the weight we should apply to human involvement is highly dependent on context. A growing corpus of scholarship has found that humans, even those technically empowered to intervene in automated processes, often cannot do so effectively.[38] This can occur for a multitude of reasons, but perhaps most vexingly of all is the "black box" problem, where a human may indeed consider the data used in the processing and have the authority to change a result once the processing occurs, but simply possesses no understanding of how the automated process arrived at the conclusion that it did. This problem plagues even the most technically-attuned humans in the loop, including engineers of the systems themselves, and will only worsen as automated processes become more sophisticated.[39]

In deference to the growing complexity of algorithmic systems, we urge CPPA to define automated decisionmaking broadly and apply opt out rights even when a human is technically "in the loop."

b. To what degree are these laws, other requirements, frameworks, or best practices aligned with the requirements, processes, and goals articulated in Civil Code § 1798.185(a)(16)?

CPRA's conception of automated decisionmaking shares much with GDPR and diverges somewhat from other state privacy laws. Like GDPR, CPRA clearly paves the path for both a right to opt out of automated decisionmaking, as well as access rights that "include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the consumer." VCDPA and CTDPA do not include similar requirements that businesses share information about the logic of the algorithm or its likely outcomes.

Though the text of CPA unfolds in much the same way as the other two state laws, the recently finalized CPA rules do require businesses that profile consumers to provide in their privacy

---

[37] Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 2.02, (March 2023), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf

[38] See, e.g., Brennan-Marquez, Kiel and Susser, Daniel and Levy, Karen, Strange Loops: Apparent versus Actual Human Involvement in Automated Decision-Making (October 2, 2019). 34 Berkeley Technology Law Journal 745–771 (2019), https://ssrn.com/abstract=3462901

[39] Will Knight, The Dark Secret at the Heart of AI, MIT Technology Review, (April 11, 2017), https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/

policy "[a] non-technical, plain language explanation of the logic used in the Profiling process."[40] The CPA rules also clarify that a business must disclose, "[t]he benefits and potential consequences of the decision based on the Profiling," which bears a resemblance to CPRA's "likely outcomes" provision.[41]

Moreover, under the CPA rules, businesses that profile consumers must include in their data protection assessments "[a]n explanation of the training data and logic used to create the Profiling system, including any statistics used in the analysis, either created by the Controller or provided by a Third Party which created the applicable Profiling system or software."[42]

c. What processes have businesses or organizations implemented to comply with these laws, other requirements, frameworks, and/or best practices that could also assist with compliance with CCPA's automated decisionmaking technology requirements?
d. What gaps or weaknesses exist in these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on consumers?

As a bare minimum, Consumer Reports believes automated decisions with legal or similarly significant effects should be explainable, and thus the Virginia and Connecticut laws appear to be weaker (barring future re-interpretation) than GDPR and CPA.

One weakness of all the state automated decisionmaking provisions compared to the GDPR is that those laws lack the right of contestation outlined in Article 22 of the GDPR. The right to contest substantially strengthens the right to an explanation; under such a regime, consumers can (theoretically, at least) use the information they have gleaned from a business' explanation to provide countervailing documentation to contest and, perhaps, overturn an unjust decision.

At the same time, GDPR's right to contest is only cursorily described in the text, which has given rise to questions about the feasibility of producing explanations detailed enough to render such a right to contest meaningful, especially in the case of complex machine learning algorithms.[43] Moreover, several years on from the implementation of GDPR, we still do not have a clear procedural understanding of what the right to contest looks like in practice.[44] Additionally, as with the right to explanation, the right to contest only exists when legal or similarly significant decisions are solely automated. In light of these limitations, some scholars have rejected the right to contest, and instead advocated for a "right to a well-calibrated machine" – in other

---

[40] Colorado Department of Law, Consumer Protection Section, Colorado Privacy Act Rules 4 CCR 904-3, Section 9.03, (March 2023), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf
[41] Ibid., Section 9.03 (A)(6)
[42] Ibid., Section 9.06(F)(5)
[43] Margot Kaminski and Jennifer Urban, The Right to Contest AI, Columbia Law Review, Vol. 121, No. 7, 2021, (November 16, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3965041
[44] Ibid.

words, the right to unbiased and accurate automated decisionmaking systems.[45] In any case, we urge the CPPA to think broadly about what access rights may entail, including whether a right to contest may be appropriate and statutorily defensible.

e. What gaps or weaknesses exist in businesses or organizations' compliance processes with these laws, other requirements, frameworks, and/or best practices for automated decisionmaking? What is the impact of these gaps or weaknesses on Consumers?

See above (*supra* Section 3, Question 3(d)) – relative to the right to contest in GDPR, it is arguable that the law does not provide a clear road map to compliance. Relative to the right to explainability, it is unclear whether existing law and enforcement has incentivized businesses to create the framework for meaningful explainability relative to more complex automated decisionmaking processes.

On top of access and opt out rights, Consumer Reports has previously advocated for algorithms to be auditable.[46] While explainability mandates may get us part of the way there, independent, and standardized third-party audits for companies whose algorithms pose significant legal effects are likely a more direct way of improving our understanding of algorithmic processes.

In addition to laws that require companies using AI to undergo independent, rigorous third-party audits, public interest researchers can play a vital role in uncovering the harms caused by algorithmic decision-making. We've advocated for several policy solutions to make public interest auditing easier.[47]

f. Would you recommend that the Agency consider these laws, other requirements, frameworks, or best practices when drafting its regulations? Why, or why not? If so, How?

See above (*supra* Section 3, Question 3(d)).

4. How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.

---

[45] Aziz Huq, A Right to a Human Decision, Virginia Law Review, Vol. 106, No. 3, (May 1, 2020), https://virginialawreview.org/articles/right-human-decision/

[46] Nandita Sampath, "Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing," Consumer Reports, (October 2022), https://digital-lab-wp.consumerreports.org/wp-content/uploads/2022/10/CR_Algorithmic_Auditing_Final_10_2022VF2.pdf

[47] Ibid.

Algorithms are increasingly used to supplement or replace human decisionmaking, and in some cases they are touted as being more objective and thorough than a human decisionmaker.[48] However, an algorithm is only as good as the engineer who designs it and the data it is trained on—human error, including biased data collection methods and the type of algorithm that is chosen by the engineer, can also cause bias. No algorithm will ever be perfect, because a model is a simplified version of real-world events. Most algorithms make mistakes — or are more accurate on certain groups than others[49] — due to these errors during the design process. This can cause real harm when the algorithm is used by a government, school, workplace, or even a landlord.[50]

As mentioned in Section 2, Question 2, employers are using facial recognition algorithms to analyze the emotional states of interviewees and spy on employees. Hospitals use algorithms to assign to patients risk scores that can determine their ability to receive certain treatments. Landlords have used automated tenant screening reports (which include an algorithmically generated score) to make determinations about potential tenants.[51] In the criminal justice system, risk assessments have been used to, among other things, quantify a defendant's future risk of misconduct to determine whether they should be incarcerated before their trial.[52]

Companies like these are typically not required to disclose how their algorithms work, how they trained them, what issues they identified with their technology, and what steps they took to mitigate harm.[53] Furthermore, people usually do not know how the algorithm works on others, so it could be difficult for them to even identify whether they were discriminated against (for example, a woman who is rejected for a job by a resume-screening algorithm may not know that it allowed a man of similar experience to pass through).

In many cases, automated decisionmaking systems, which rely on large stores of data to run, exist on top of a foundation of improperly sourced data. Consumers who did not have the right to object to their personal data being used to train an algorithm are now being evaluated by that

---

[48] Rebecca Heilweil, "Artificial intelligence will help determine if you get your next job," Vox, (December 12, 2019), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen; Sendhil Mullainathan, "Biased Algorithms Are Easier to Fix Than Biased People," The New York Times, (December 6, 2019), https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html.

[49] The National Institute of Standards and Technology found that certain facial recognition algorithms were more likely to misidentify Asian and African American faces relative to Caucasians. "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," National Institute of Standards and Technology: News, (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[50] There are entire books written about these issues, such as Weapons of Math Destruction by Cathy O'Neil (Crown Publishing Group, 2016) and Race After Technology by Ruha Benjamin (Polity, 2019).

[51] Kaveh Waddell, "How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times," Consumer Reports, (March 11, 2021), https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-toughtimes-a2331058426.

[52] Alex Chohlas-Wood, "Understanding risk assessment instruments in criminal justice," Brookings Institution, (June 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice.

[53] Hannah Bloch-Wehba, "Transparency's AI Problem," Knight First Amendment Institute at Columbia University, (June 17, 2021), https://knightcolumbia.org/content/transparencys-ai-problem.

same algorithm. Recent settlements at the FTC that use the "algorithmic disgorgement" remedy imply that the Commission is coming to a similar understanding. That type of improper collection and subsequent usage should be thought of as a privacy invasion in and of itself.

5. What experiences have consumers had with automated decisionmaking technology, including algorithms? What particular concerns do consumers have about their use of businesses' automated decisionmaking technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.

See above (*supra* Section 3, Question 4 and Section 2, Question 2).

6. How prevalent is algorithmic discrimination based upon classifications/classes protected under California or federal law (e.g., race, sex, and age)? Is such discrimination more pronounced in some sectors than others? If so, which ones? Please provide specific examples, studies, cases, data, or other evidence of such discrimination when responding to this question, if possible.

See above (*supra* Section 2, Question 2) for examples.

While some types of data are more capable of serving as proxies on their own due to historical injustices (i.e. location data), another risk that increases along with the ability of firms to process enormous data sets is the risk of businesses combining many small data points to create a profile for a person that implicitly reveals or exploits protected traits. Moreover, even when there is no intention to discriminate, black box algorithms can produce discriminatory results by replicating patterns of inequity that are already present in societal data inputs. This segmentation is often done through algorithms that are inherently difficult for external observers to test and hold accountable — especially when companies take affirmative measures to frustrate researchers testing for potential bias.

7. How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Opt out rights may reduce instances of algorithmic discrimination if fewer individuals are subject to automated decisions, but on their own those rights will not eliminate the ability of algorithms to discriminate. Access and explainability rights supplemented with a right to contest could also reduce discrimination if consumers are able to leverage knowledge of an algorithm's logic or inputs to refute its decisions as discriminatory.

Ideally consumers should not be forced to take action to "opt out" of algorithmic discrimination or contest discriminatory decisions on an individual basis - discriminatory technologies should be clearly prohibited through law. Consumer Reports has previously advocated for

anti-discrimination provisions in ADPPA and included similar provisions in our model state privacy act that use a disparate impact analysis.[54]

8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors(e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?

Consumer Reports believes all consumer rights, including access and opt-out rights relating to automated decisions with legal or similarly significant effects, should apply as broadly as possible. See above (*supra* Section 2, Question 3(a)) for our view on the difficulties of differentiating between "risky" and "non-risky" technologies.

9. What pieces and/or types of information should be included in responses to access requests that provide meaningful information about the logic involved in automated decisionmaking processes and the description of the likely outcome of the process with respect to the consumer? In addition:

> *a. What mechanisms or frameworks should the Agency use or require to ensure that truly meaningful information is disclosed?*
>
> *b. How can such disclosure requirements be crafted and implemented so as not to reveal a business or organization's trade secrets?*

10. To the extent not addressed in your responses to the questions above, what processes should be required for access and opt-out rights? Why?

See above (*supra,* Section 3, Question 3 (c)) for a discussion on the difficulties of producing meaningful information about the logic of automated decisionmaking processes.

****

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 Matt Schwartz (matt.schwartz@consumer.org) or Justin Brookman (justin.brookman@consumer.org) for more information.

---

[54] Consumer Reports, Model State Privacy Act, (Feb. 2021), Sections 126 and 127, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf .