Model State Privacy Act

FEBRUARY, 2021

Consumer Reports | Digital Lab

INTRODUCTION

Over the last thirty years, companies have dramatically expanded their data collection practices as they have found new ways to monetize consumers' private information, but there are few federal requirements to keep that data private and secure. This lack of legal protections is particularly frustrating because privacy is a basic human right, enshrined in American jurisprudence and in nearly a dozen state constitutions.[1] While there are federal laws that provide certain protections for financial[2] and some health data,[3] there is no comprehensive federal privacy law granting consumers baseline privacy and security protections, covering tech giants like Google, Amazon, and Facebook. The Federal Trade Commission (FTC) has taken action against companies for privacy and security violations under its authority to police unfair and deceptive acts and practices,[4] but it is vastly underpowered and under-resourced.[5] California has adopted a landmark privacy law, the California Consumer Privacy Act (CCPA), but consumers have struggled to exercise their new privacy rights.[6]

Consumers shouldn't bear the burden of securing their own privacy. This model bill prohibits companies from engaging in the most privacy-invasive behaviors. The data minimization provision limits companies' collection, use, and disclosure of data to what is reasonably necessary to operate the service. In contrast, existing privacy laws typically require consumers to either opt in or opt out of the disclosure of their data. Both are better than the FTC's "notice-and-choice" regulatory approach, which directs companies to outline their privacy practices in a disclosure.[7] But neither is ideal. While opt in may be preferable to opt out, particularly in the absence of a global opt-out option, companies have been able to force consumers to consent to more sharing that they intended through the use of dark patterns—deceptive interfaces that subvert user intent.[8] In response to Europe's recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data

[1] National Conference of State Legislatures, Privacy Protections in State Constitutions (May 11, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.
[2] Gramm-Leach-Bliley Act, 113 Stat. 1338.
[3] Health Insurance Portability and Accountability Act, 110 Stat. 1936.
[4] Fed. Trade Comm'n, Privacy and Security Enforcement (last visited May 19, 2020), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.
[5] Tony Romm, *The Agency in Charge of Policing Facebook and Google is 103 Years Old. Can it Modernize?* WASH. POST (May 4, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/.
[6] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* CONSUMER REPORTS DIGITAL LAB (Oct. 1, 2020), http://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf. California voters have recently ratified the California Privacy Rights Act (CPRA), which refines and strengthens the CCPA. Most provisions will become operative on January 1, 2023.
[7] Florencia Marotta-Wurgler, *Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies* at 2-3 (Apr. 2015), https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf.
[8] Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, THE VERGE (Aug. 29, 2013), https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you.

for any number of undisclosed purposes.[9] Consumers shouldn't be asked to opt in to harmful data sharing; it should simply be restricted.

Consumer Reports proposes this model legislation to ensure that companies are required to honor consumers' privacy. This model law uses the CCPA as a baseline,[10] and provides additional protections to ensure that consumers' privacy rights are respected by default—in other words, without the consumer having to take action. The model bill provides eight key protections:

- Data minimization and a broad prohibition on secondary data sharing;
- Opt out of first-party advertising;
- Right to delete;
- Right to access and data portability;
- Right to correct;
- Data security;
- Non-discrimination; and
- Strong enforcement.

In the absence of comprehensive consumer privacy protections on the federal level, momentum for privacy and data security laws has moved to the states. The CCPA, which went into effect on January 1, 2020, is one of the first comprehensive laws to protect consumers' online privacy.[11] The CCPA advances consumer protections in several important ways—increased transparency, and the right to access, delete, and opt out of the sale of information to third parties. But while it is a good start, the CCPA is not strong enough to fully protect consumer data. The CCPA provides few limits on companies' collection of data—which inherently threatens consumer privacy. The unchecked collection and sharing of data—even if it has nothing to do with the service requested by the consumer—has allowed companies like Google and Facebook to grow into behemoths with the ability to draw unparalleled insights into a consumer's activities, associations, and preferences—and even to predict these behaviors. Once collected, even under the CCPA, there are few limits on what companies can do with the data.

The CCPA also puts a lot of responsibility on the consumer to figure out every company that collects information about them and opt out—which is too burdensome for consumers. Consumer Reports has found that consumers experience significant difficulty exercising their rights under the CCPA. In our recent study, hundreds of volunteers tested the opt-out provision of the CCPA, by submitting DNS requests to companies listed on the data broker registry. Many data brokers' opt-out processes are so onerous that they have substantially impaired consumers' ability to opt out, highlighting serious flaws in the CCPA's opt-out model. Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software. Some data brokers asked consumers to submit information or documents that they were reluctant to provide, such as a government ID number, a photo of their government ID, or a selfie. Consumers were often forced to wade through confusing and intimidating disclosures to opt out. About 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.[12] In the absence of default privacy protections, the new

[9] *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[10] Cal. Civ. Code § 1798.100 et seq.
[11] *Id.* at § 1798.198.
[12] *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, *supra* note 6.

Global Privacy Control, a proposed standard to allow consumers to send a global "Do Not Sell" signal, could help make the CCPA more workable for consumers[13] (CCPA regulations require companies to honor these signals;[14] CPRA adds this requirement to the statute).[15] The CCPA's authorized agent provisions, which allow consumers to delegate third parties to submit requests on their behalf, also help provide a practical option for consumers seeking to submit requests to multiple companies.[16]

Additionally, some adtech platforms and publishers, including Google and Facebook, have exploited ambiguities in the CCPA to not honor consumer requests to stop the sale of their information to third parties.[17] The recently-ratified California Privacy Rights Act will help close up loopholes that companies have exploited to continue to deliver targeted advertising outside of the opt out—though those provisions will not go into effect until 2023.[18]

Some states have been moving in the wrong direction following passage of CCPA. Several states have pursued legislation that is weaker than the CCPA. For example, in 2019, an industry-favored privacy bill, SB 5376, nearly passed the Washington State legislature, over the objections of privacy advocates.[19] The 2019 bill—based on a risk assessment model that would have essentially given companies the choice of whether or not to comply—unfortunately has been replicated in other states, such as Illinois,[20] Minnesota,[21] and Arizona.[22] (A much-improved Washington Privacy Act also failed to make it across the finish line in 2020).[23] In 2019, Nevada passed a bill giving consumers a limited right to opt out of the sale of their data to third parties—but the new law is riddled with exemptions, and due to its narrow definition of sale, does not completely cover data used for online tracking.[24] Weak privacy legislation could be worse than no privacy legislation at all, if it does nothing to rein in existing data use practices and hinders efforts to pass effective legislation in other states or on the federal level.

That's why it's crucial that states pass privacy legislation that protects consumers' privacy by default. Below, we outline the key provisions for strong legislation:

---

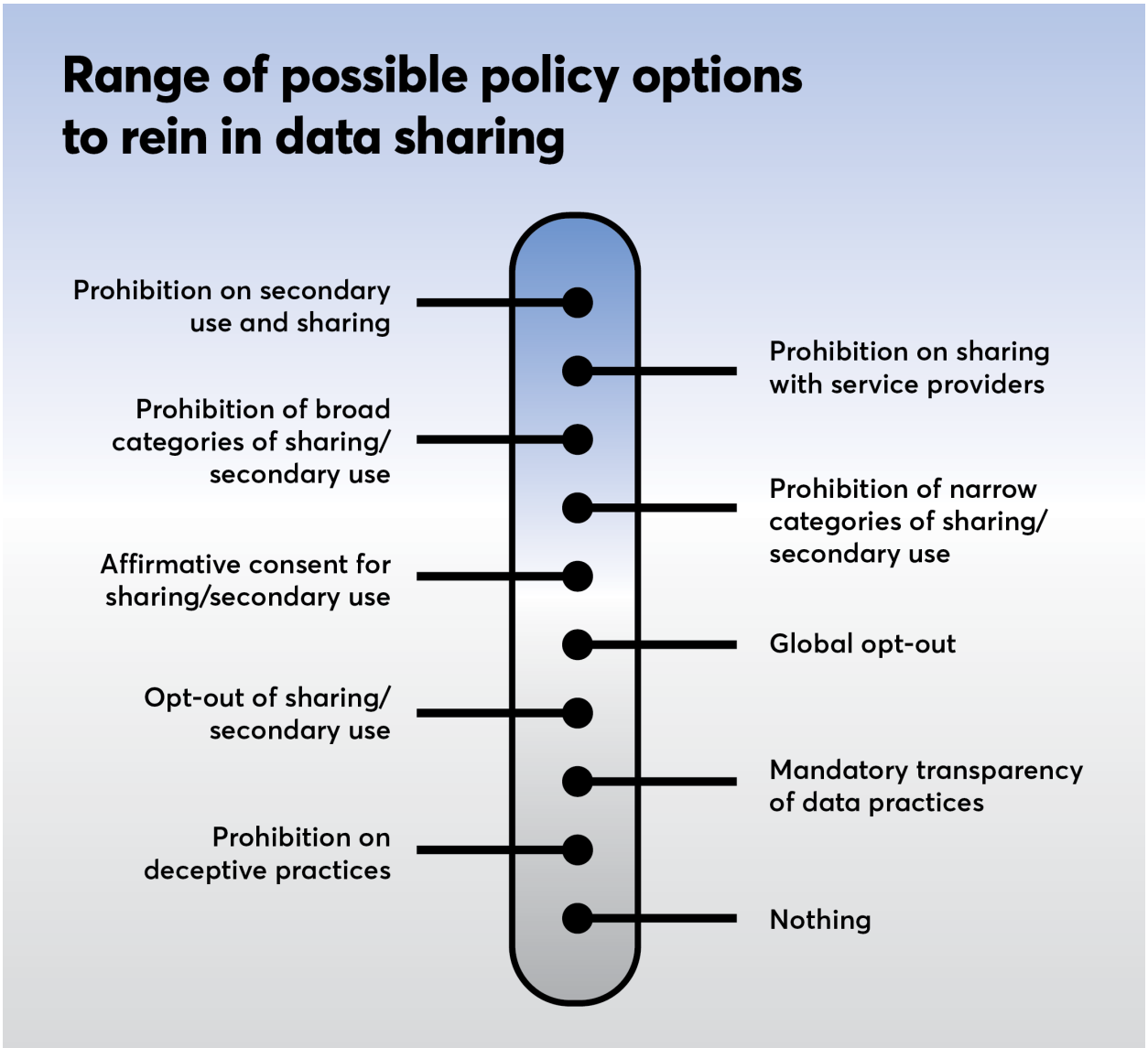
[13] Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.
[14] Cal. Code Regs. tit. 11 § 999.315(c) (2020).
[15] Cal. Civ. Code § 1798.135(e).
[16] Consumer Reports has begun to explore submitting CCPA requests on behalf of consumers. See Maureen Mahoney, Ginny Fahs, and Don Marti, *The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act*, CONSUMER REPORTS DIGITAL LAB (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_AuthorizedAgentCCPA_022021_VF_.pdf.
[17] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act* (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.
[18] California Privacy Rights Act (2020), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.
[19] Letter from Consumer Reports et al. to The Honorable Christine Rolfes (Feb. 21, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/02/SB-5376-Privacy-Coalition-Letter-Oppose.pdf; Letter from Consumer Reports et al. to The Honorable Zach Hudgins (March 25, 2019), https://advocacy.consumerreports.org/wp-content/uploads/2019/03/Privacy-Coalition-Letter-Opposing-ITED-v.-4.pdf
[20] SB 2263 (2019).
[21] HF 3936 (2020).
[22] HB 2729 (2019).
[23] Maureen Mahoney, *Washington State Fails to Advance Game-Changing Privacy Law,* MORNING CONSULT (Mar. 16, 2020), https://morningconsult.com/opinions/washington-state-fails-to-advance-game-changing-privacy-law/.
[24] NRS 603A.345, https://www.leg.state.nv.us/NRS/NRS-603A.html.

Data minimization and a broad prohibition on secondary data sharing: Privacy laws must set limits on the data that companies can collect and share. Consumers should be able to use an online service or app safely without having to take any action, such as opting in or opting out. This model bill helps ensure privacy by default by requiring data minimization in Section 2, 103(a)-(b), in other words, limiting data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, with some exceptions for operational purposes. Falling outside of the limits of what is reasonably necessary is the sale of data to third parties, which is contrary to consumer expectations and is not needed to provide the service.

A strong default prohibition on data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially hundreds of different companies. We do not characterize this framework as an "opt-in" approach either, as secondary data sharing is simply prohibited. While consumers are always free to share data with whomever they like, a privacy law should not encourage companies to coerce consumers into giving permission for additional tracking or sharing, such as by denying consumers access to the site content without agreement to the information-sharing terms, as many companies have done in response to the Global Data Protection Regulation (GDPR) in Europe. If companies want to collect personal data, it should only be as functionally necessary for the specific product a consumer has requested, not for monetization. Privacy law should also prohibit discrimination or differential treatment against consumers who do not agree to share data for a separate unrelated product. If a consumer affirmatively wants to fill out a survey or allow advertisers to monitor cross-site and -app behavior to recommend ads, that is their prerogative. But too often manipulative and confusing consent flows lead users into granting permission to unexpected and unwanted data collection or sharing. Existing consumer protection law prohibits deceptive interfaces, but a privacy statute could more clearly prohibit abusive "dark patterns" that subvert user autonomy.

Section 3(m) lists permitted secondary uses that a company can reasonably do without permission from the consumer: this includes fixing errors, performing internal research (based on first-party data) to improve its own product, and providing customized content or advertising. In other words, this bill permits a fair amount of first-party uses of the data so that consumers can continue to receive the services that they would normally expect—such as having sites recommend products that they might like—without being pummeled with opt-in notices. Consent fatigue is a real concern—if consumers begin to expect to have to opt in to simply use the service, they will be less likely to make a distinction between reasonable and harmful uses of data.[25] The bill also takes the burden of managing privacy and data collection off of the consumer and puts it, appropriately, onto the company.

[25] Neil M. Richards and Woodrow Hartzog, *The Pathologies of Digital Consent* at 1497-8, WASHINGTON UNIVERSITY LAW REVIEW (2019), https://ssrn.com/abstract=3370433.



Opt out of first-party advertising: However, some consumers might be uncomfortable with companies tracking their purchases and offering them suggestions about what they might like. That's why we have provided an opt out for first-party use of data for advertising purposes in Section 2, 103(c). This will ensure that consumers who are more sensitive to first-party advertising can exercise their privacy preferences, without running the risk of consent fatigue.

Right to delete: Consistent with the data minimization principle, consumers should be able to delete data when it is no longer needed. This will help reduce the risk of unwanted disclosure, including through a data breach. For example, the Capital One breach of 2019 included the disclosure of data from credit applications that were over ten years old.[26] The right to delete provision in this bill tracks the CCPA, which is designed to allow businesses to continue to retain

[26] Capital One, Information on the Capital One Cyberincident (Sept. 23, 2019), https://www.capitalone.com/facts2019/.

data if it is needed to continue to provide the service, for research purposes, and for recall and warranty notifications.

Right to access and data portability: Consumers deserve to know the specific information that companies have on file. This model bill gives consumers the ability to access the specific pieces of data collected about them, as well as the specific third parties to whom their information was disclosed—which will make it easier for consumers to exercise their privacy preferences with respect to those companies. It is more expansive than the CCPA, which provides only the categories of third parties to whom the data is sold. This bill also ensures data portability, in other words, it requires companies to provide data in a format that could be easily transferred to a competing service, helping to improve competition among online services. This draft improves upon the CCPA by giving consumers the right to direct the company to transfer that information to another entity so that the consumer does not have to download and port the information themselves.

Right to correct: Personal information is often used to make important decisions about consumers, such as with respect to employment and housing—and data brokers' files often include incorrect information.[27] Consumers should have the right to ensure that the information is accurate. The Fair Credit Reporting Act,[28] the GDPR,[29] and the California Privacy Rights Act[30] all include a right to correct, suggesting that correction rights are increasingly considered one of the basic digital privacy rights.

Non-discrimination: This model state law includes a provision to ensure that companies can't charge consumers more for exercising their privacy rights. Unfortunately, ambiguity in CCPA's text could allow for programs that monetize data by selling personal information about customer habits to third-party data brokers. Consumers could be forced to choose between affordable necessities and their own rights, and retailers can continue to profit off of business models that exploit consumers' privacy without meaningful consumer choice. This model bill cuts off exploitative programs that could separate consumers into privacy haves and have-nots, and clarifies that legitimate loyalty programs, which reward consumers for repeated patronage, are supported by this bill. This bill also ensures that consumers' personal information (like browsing history) can't be used to deny them economic opportunities and benefits.

Data security: This bill ensures that companies are required to protect all information that is reasonably linkable to a consumer. Companies should be required to keep behavioral data, search history, and shopping history secure, as it can reveal more about consumers than they might want to share with others: their sexual preferences, health issues, and political activities. Over 20 states require businesses to keep data secure, but those requirements typically cover only a limited set of personal information (such as banking and other financial information that could lead to identity theft).[31]

---

[27] Persis Yu, *Big Data: A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. at 15 (Mar. 2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf.
[28] 15 U.S.C. § 1681.
[29] European Parliament and Council of European Union (2016) *Regulation (EU) 2016/679*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
[30] California Privacy Rights Act, *supra* note 18.
[31] National Conference of State Legislatures, Data Security Laws: Private Sector (May 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

Strong enforcement: Finally, the CCPA's weak enforcement provisions have been corrected in this model law by adding a private right of action, removing the requirement that the AG provide individual compliance advice to companies, and removing the right to cure (the guidance requirement and right to cure in the CCPA also will be removed from the law when the California Privacy Rights Act becomes operative in 2023). Strong enforcement is essential to make sure that companies comply. The California AG has the resources to bring only an estimated three cases a year for privacy violations, which provides companies with little incentive to comply, given that their chances of getting caught are minimal.[32] The right to cure provision is particularly problematic, as it essentially constitutes a get-out-of-jail-free card for any company that is caught violating the law, provided they can fix their behavior in 30 days. (And given the nature of privacy violations, it's unclear how to "cure" the inappropriate disclosure of a consumer's personal information). In Europe, clearly illegal data sharing practices have continued unabated, despite the GDPR. Regulators as yet appear unwilling to truly hold companies accountable. For example, the UK regulator found that RTB behaviors—the buying and selling of consumer data to sell space on sites for targeted advertising—violates the consent requirement of the GDPR, but still hasn't penalized any companies for continuing to engage in the behavior without consumer consent.[33] While the issue is not without debate, we believe consumer rights are most protected by providing for a private right of action to create appropriate incentives for compliance.

Finally, this is an evolving document that we will update as more information becomes available.

[32] Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court,* SAN FRANCISCO PUBLIC PRESS (May 15, 2019), https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.
[33] Simon McDougall, *Blog: Adtech - The Reform of Real Time Bidding Has Started and Will Continue*, ICO (Jan. 17, 2020), https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.

MODEL STATE PRIVACY ACT

Section 1. Short title. This Act may be cited as the Consumer Privacy Act.

Section 2. Requirements. The following is added to the code of statutes:

100. Transparency about the collection, use, retention, and sharing of personal information.[34]

(a) A business that collects a consumer's personal information shall disclose the following general information in its privacy policy or policies and update that information at least once every 12 months.

(1) A description of how an individual may exercise their rights pursuant to subsections 103, 105, 110, 115, and 120 and one or more designated methods for submitting requests.

(2) The privacy policy shall be:

(A) Clear and written in plain language, such that an ordinary consumer would understand it;

(B) Conspicuous and posted in a prominent location, such that an ordinary consumer would notice it; and

(C) Made publicly accessible before the collection of personal information.[35]

(b) A large business that collects a consumer's personal information shall also disclose the following comprehensive information in an online privacy policy or policies, and update that information at least once every 12 months:

(1) The personal information it collects about consumers.

(2) The categories of sources from which the personal information is collected.

(3) A reasonably full and complete description of the methods it uses to collect personal information.

(4) The specific purposes for collecting, disclosing, or retaining personal information.

(5) The personal information it discloses about consumers, or if the business does not disclose consumers' personal information, the business shall disclose that fact.

(6) The categories of third parties with whom it shares personal information, or if the business does not disclose consumers' personal information to third parties, the business shall disclose that fact.

(7) The categories of service providers with whom it shares personal information, or if the business does not disclose consumers' personal information to service providers, the business shall disclose the fact.

(8) A description of the length(s) of time for which personal information is retained.

(9) If personal information is deidentified such that it is no longer considered personal information but subsequently retained, used, or shared by the company, a description of the method(s) of deidentification.

---

[34] Intel, Ethical and Innovative Data Use Act of 2019, Section 4(f), (May 23, 2019), https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill-05-25-19.pdf. This bifurcated notice—which requires both an easy-to-read, consumer-facing section to explain to consumers how to exercise their rights; and a second, longer section, intended for regulators and privacy testing organizations, that explains the large business's data use practices, so they can be held accountable for failure to comply—is adapted from Intel's 2019 model privacy bill.

[35] *Id.* at Section 4(f)(3)(B).

103. Data minimization and opt out of first party advertising.

(a) A business that collects a consumer's personal information shall limit its collection and sharing of that information with third parties to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or is reasonably necessary for security or fraud prevention.[36] Monetization of personal information shall not be considered reasonably necessary to provide a service or conduct an activity that a consumer has requested or reasonably necessary for security or fraud prevention.

(b) A business that collects a consumer's personal information shall limit its use and retention of that information to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested or a related operational purpose, provided that data collected or retained solely for security or fraud prevention may not be used for operational purposes.

(c) A consumer shall have the right, at any time, to direct a business that uses personal information about the consumer to personalize advertising not to use the consumer's personal information to personalize advertising, and the business shall have the duty to comply with the request, promptly and free of charge, pursuant to regulations developed by the Attorney General. A business that uses a consumer's personal information to personalize advertising shall provide notice that consumers have the "right to opt out" of the use of their personal information to personalize advertising.[37]

104. Prohibition of dark patterns.

(a) It shall be unlawful for any company to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice, as further defined by regulation.[38]

105. Deletion of personal information.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected.

(b) A business that collects personal information about consumers shall disclose, pursuant to the notice requirements of subsection 130, the consumer's right to request the deletion of the consumer's personal information.

---

[36] In this model law, data minimization puts real limits on the company by allowing only the collection and sharing of data needed to provide the service requested by the consumer. While the concept of data minimization is included in the GDPR, the GDPR's formulation is too weak, allowing data collection and sharing this is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." Companies could still list any purposes they would like into the policy to collect whatever they want—taking advantage of the fact that consumers don't typically read privacy policies.

[37] This subsection adds protections to the CCPA—data minimization—that are similar to CA AB 3119 (2020), which would limit collection and sharing to what is reasonably necessary to operate the service, with exemptions for operational purposes. This model bill improves upon AB 3119 since it does not require the consumer to opt-in to data sharing that is necessary to operate the service. The goal is to prevent consumers from being barraged with unnecessary consent dialogues, and to ensure that consumers can both use the service and have their privacy protected.

[38] This definition of "dark patterns" is adapted from S. 1084 (2019), The DETOUR Act, https://www.congress.gov/bill/116th-congress/senate-bill/1084/text. Subverting consumer intent online has become a real problem, and it's important to address. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception. See Mathur, Acar, Friedman, Lucherini, Mayer, Chetty, and Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, CONSUMERPROC. ACM HUM.-COMPUT. INTERACT. (2019), https://webtransparency.cs.princeton.edu/dark-patterns/.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) If a consumer submits a deletion request to a service provider that has collected, used, processed, or retained the consumer's personal information in its role as a service provider, then the service provider shall direct the consumer to the business where the consumer can submit their deletion request.

(e) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer.[39]

(2) Detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise constitutionally-protected speech, or ensure the right of another consumer to exercise his or her right to constitutionally-protected speech, including speech conducted through use of a business.

(5) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(6) Comply with a legal obligation.

110. Access to and portability of retained personal information.

(a) If a business collects personal information about a consumer, the consumer shall have the right to ask the business for the following information, and the business shall have the duty to provide it, promptly and free of charge, upon receipt of a verifiable request:

(1) The specific pieces of personal information that the business retains about that consumer.

(2) Its purpose for collecting the personal information.

(b) When a business receives a verifiable consumer request from a consumer for the specific pieces of their personal information, the business shall disclose that information in an electronic, portable, machine-readable, and readily-useable format or formats to the consumer, or to another business of the consumer's designation. The Attorney General shall issue regulations to implement this subsection.

115. Access to disclosures of personal information.

(a) If a business discloses personal information about a consumer to a third party or service provider, the consumer shall have the right to ask the business for the specific third parties or service providers to whom the personal information was disclosed, and the business

[39] This provision was added to the CCPA by AB 1146 (2019), to ensure that the CCPA does not interfere with consumer notification in the event of a recall or to take advantage of a warranty.

shall have the duty to provide it, promptly and free of charge, upon receipt of a verifiable request.[40]

120. Right to correct inaccurate personal information.[41]

(a) A consumer shall have the right to require a business that maintains inaccurate personal information about the consumer to correct such inaccurate personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to subsection 130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate information shall use commercially reasonable efforts to correct the inaccurate personal information, as directed by the consumer, pursuant to subsection 130.

125. No discrimination by a business against a consumer for exercise of rights.

(a) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, or did not agree to information processing for a separate product or service, including, but not limited to, by:

(1) Denying goods or services to the consumer.

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(3) Providing a different level or quality of goods or services to the consumer.

(4) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(5) This title shall not be construed to prohibit a business from offering discounted or free goods or services to a consumer if the offering is in connection with a consumer's voluntary participation in a program that rewards consumers for repeated patronage, if personal information is used only to track purchases for loyalty rewards, and the business does not share the consumer's data with third parties pursuant to that program.[42]

126. Discrimination in economic opportunities.[43]

(a) It is unlawful to process information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, or insurance, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

(b) The unlawful processing of personal information based on disparate impact is established under this subsection only if:

---

[40] This subsection expands upon the CCPA by requiring companies to provide specific third parties to whom the information was sold, rather than just the categories of companies, so consumers can more easily exercise their rights with respect to those companies.

[41] This subsection is adapted from CPRA § 1798.106.

[42] This subsection removes from the CCPA the existing § 1798.125(e) that could allow companies to charge consumers more for exercising their privacy rights. In its place is a provision making it clear that bona fide loyalty programs, that reward consumers for repeated patronage, are allowed and even encouraged, as long as these companies are prohibited from selling data to third parties. It is similar to consensus language in the Washington Privacy Act (2021), Sec. 107(v)(7), http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062-S2.pdf?q=20210221185931.

[43] This subsection is drawn from *The Online Civil Rights and Privacy Act of 2019*, FREE PRESS ACTION AND THE LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW, Section 3(a) (Mar. 11, 2019), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

(1) A complaining party demonstrates that the processing of personal information causes a disparate impact on the basis of a protected characteristic; and

(2) The respondent fails to demonstrate that the challenged processing of information is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; or

(3) The complaining party shows that an alternative policy or practice could serve such interests with a less discriminatory effect.

(c) With respect to demonstrating that a particular processing of personal information causes a disparate impact as described in paragraph (a), the complaining party shall demonstrate that any particular challenged component of the processing of personal information causes a disparate impact, except that if the components of the respondent's processing of personal information are not reasonably capable of separation for analysis, the processing of personal information may be analyzed as a whole. Machine learning algorithms are presumed to be not capable of separation for analysis unless respondent proves otherwise by a preponderance of the evidence.

127. Discrimination in public accommodations.[44]

(a) It is unlawful to process personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, or disability.

(b) The standards for disparate impact cases stated in Section 126(b)-(c) shall apply to disparate impact cases with respect to this paragraph.

(c) It is unlawful for any person to:

(1) Withhold, deny, deprive, or attempt to withhold, deny, or deprive, any person of any right or privilege secured by this paragraph;

(2) Intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce, any person with the purpose of interfering with any right or privilege secured by this paragraph; or

(3) Punish or attempt to punish any person for exercising or attempting to exercise any right or privilege secured by this paragraph.

128. Reasonable security.

(a) A business or service provider shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the information and the purposes for which the personal information will be used, to protect consumers' personal information from unauthorized use, disclosure, access, destruction, or modification.

130. Business implementation of duties.

(a) A business shall:

(1) (A) Make available to consumers two or more designated methods for submitting requests permitted by this title, including, at a minimum, a telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address or online portal for submitting requests for information required to be disclosed pursuant to subsections

[44] *Id.* at Section 3(b). This subsection is drawn from Free Press Action and the Lawyers' Committee for Civil Rights Under Law's Online Civil Rights and Privacy Act of 2019.

110 and 115, or for requests for deletion or correction pursuant to subsections 105 and 120, respectively.[45]

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to subsections 110 and 115, or for requests for deletion or correction pursuant to subsections 105 and 120, respectively.

(2) Disclose and deliver the required information to a consumer free of charge, or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request, within 45 days of receiving a verifiable consumer request. The business shall promptly take steps to determine whether the request is a verifiable consumer request from the identified consumer. The time period may be extended once by 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. It shall be delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option, if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable request.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in this Act, and how to direct consumers to exercise their rights in this Act.

(4) Limit the use of any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification, and not further disclose the personal information or retain it longer than necessary for the purposes of verification.

(b) A business is not obligated to provide the information required by subsections 110 and 115 to the same consumer more than twice in a 12-month period.

(c) A service provider shall not be required to comply with a verifiable consumer request pursuant to subsections 110, 115, and 120 to the extent that the service provider has collected personal information about the consumer in its role as a service provider. A service provider shall provide assistance to a business with which it has a contractual relationship with respect to the business's response to a verifiable consumer request, including but not limited to by providing to the business the consumer's personal information in the service provider's possession, which the service provider obtained as a result of providing services to the business, and by correcting inaccurate information. A service provider that collects personal information on behalf of a business shall be required to assist the business in complying with the requirements of subsection 100.[46]

Section 3. Definitions.

For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

[45] This incorporates amendments to the CCPA made by AB 1564 (2019).
[46] This clarification of the role of service providers is added by CPRA § 1798.130(a)(3)(A).

(b) “Biometric information” means an individual’s physiological, biological or behavioral characteristics or an electronic representation of such, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) “Business” means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of [XX], and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of fifty million dollars ($50,000,000) in the preceding calendar year, as adjusted pursuant to Section 8.

(B) Alone or in combination, annually buys, receives for the business’ commercial purposes, shares, or discloses for commercial purposes, alone or in combination, the personal information of [100,000] or more consumers, households, or devices.[47]

(C) Derives 50 percent or more of its annual revenues from sharing consumers’ personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers’ personal information. “Control” or “controlled” means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark, such that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(e) “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.

(f) “Commercial purposes” means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. “Commercial purposes” do not include for the purpose of

[47] CPRA raises one of the CCPA’s thresholds: from a company that receives or shares the data of 50,000 consumers, households, or devices per year to one that receives or shares the data of 100,000 consumers, households, or devices per year. Since “consumer” refers to a resident of the state, these numbers will not be appropriate for states with much smaller populations, and we recommend adopting a threshold that is roughly proportionate.

engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a [XX] resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, reasonably be associated with, or reasonably be linked, directly or indirectly, to a particular consumer, provided that the business:

(1) Takes reasonable measures to ensure that the data could not be re-identified;

(2) Publicly commits to maintain and use the data in a de-identified fashion and not to attempt to reidentify the data; and

(3) Contractually prohibits downstream recipients from attempting to re-identify the data.[48]

(i) "Designated methods for submitting requests" means a mailing address, email address, Internet Web page, Internet Web portal, telephone number, or other applicable contact information, whereby consumers may submit a request under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 8.

(j) "Device" means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "Intentionally interacts" means when the consumer intends to interact with a person via one or more deliberate interactions, such as visiting the person's website or purchasing a good or service from the person. Hovering over, muting, pausing, or closing a given piece of content, or using a communications service to interact with a third-party website, does not constitute a consumer's intent to interact with a person.

(m) "Large business" is a business that, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of [10,000,000] or more consumers in a calendar year.[49]

(n) "Operational purpose" means the use of personal information when reasonably necessary and proportionate to achieve one of the following purposes, if such usage is limited to the first-party relationship and customer experience:

(1) Debugging to identify and repair errors that impair existing intended functionality.

(2) Undertaking internal research for technological development, analytics, and product improvement, based on information collected by the business.

(3) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, or to

---

[48] This definition is similar to that in CPRA and tracks the Federal Trade Commission's definition of deidentified: that a company cannot reidentify the information, even if they wanted to. See, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMM'N at 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[49] This definition of "large business" for bifurcated notice obligations reflects the one included in the California Attorney General's CCPA regulations, § 999.317(g). Since "consumer" refers to a resident of the state, these numbers likely will not be appropriate for states with much smaller populations than California, and we recommend adopting a threshold that is roughly proportionate.

improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(4) Customization of content based on information collected by the business.

(5) Customization of advertising or marketing based on information collected by the business.

(o) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(p) (1) "Personal information" means information that identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device.[50]

(2) "Personal information" does not include publicly available information. For the purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(q)(1) "Place of public accommodation" includes all businesses of any kind, whether for-profit or not for-profit, that offer goods or services of any kind to the general public, whether for a charge or not for a charge. This includes businesses that offer goods or services through the Internet or any other medium of communications, regardless of whether or not they operate from a physical location.[51]

(2) "Place of public accommodation" does not include a tax-exempt religious entity, a distinctly private club, or a distinctly private online discussion forum. A club or online discussion forum shall be deemed distinctly private if (1) Its primary purpose is expressive association; (2) It is membership-based and has no more than 1000 members; and (3) It does not regularly receive payment directly or indirectly on behalf of non-members for dues, fees, use of physical or online facilities, or goods or services of any kind, for the furtherance of trade or business.[52]

(r) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(s) "Service" or "services" means work, labor, and services, including services furnished in connection with the production, sale or repair of goods.

(s) "Service provider" means a person that processes personal information on behalf of a business and to which the business discloses a consumer's personal information pursuant to a written or electronic contract, provided that (1) the contract prohibits the person from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, including a prohibition on retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business; and (2) the service provider does not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.[53]

---

[50] This definition of personal information is similar to the CCPA, in that it covers information reasonably linkable to a consumer, both directly or indirectly. It's important to have a broad definition of personal information to ensure that targeted advertising is covered by the law: information disclosed for targeted advertising purposes cannot always be associated with an individual consumer. However, unlike the CCPA, this definition does not include examples of categories of personal information, because a list could have the unintended effect of limiting the information covered by the law.

[51] From David Brody and Sean Bickford, *Discriminatory Denial of Service: Applying State Public Accommodations Laws to Online Commerce*, LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW at 7 (Jan. 2020), https://lawyerscommittee.org/wp-content/uploads/2019/12/Online-Public-Accommodations-Report.pdf.

[52] *Id.*

[53] The service provider exemption improves upon the CCPA's and CPRA's by tightly limiting use of the information and preventing service providers from combining information received from multiple companies. Without these

(t) “Share” means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.[54]

For purposes of this title, a business does not share personal information when:

(1) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with one or more third parties, provided the third party or parties do not also share the personal information, unless that disclosure would be consistent with the provisions of this title.

(2) The business discloses the personal information of a consumer with a service provider and the business has provided notice that the information is being used or disclosed in its terms and conditions consistent with subsection 100.

(3) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or disclosed consistently with this title. A third party may not materially alter how it uses or discloses the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection.

(u) “Third party” means a person who is not any of the following:

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer’s current interaction with the business under this title.

(2) A service provider to whom the business discloses a consumer’s personal information pursuant to a written contract, which includes a certification made by the person receiving the personal information that the person understands the restrictions under the Consumer Privacy Act and will comply with them.

(v) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify.[55] A business is not obligated to provide any personal information to a consumer pursuant to subsections 110 and 115, to delete personal information pursuant to subsection 105, or to correct inaccurate personal information pursuant to subsection 120, if the business cannot verify that the consumer making the request is the consumer about whom the business has collected personal information or is a person authorized by the consumer to act on such consumer’s behalf.[56]

---

protections, service providers (such as Salesforce) could build huge databases of customer data, allowing them to develop even more sensitive insights into consumers’ behavior.

[54] This definition is similar to the CCPA’s definition of sale, except it adds a final clause, “or otherwise for a commercial purpose,” to ensure that transfers of data for targeted advertising purposes are covered (this loophole is addressed by CPRA). Some incorrectly claim that because money isn’t necessarily exchanged for data, data transfers for targeted advertising purposes aren’t a sale under the CCPA—therefore, consumers don’t have the right to opt out. See, Tim Peterson, *‘We’re Not Going to Play Around’: Ad Industry Grapples with California’s Ambiguous Privacy Law,* DIGIDAY (Dec. 9, 2019), https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/.

[55] This “authorized agent” provision mirrors language in the CCPA that gives consumers the right to delegate to third parties the ability to submit requests on their behalf, providing a practical option for submitting requests to multiple companies.

[56] It’s appropriate to require identity verification for access, correction, and deletion requests, however, opt outs should not require verification, since that would exempt information that can’t be associated with an identifiable consumer.

Section 4. Exceptions.

(a) The obligations imposed on businesses by this title shall not restrict a business's or service provider's ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, share, or disclose consumer information that is deidentified or in the aggregate derived from personal information.

(6) Collect or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of [XX]. For purposes of this title, commercial conduct takes place wholly outside of [XX] if the business collected that information while the consumer was outside of [XX], no part of the sharing of the consumer's personal information occurred in [XX], and no personal information collected while the consumer was in [XX] is shared. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in [XX] and then collecting that personal information when the consumer and stored personal information is outside of [XX].

(b) Nothing in this title shall require a business to violate an evidentiary privilege under [XX] law or federal law or prevent a business from providing the personal information of a consumer who is covered by an evidentiary privilege under [XX] law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Personal information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) This title shall not apply to activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal

characteristics, or mode of living by a consumer reporting agency, as defined by subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code. This paragraph shall only apply to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, disclosed, sold, communicated, or used except as authorized by the Fair Credit Reporting Act.[57]

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102) or the [XX state financial privacy law], and implementing regulations, if it is inconsistent with that act, and only to the extent of the inconsistency.[58]

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.), if it is in conflict with that act.

(g) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verifiable consumer request may be extended by up to a total of 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider in compliance with this title shall select as service providers entities that are capable of adhering to the restrictions set forth in this title, and enforce compliance in adhering to these restrictions, through effective enforceable contractual obligations and regular evaluation of compliance.[59] A service provider shall not be liable under this title for the obligations of a business for which it provides

---

[57] Since consumer reporting agencies are incompletely covered by FCRA (some also sell information for non-FCRA covered purposes, such as for marketing or advertising), it's important that the FCRA carveout is carefully tailored only to FCRA-covered activities. See, Steven Melendez and Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information,* FAST COMPANY (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[58] Too many state privacy bills inappropriately exempt information covered by the Gramm-Leach-Bliley Act (GLBA). GLBA is weak legislation that primarily provides an opt out of disclosure to third parties and does not provide access or deletion rights. It would be inappropriate to treat sensitive financial data less strictly than other data. Moreover, GLBA explicitly allows for stronger state laws. See GLBA (Sec. 507), which clarifies that states can pass stronger laws. https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

[59] This model act adds new oversight responsibilities to companies' existing CCPA requirements to ensure that their service providers are complying with the law.

services as set forth in this title, provided that the service provider shall be liable for its own violations of this title.

(i) This title shall not be construed to require a business to:

(1) Comply with a verifiable consumer request to access, delete, or correct personal information pursuant to subsections 105, 110, 115, or 120 if all of the following are true:

(A) (i) The business is not reasonably capable of linking or associating the request with the personal information, or

(ii) It would be unreasonably burdensome for the business to link or associate the request with the personal information;

(B) The business does not use the information to recognize or respond to the specific consumer who is the subject of the personal information or link or associate the personal information with other personal information about the same specific consumer.

(C) The business does not share the personal information to any third party, or otherwise voluntarily disclose the personal information to any third party other than a service provider except as otherwise permitted in this subsection.

(2) Maintain information in identifiable, linkable or associable form, or to collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.[60]

(j) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(k) Nothing herein shall apply to the publication of newsworthy information to the public, or to the collection or editing of information for that purpose.

Section 5. Consumer's private right of action.

(a) A consumer who has suffered a violation of this Act may bring a lawsuit against the business that violated this Act. A violation of this Act shall be deemed to constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this Act.

(b) A consumer who prevails in such a lawsuit shall obtain the following remedies:

(1) Damages in an amount not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(2) Injunctive or declaratory relief, as the court deems proper.

(3) Reasonable attorney fees and costs.

(4) Any other relief the court deems proper.

(c) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(d) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible and the behavior underlying the violations was unintentional, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual

[60] This paragraph adds new guidance to companies for compliance with the CCPA: the goal is to ensure that companies are not encouraged to reidentify information kept in a bona fide deidentified form in order to respond to consumer requests.

statutory damages or class-wide statutory damages may be initiated against the business. A cure shall not be possible for violations of sections 103, 104, 105, 110, 115, 120, 125, 126, 127, and 128. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.[61]

(e) A consumer bringing an action shall notify the Attorney General within 30 days that the action has been filed.

Section 6. Enforcement.

(a) The State Attorney General, a County District Attorney, or a City Corporation Counsel may bring a civil action, in the name of the people of the state, against any business, service provider, or other person that violated this Act.

(b) Any person, business, or service provider that violates this title may be liable for a civil penalty of up to seven thousand five hundred dollars ($7,500) for each intentional violation and of up to two thousand five hundred dollars ($2,500) for each unintentional violation.

Section 7. Construction. This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information. The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sharing of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

Section 8. Attorney General regulations.

(a) The Attorney General has the ability to issue regulations including, but not limited to, the following areas:

(1) Detailing and updating as needed the types of information that are "personal information," the definition of "deidentified," "intentionally interacts," and "dark patterns," in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Establishing what is reasonably necessary to provide a service or conduct an activity that a consumer has requested, or is reasonably necessary for security or fraud prevention.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.

(4) Adjusting the monetary threshold in Section 3(c)(1)(A) in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(5) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to

[61] A limited right to cure could make sense in the context of a private right of action; however, the right to cure is inappropriate in administrative enforcement, because it could provide incentives for companies to break the law. The right to cure in administrative enforcement was removed from the CCPA by Proposition 24.

consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings.

(6) Establishing rules and procedures to further the purposes of subsections 105, 110, 115, and 120 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain personal information, delete personal information, or correct inaccurate personal information pursuant to subsection 130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business' determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business' authentication of the consumer's identity.

(7) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer or the consumer's authorized agent to opt out of the use of their personal information to personalize advertising pursuant to Section 103(c).

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the use of their personal information to personalize advertising.

(8) Establishing rules and procedures to govern business compliance with 100(d), to provide information in an electronic, portable, machine-readable, and readily-useable format or formats to the consumer, or to another business of the consumer's choice.

(b) The Attorney General may update the foregoing regulations, and adopt additional regulations, as necessary to further the purposes of this title.

(c) Before adopting any regulations, the Attorney General shall solicit broad public participation concerning those regulations.

Section 9. Intermediate transactions. If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.[62]

Section 10. Non-waiver. Any provision of a contract or agreement of any kind, including an arbitration agreement, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.

Section 11. Construction. This title shall be liberally construed to effectuate its purposes.

Section 12. Effective date. This title shall be operative one year after it is enacted.

Section 13. **Severability**.
(a) The provisions of this bill are severable. If any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

[62] This provision is adapted from CPRA § 1798.190 to help prevent non-compliance.

Please contact **Justin Brookman (justin.brookman@consumer.org)** or **Maureen Mahoney (maureen.mahoney@consumer.org)** for more information.