The State Data Privacy Act

A Proposed Compromise by Consumer Privacy Advocates

BY ELECTRONIC PRIVACY INFORMATION CENTER AND CONSUMER REPORTS

UPDATED APRIL 2025

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

CR Consumer Reports

Authors

This bill received feedback and comments from dozens of people, but was primarily drafted by four authors.

Caitriona Fitzgerald - Deputy Director, Electronic Privacy Information Center - fitzgerald@epic.org
Maggie Oates - Policy Analyst, Consultant, Consumer Reports - hello@maggieoates.com
Matt Schwartz - Policy Analyst, Consumer Reports - matt.schwartz@consumer.org
Kara Williams - Law Fellow, Electronic Privacy Information Center - williams@epic.org

A section-by-section summary and multiple formats of this bill are available on CR and EPIC's sites.

Endorsements

The State Data Privacy Act was published by EPIC and Consumer Reports. It has been endorsed by Accountable Tech, the Center for Democracy & Technology (CDT), Common Sense Media, the Consumer Federation of America (CFA), Issue One, U.S. Public Interest Research Group (U.S. PIRG), Public Knowledge, and Young People's Alliance (YPA).

Summary

Why is a state compromise bill needed? State legislatures have an opportunity to lead on privacy.

In the absence of a federal privacy law in the United States, **state legislators have the opportunity to be the champions of protecting privacy** for everyday people. As of September 2024, 19 states have signed state privacy laws, but unfortunately most of those laws—heavily influenced by Big Tech—fail to protect consumers from the harms of online tracking and data abuse as well as they could. In our State Data Privacy Act, we set forth a compromise bill built on existing state laws that meaningfully protects privacy while encouraging innovation.

Why redline the Connecticut Data Privacy Act? States need a more protective and practical bill.

Every American deserves privacy protections, so we set out to craft a proposed privacy bill that *works for businesses and consumers alike*. The base text of the State Data Privacy Act is the Connecticut Data Privacy Act (CTDPA), a bill that industry often cites as a model for other states to adopt. In our view, CTDPA contains far too many loopholes that prevent it from offering strong privacy protections, but it is an established bill that many state lawmakers are already familiar with. Strengthening the CTDPA provides consistency for businesses while giving consumers meaningful privacy protections.

The goals of the State Data Privacy Act are to:

- Limit ubiquitous online tracking;
- Encourage more privacy-protective methods of online advertising;
- Protect the most sensitive data, including data about kids and teens;
- Use language from existing state laws; and
- Allow for meaningful enforcement of the law to ensure compliance.

The State Data Privacy Act borrows existing language from strong state laws and federal bills wherever possible. Borrowing existing language reduces the chances of conflicts of law and, in many cases, also represents years of deliberation and stakeholder discussions. Because our organizations have been involved in privacy advocacy at the state level for many years, we are familiar with recurring patterns of contention and compromise between businesses and consumer privacy advocates. While this draft does not represent the ideal privacy bill for any of the signatory organizations, it is a compromise that would meaningfully protect consumers.

What changed? Key amendments were necessary to provide meaningful privacy protections.

Data Minimization. A strong privacy law should limit the data companies can collect and use to match what consumers expect based on the context of their interaction with the business. In contrast, the core of the framework found in many state laws is notice-and-choice focused on disclosures in privacy policies. These laws allow businesses to continue collecting whatever personal data they want and using it for any reason they want as long as they disclose that practice in their privacy policies—policies that very few consumers read or could even decipher if they did—meaning the status quo of massive data collection and sale continues uninterrupted. Rather than continue with this approach that harms consumers, the State Data Privacy Act sets out a rule that businesses can only collect and use data when it is "reasonably necessary" to provide the services the consumer asks for. Personal data collected in compliance with these rules may be used for most forms of advertising, providing businesses with data they desire to target ads while avoiding harmful effects stemming from the overcollection of personal data. Adding data minimization requirements is arguably the most important improvement over CTDPA and other similar state laws. (Section 6)

Sensitive Data Protections. We added critical protections for the most sensitive personal data. Sensitive data (including precise geolocation, health data, data about minors, and more) cannot be sold or used for targeted advertising. While the State Data Privacy Act largely moves away from a consent-based system, we kept requirements for affirmative consent when sensitive data changes hands. (Section 1, Section 6)

Clarity on Advertising Rules. Much of the debate around privacy laws comes down to the types of data that are available to use for targeted advertising. The State Data Privacy Act sets forth clear definitions of the different forms of online advertising, aiming to give businesses flexibility to advertise while protecting privacy. Read more below in "Can businesses still advertise?" (Section 1, Section 4, Section 6)

Enforcement. Existing bills mainly rely on state Attorneys General (AG) to enforce privacy protections. AG offices often have limited resources to conduct investigations and enforce the law. Leaving enforcement solely in the hands of under-resourced state AGs makes it much more likely that state privacy laws will be under-enforced—and businesses may be willing to take the risk of not complying with the law because they know that their state AG is unlikely to have the time, money, or staff to investigate violations. Instead, consumers who have been harmed by violations of the law should have the ability to take action to protect themselves, so the State Data Privacy Act includes a private right of action. The bill proposes a compromise that exempts small businesses from the private right of action in recognition of the fact that small businesses often collect less personal data and have fewer resources to implement new legal compliance programs. This narrower private right of action is the best way to protect consumers' privacy while preserving state resources and protecting small businesses. (Section 12)

Enhanced Protections for Children and Teens. The State Data Privacy Act includes enhanced privacy protections for minors under 18 years of age. Targeted advertising to minors is prohibited, as is already law in Maryland. The sale of minors' personal data is also banned. Any personal data about a minor is considered sensitive data and therefore can only be collected and used if strictly necessary for the product or service the minor is requesting. If transferring such data is strictly necessary, the company must still request consent before the transfer – from the parent for a child under 13, or from the teen themselves for minors ages 13 to 18. Note that this bill was updated in April 2025 to change the knowledge standard for determining when a controller "knows" a user is a minor to "knew or should have known, based on knowledge fairly implied under objective circumstances." (Section 1, Section 6)

Removed Loopholes that Exempt Big Institutions. CTDPA and most state privacy laws provide entity-level exemptions to any business that already comply with federal privacy laws involving health, finance, or education. In an ideal world, many advocates would like to see all of these exemptions removed (particularly because most existing federal privacy laws are decades old and do not provide the level of protection in the State Data Privacy Act). Still, we recognize that some compromises on narrowly tailored exemptions for already-regulated data may be necessary to ease compliance burdens for businesses. To that end, we included narrow, data-level exemptions for the *data* covered by existing federal law rather than exempting an entire entity simply because some personal data they handle falls under existing law. The personal data collected from a consumer who visits a hospital's website shouldn't be without protection simply because the hospital has to comply with federal privacy laws for its health data. (Section 3)

Definitions. Definitions are the core of any comprehensive bill. After discussions in many states, we've solidified important definitions like "targeted advertising" and "sensitive data." We added a few useful definitions for clarity, including "small business" and "third party." (Section 1)

Note: In June 2023, Connecticut passed amendments to the CTDPA, primarily focused on consumer health data and protections for minors. The State Data Privacy Act integrates some, but not all, of these amendments.

Where are the compromises? Businesses can still thrive while also protecting privacy.

The debate over privacy legislation is often seen as a conflict between consumer privacy advocates on one side and Big Tech on the other. Small businesses are often caught in the middle, wanting to protect their customers but reliant on the digital advertising models offered to them by ad giants. The State Data Privacy Act aims to resolve these conflicts by proposing compromises on what are often the most contentious issues. These compromises balance the needs of businesses, consumers, and legislators alike.

The Problem	Our Compromise
Compliance with varying state laws. Many existing state privacy laws need to be stronger, but companies are concerned with keeping up with many differing state laws.	The Connecticut Data Privacy Act is the base text of the State Data Privacy Act, and strong language from existing state privacy laws was used for amendments wherever possible.
Targeted advertising systems are invasive, commodifying and sharing every bit of our personal data, but are often perceived to be critical for businesses to advertise effectively.	Cross-context behavioral advertising is banned by default, but businesses can use the data they collect directly from their customers to target them with ads. Re-targeting is also allowed by default, pursuant to an opt-out.
Marketing measurement. Businesses need to collect data to track the efficacy of their ads and prevent click-farm fraud, but they often use marketing measurement as an excuse to collect personal data.	Legitimate marketing measurement is allowed by default, but consumers can opt out of marketing measurement associated with targeted ads.
Communications with customers. Businesses often wish to communicate with customers, including through sending surveys, to improve their products. Some businesses have expressed concern that privacy laws may prohibit this practice.	Most first-party communications, such as direct mail, email, or text message communications are allowed by default.
Innovation. Businesses want to use personal data to develop new products, but doing so sometimes involves retaining personal data indefinitely.	Companies can de-identify personal data to develop new products.
Consent Fatigue. Informed consent is an important part of consumer protection, but excessive consent pop-ups burden businesses and create consent fatigue among consumers.	The data minimization rules limit the collection and use of personal data by default, reducing reliance on consent mechanisms. The universal opt-out provides consumers with a one-click method to express their privacy preferences more easily. The consent requirements that remain are reserved only for particularly high-risk actions, such as transferring sensitive data.
Loyalty programs are helpful marketing tools that many consumers want to participate in, but businesses often use such programs to monetize and share consumers' personal data.	Legitimate loyalty programs are unaffected, with only narrow restrictions on sharing and selling data for unrelated purposes.
Liability of businesses. Companies rely on processors to help operate their business. They don't have perfect oversight over processors, but consumers also need protection from negligent processors who are receiving their personal data.	Businesses and processors must agree on data protection measures and operate under a contract. Processors may not combine data they receive from different businesses. Businesses aren't liable for the mistakes of processors if they provide reasonable oversight.
Data minimization. Data minimization centers the expectations of consumers. However, there are many legitimate behind-the-scenes uses for data that consumers might not expect.	For clarity, the bill includes a list of important behind-the-scenes activities businesses may need to operate, such as legal defense, fraud prevention, or public safety.

Can businesses still advertise? Simplifying digital advertising into three types provides clear rules for businesses.

The digital marketing industry is complex and constantly evolving as businesses develop new advertising tools and strategies. A strong privacy bill should protect consumers from the most invasive forms of digital marketing while allowing businesses to reach potential customers.

The State Data Privacy Act aims to set clear rules for online advertising by breaking it down into three core forms of advertising. The bill provides different rules for each type of advertising based on the privacy risks associated with each type.

1. Contextual advertising. Businesses engage in contextual advertising when they select advertisements to show consumers based on the topic or content of the media surrounding the advertisement. For example, if the NFL pays to place an advertisement for football tickets on the ESPN app, that is contextual advertising. Contextual advertising relies on generalizable inferences that people might be interested in products or services related to the content on the website, app, publication, or search result they are viewing. Contextual advertising may also include using a consumer's general location to show ads for local businesses, events, and services. For example, if a local restaurant opens a new location on the other side of town, that restaurant can advertise to consumers within a 10-mile radius of the new location. Contextual advertising is the most privacy-protective of the three advertising types because the ads consumers see do not vary based on their identities. Contextual advertising is one form of advertising permitted under the State Data Privacy Act.

2. First-party advertising. Businesses engage in first-party advertising when they advertise in their own store, on their own website or app, or communicate directly with consumers through mail, email, or text messaging using data they collect. For example, suppose a retailer collects order information or website views as permitted under the data minimization rules. As long as that data does not include sensitive data, the first party may use that data to advertise. This type of advertising aligns with what consumers expect. Most consumers understand that when they browse a company's website and make a purchase, that company is collecting data about what consumers did on the site. First-party advertising is permitted in the State Data Privacy Act.

3. Targeted advertising. There are varying forms of targeted advertising, all with different levels of risk to privacy and data security. In the interest of drafting a strong bill that prevents the worst data abuses, the State Data Privacy Act distinguishes between the primary methods of targeted advertising and sets different levels of data protection for each.

Cross-contextual behavioral advertising requires tracking consumers everywhere they go online (often without their knowledge) and building invasive profiles based on that data to target them with ads. An example is the Meta Pixel, which is embedded on many websites and automatically sends consumers' browsing history to Meta. By including data collected over time and across websites as a category of sensitive data, the State Data Privacy and Protection Act bans this invasive practice.

Retargeting is what most people think of when they think of targeted ads. Retargeting involves targeting consumers who visited a website with ads elsewhere online. If a consumer views sneakers on a retailer's website and that retailer then targets that consumer with ads for those same sneakers on third-party websites, that type of advertising is retargeting. Retargeting is permitted under the State Data Privacy Act, though consumers can opt out of this type of targeted advertising, including (for those with a generalized preference not to receive retargeted ads) through universal opt-out signals.

Targeted advertising relies on both:

- ✔ Profiling of an individual or group
- ✔ Targeting based on third-party data

Targeted advertising does not include:

- ✘ Contextual advertising
- ✘ First-party advertising

While many privacy advocates like us ultimately want to see stricter limits placed on first-party and targeted advertising, this tiered structure is a realistic starting point. It ensures businesses have plenty of methods of marketing themselves to potential consumers while protecting consumers from the use of their personal data in the most unexpected and harmful ways.

The State Data Privacy Act provides state lawmakers with the opportunity to protect their constituents.

The State Data Privacy Act is not the model bill that we as consumer privacy advocates would write if we were setting out to write our ideal privacy bill. But it represents a reasonable compromise that gives businesses the consistency they seek across state laws while making the changes that are necessary to ensure that the law actually offers meaningful privacy protections. EPIC and Consumer Reports look forward to working with state lawmakers interested in the State Data Privacy Act.

For a more in-depth dive on the bill, please refer to our section-by-section summary. The summary and versions of this bill are available on CR and EPIC's sites.

[State] Data Privacy Act

Section 1. Definitions.

As used in this chapter, unless the context otherwise requires:
(1) “Affiliate” means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, “control” and “controlled” mean:

(A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company;
(B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or
(C) the power to exercise controlling influence over the management of a company.

(2) “Affirmative Consent” means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a controller, provided:

(A) the request is provided to the consumer in a clear and conspicuous stand-alone disclosure;
(B) the request includes a description of the processing purpose for which the consumer’s consent is sought and:

(1) clearly distinguishes between an act or practice that is necessary to fulfill a request of the consumer and an act or practice that is for another purpose;
(2) clearly states the specific categories of personal data that the controller intends to collect, process, or transfer under each act or practice; and
(3) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable consumer to identify and understand each act or practice;

(C) the request clearly explains the consumer's rights related to consent;
(D) the request is made in a manner reasonably accessible to and usable by consumers with disabilities;
(E) the request is made available to the consumer in each language in which the controller provides a product or service for which authorization is sought;

The definition of consent in existing state laws falls short of requiring clear, specific, and easy to understand requests for consent. The proposed language here is derived from bipartisan federal privacy proposals, including the American Data Privacy and Protection Act and the American Privacy Rights Act.

(F) the option to refuse to give consent is at least as prominent as the option to give consent and the option to refuse to give consent takes the same number of steps or fewer as the option to give consent; and

(G) affirmative consent to an act or practice is not inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller.

"Affirmative Consent" does not include:

(A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(B) hovering over, muting, pausing or closing a given piece of content;

(C) agreement obtained through the use of a false, fraudulent, or materially misleading statement or representation; or

(D) agreement obtained through the use of dark patterns.

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, gait, or other unique biological patterns or characteristics that can be used to identify a specific individual. "Biometric data" does not include:

(A) a digital or physical photograph,

(B) an audio or video recording, or

(C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(5) "Business associate" has the same meaning as provided in HIPAA.

(6) "Child" has the same meaning as provided in COPPA.

(7) "Collect" means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means.

(8) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(9) "Consumer health data" means any personal data that describes or reveals a consumer's past, present, or future physical or mental health

We propose adding "gait," which was included in the Oregon Consumer Privacy Act and California Consumer Privacy Act's definitions of biometric data.

Biometric data is sensitive if it can be used to identify an individual, not only if it affirmatively used to do so. The CT Attorney General recently recommended to the Legislature that they amend CTDPA to make this change. This is also the standard under the Oregon Consumer Privacy Act.

Including a standalone definition of "collect" rather than including it under "processing" allows for different rules for each type of activity. This language was taken from the American Data Privacy and Protection Act with minor adaptation.

The "past, present, or future" standard is taken from Washington's My Health, My Data Act.

condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data;

(10) "Contextual advertising" means displaying or presenting an advertisement that does not vary based on the identity of the individual recipient and is based solely on—

(A) the immediate content of a webpage or online service within which the advertisement appears; or

(B) a specific request of the consumer for information or feedback if displayed in proximity to the results of such request for information;

Provided, however, that a controller may use the following types of personal data to display a contextual advertisement so long as the personal data is not used to make inferences about the consumer, profile the consumer, or for any other purpose, and that the consumer may use technical means to obfuscate or change their physical location and to specify a language preference —

(A) such technical specifications as are necessary for the ad to be delivered and display properly on a given device;

(B) a consumer's immediate presence in a geographic area with a radius no smaller than 10 miles, or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data; or

(C) the consumer's language preferences, as inferred from context, browser settings, or user settings.

(11) "Controller" means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

(12) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(13) "Covered entity" has the same meaning as provided in HIPAA.

(14) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern".

(15) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions that result in access to, or the provision or denial by the controller of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

One key element of this proposed bill is specific definitions for different types of online advertising. We propose adding this definition of contextual advertising to differentiate between more invasive types of advertising subject to data minimization and/or the opt-out.

The phrase "access to" is taken from the Colorado Privacy Act.

(16) “De-identified data” means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data:

(A) takes reasonable physical, administrative, and technical measures to ensure that such data cannot be associated with an individual or be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual,
(B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and
(C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(17) “First party” means a consumer-facing controller with which the consumer intends or expects to interact.

(18) “First-party advertising” means processing by a first party of its own first-party data for the purposes of advertising and marketing and carried out—

(A) through direct communications with a consumer, such as direct mail, email, or text message communications;
(B) in a physical location operated by the first party; or
(C) through display or presentation of an advertisement on the first party’s own website, application or its other online content.

“First-party advertising” includes marketing measurement related to such advertising and marketing.

We propose defining the terms “first party,” “first-party advertising,” and “first-party data” to differentiate first-party advertising from contextual advertising and targeted advertising, which are subject to different rules under the Act.

(19) “First-party data” means personal data collected directly from a consumer by a first party, including based on a visit by the consumer to or use by the consumer of a website, a physical location, or an online service operated by the first party.

(20) “Gender-affirming health care services” means all medical care relating to the treatment of gender dysphoria as set forth in the most recent edition of the American Psychiatric Association's “Diagnostic and Statistical Manual of Mental Disorders” and gender incongruence, as defined in the most recent revision of the “International Statistical Classification of Diseases and Related Health Problems.”

(21) “Gender-affirming health data” means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

(22) “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(23) “Identified or identifiable individual” means an individual who can be readily identified, directly or indirectly.

(24) “Marketing measurement” means measuring and reporting on marketing performance or media performance by the controller, including

processing personal data for measurement and reporting of frequency, attribution, and performance.

(25) “Minor” means any consumer who is younger than 18 years of age.

Adding a definition for “minor” clarifies that all personal data of individuals under 18 is inherently sensitive.

(26) “Person” means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

(27) “Personal data” means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked or reasonably linkable to an individual. “Personal data” does not include de-identified data or publicly available information.

(28) “Precise geolocation data” means information derived from technology, including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals with precision and accuracy within a radius of one thousand seven hundred fifty feet. “Precise geolocation data” does not include the content of communications, a photograph or video, metadata associated with a photograph or video that cannot be linked to an individual, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(29) “Process” and “processing” mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion or modification of personal data.

(30) “Processor” means a person who collects, processes, or transfers personal data on behalf of, and at the direction of, a controller or another processor, or a Federal, State, Tribal, or local government entity.

(31) “Profiling” means any form of processing performed on personal data to evaluate, analyze or predict personal aspects including an individual’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(32) “Protected health information” has the same meaning as provided in HIPAA.

(33) “Publicly available information” means information that has been lawfully made available to the general public from:

(A) federal, state or municipal government records, if the person collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(B) widely distributed media; or

(C) a disclosure to the general public as required by federal, state, or local law.

"Publicly available information" does not include:

(A) Any obscene visual depiction, as defined in section 1460 of title 18, United States Code;

(B) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive data with respect to a consumer;

(C) biometric data;

(D) personal data that is created through the combination of personal data with publicly available information;

(E) genetic data, unless otherwise made publicly available by the individual to whom the information pertains;

(F) information made available by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has restricted the information to a specific audience; or

(G) intimate images, authentic or computer-generated, known to be nonconsensual.

We recommend adding these exclusions to the definition of "publicly available information," because in some instances, the potential privacy risks are likely to outweigh societal benefits of considering this information publicly available. This updated text is largely lifted from the American Privacy Rights Act.

(34) "Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning (A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment, (B) a social, psychological, behavioral or medical intervention, (C) a surgery or procedure, including, but not limited to, an abortion, (D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion, (E) a bodily function, vital sign or symptom, (F) a measurement of a bodily function, vital sign or symptom, or (G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

(35) "Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(36) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include:

(A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(C) the disclosure or transfer of personal data to an affiliate of the controller;

(D) with the consumer's affirmative consent, the disclosure of personal data where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; or

(E) the disclosure of personal data that the consumer:

(i) intentionally made available to the general public via a channel of mass media; and

(ii) did not restrict to a specific audience.

(37) "Sensitive data" means personal data that includes:

(A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, status as transgender or non-binary, union membership, income level or indebtedness, or citizenship or immigration status;

(B) consumer health data;

(C) genetic or biometric data;

(D) personal data of a consumer that a controller knew or should have known, based on knowledge fairly implied under objective circumstances, is a minor;

(E) precise geolocation data;

(F) a government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public;

(G) the online activities of a consumer (or device linked or reasonably linkable to a consumer) over time and across websites, online applications, or mobile applications that do not share common branding, or data generated by profiling performed on such data.

Classifying the online activities of consumers as sensitive data reflects the reality that this type of data is commonly collected outside of consumer's view and transferred to third parties to facilitate "cross-contextual behavioral advertising" and the building of invasive profiles based on this data to target individuals with ads. We propose banning targeted advertising based on this type of data, though less invasive forms of targeted advertising are still permitted.

(38) "Small business" means a controller or processor that meets the following criteria for the period of the 3 preceding calendar years (or for the period during which the controller or processor has been in existence if such period is less than 3 years):

(A) The controller or processor' average annual gross revenues during the period did not exceed $40,000,000, indexed to the Producer Price Index reported by the Bureau of Labor Statistics;

(B) The controller or processor, on average, did not annually collect, process, retain, or transfer the personal data of more than 200,000 individuals during the period for any purpose other than initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product; and

(C) The controller or processor did not transfer personal data to a third party in exchange for revenue, except for purposes of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product.

Added a "small business" definition to exempt small businesses from the private right of action.

(39) “Targeted advertising” means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier (or to a group of consumers or devices identified by unique persistent identifiers), if the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent identifier.

“Targeted advertising” includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such advertisements.

“Targeted advertising” does not include:

(A) first-party advertising; or

(B) contextual advertising.

(40) “Third party” means a person that collects personal data from another person that is not the consumer to whom the data pertains and is not a processor with respect to such data. “Third party” does not include a person that collects personal data from another entity if the two entities are affiliates.

(41) “Trade secret” has the same meaning as provided in *[insert reference to state’s trade secret definition]*

(42) “Transfer” means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party orally, in writing, electronically, or by any other means.

(43) "Unique persistent identifier" means a technologically created identifier to the extent that such identifier is reasonably linkable to a consumer or a device that identifies or is linked or reasonably linkable to 1 or more consumers, including device identifiers, Internet Protocol addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer numbers, unique pseudonyms, user aliases, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to 1 or more consumers or devices. The term "unique persistent identifier" does not include an identifier assigned by a controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by a consumer with respect to the collecting, processing, and transfer of personal data or otherwise limiting the collecting, processing, or transfer of personal data.

Section 2. Applicability.

The provisions of this chapter apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year:
(a) Collected or processed the personal data of not less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
(b) collected or processed the personal data of not less than 10,000 consumers and derived more than 20 per cent of their gross revenue from the sale of personal data.

The applicability threshold of 35,000 consumers is from Delaware's and New Hampshire's privacy laws but can be adjusted based on state population.

Section 3. Scope.

(a) The provisions of this chapter do not apply to any Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state.
(b) The following information and data is exempt from the provisions of this chapter:

(1) protected health information that a covered entity or business associate collects or processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with HIPAA and regulations promulgated under HIPAA;
(2) patient-identifying information for purposes of 42 USC 290dd-2;
(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46;
(4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;
(5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law;
(6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.;

This data-level exemption for HIPAA-covered entities mirrors the standard under the Oregon Consumer Privacy Act.

(7) patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time;
(8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;
(9) Personal information collected, processed, or sold subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.;
(10) 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, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time;
(11) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time;
(12) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time;
(13) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time;
(14) data collected, processed, or maintained

(A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role,
(B) as the emergency contact information of an individual under this chapter used for emergency contact purposes, or
(C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and

(15) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Federal Aviation Act of 1958, 49 USC 40101 et seq., to the extent this chapter is preempted by the Federal Aviation Act of 1958, and

In an ideal world, advocates would like to see some of these exemptions removed. The CT law exempted many entities, which we either struck or changed to data-level exemptions. Where there are not preexisting federal privacy laws that cover the entity in question (e.g. nonprofits), we do not believe these entities should be exempt. In cases where there are preexisting federal privacy laws (e.g. financial institutions, hospitals), we believe data-level exemptions are more appropriate. We recommend that states evaluate each exemption and determine whether its inclusion is necessary in their state. Some states, for example, may determine that they do not need an exemption for data covered by the Driver's Privacy Protection Act or Farm Credit Act

the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to this chapter.

Section 4. Consumer rights.

(a) A consumer shall have the right to:

(1) Confirm whether or not a controller is collecting or processing the consumer's personal data and access such personal data;

(2) obtain from a controller a list of specific third parties, other than natural persons, to which the controller has transferred either (i) the consumer's personal data; or (ii) any personal data;

(3) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

(4) delete personal data provided by, or obtained about, the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source, and derived data;

(5) obtain a copy of the consumer's personal data collected or processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

(6) opt out of the collection and processing of the personal data for purposes of

(A) targeted advertising,

(B) the sale of personal data, or

(C) profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 5 of this act to exercise the rights of such consumer specified in this section on behalf of the consumer. In the case of personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

The added explanation of what types of personal data are covered by the deletion right clarifies the right and ensures that inferences about the consumer can also be deleted. This addition comes from the Oregon Consumer Privacy Act but is also consistent with the Colorado Privacy Act and the GDPR.

Our proposal allows consumers to designate authorized agents to help them exercise any of the rights under the Act, not just the opt-out. This mirrors the California Consumer Privacy Act. See Consumer Reports' report on the importance of authorized agents here: https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/

(c) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (5), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not require authentication to exercise an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

The provision stating that controllers cannot require consumers to engage in invasive authentication procedures for an opt-out request is consistent with most other states. There is low risk of fraud or consumer harm from unauthenticated opt-outs.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (4) of subsection (a) of this section by deleting the consumer's personal data retained by the controller and retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to this chapter.

Ensuring controllers must delete data and retain a record of the request addresses a loophole present in other state laws that allows data brokers to comply with deletion requests by still retaining consumer data as long as they don't use it. This is confusing for consumers and presents a data leak risk.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

(e) A controller may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in this section through—

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the use of dark patterns.

Banning dark patterns and other unfair and deceptive business practices ensures that controllers can't use these practices to make exercising privacy rights more difficult.

(f) A controller or processor may not collect, process, or transfer personal data in a manner that discriminates against an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of individuals' actual or perceived race, color, sex, sexual orientation, gender identity, disability, religion, ancestry or national origin.

This civil rights language makes clear that data-driven discrimination is illegal and is pulled from a previous draft of the American Privacy Rights Act and from the American Data Privacy and Protection Act.

(g) Subsection (f) does not apply to:

(1) The collection, processing, or transfer of personal data for the sole purpose of:

(A) A controller or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with state or federal law; or

(B) Diversifying an applicant, participant or customer pool; or

(2) A private establishment, as described in 42 United States Code, Section 2000a(e).

Section 5. Authorized agent.

A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to exercise rights specified in subsection (a) of section 4 of this act. A controller shall comply with a request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

Section 6. Actions of controllers.

(a) A controller shall:
(1) Limit the collection, processing, and transfer of personal data to what is reasonably necessary to provide or maintain:

(A) a specific product or service requested by the consumer to whom the data pertains including any routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting;
(B) a communication, that is not an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer; or
(C) a purpose permitted under Section 10 of this Act.

Except with respect to sensitive data, a controller may process or transfer personal data collected under this subsection to provide first-party advertising or targeted advertising; provided, however, that this paragraph does not permit the processing or transfer of personal data for targeted advertising to a consumer who has opted out of such advertising pursuant to section 4, 5, or 6, or to a consumer under circumstances where the controller knew or should have known, based on knowledge fairly implied under objective circumstances, that the consumer is a minor;

(2) not collect, process, or transfer sensitive data concerning a consumer except when such collection, processing, or transfer is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;
(3) not sell sensitive data;
(4) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue, including disposing of personal data in accordance with a retention schedule that requires the deletion of

The ban on sale of sensitive data comes from the Maryland Online Data Privacy Act.

personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred;
(5) not transfer sensitive data concerning a consumer without obtaining the consumer's affirmative consent, or, in the case of the collection or processing of personal data concerning a known child, without collecting or processing such data in accordance with COPPA;
(6) provide an effective mechanism for a consumer to revoke the consumer's affirmative consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's affirmative consent and, upon revocation of such affirmative consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request;
(7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, under circumstances where a controller knew or should have known, based on knowledge fairly implied under objective circumstances, that the consumer is a minor; and
(8) not discriminate or retaliate against a consumer for exercising any of the consumer rights contained in this chapter, or for refusing to agree to the collection or processing of personal data for a separate product or service, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.
(b) Nothing in subdivision (8) of this subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a financial incentive program such as a bona fide loyalty, rewards, premium features, discounts or club card program, provided that the controller may not transfer personal data to a third party as part of such program unless:

(1) The transfer is functionally necessary to enable the third party to provide a benefit to which the consumer is entitled;
(2) the transfer of personal data to the third party is clearly disclosed in the terms of the program; and
(3) the third party uses the personal data only for purposes of facilitating a benefit to which the consumer is entitled and does not process or transfer the personal data for any other purpose.

The sale of personal data shall not be considered functionally necessary to provide a financial incentive program. A controller shall not use financial incentive practices that are unjust, unreasonable, coercive or usurious in nature.

These additional restrictions around financial incentive programs protect legitimate loyalty programs while prohibiting them from being used as a way to evade coverage under this Act or for companies to profit from consumers' personal data in a way that consumers do not reasonably anticipate.

The prohibition on using financial incentive practices that are unjust, unreasonable, coercive or usurious comes from the California Consumer Privacy Act regulations.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes:

(1) The categories of personal data collected and processed by the controller, including a separate list of categories of sensitive data collected and processed by the controller, described in a level of detail that provides consumers a meaningful understanding of the type of personal data collected or processed;

(2) the purpose for collecting and processing each category of personal data the controller collects or processes described in a way that gives consumers a meaningful understanding of how each category of their personal data will be used;

(3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller transfers to third parties, if any, and the purposes for those transfers;

(5) the categories of third parties, if any, to which the controller transfers personal data;

(6) The length of time the controller intends to retain each category of personal data, or, if it is not possible to identify the length of time, the criteria used to determine the length of time the controller intends to retain categories of personal data; and

(7) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

These additional requirements for the level of clarity that privacy notices must meet were taken from the Colorado Privacy Act regulations.

If a controller makes a material change to its privacy notice, the controller shall notify each consumer affected by the material change before implementing the material change with respect to prospectively collected personal data and provide a reasonable opportunity for each consumer to withdraw consent. A controller should provide a reasonable opportunity for each consumer to affirmatively consent to further materially different processing or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy notice to each affected consumer, taking into account available technology and the nature of the relationship.

These additional requirements that controllers must inform consumers about material changes to privacy policies comports with current FTC jurisprudence.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such sales or processing, as well as the manner in which a consumer may exercise the right to opt out of such sales or processing.

(e) (1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means shall take into account the ways in which consumers normally

interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A)

(i) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising, the sale of the consumer's personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and

(ii) Not later than X, allowing a consumer to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer's personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(I) Be consumer-friendly and easy to use by the average consumer; and

(II) Enable the controller to reasonably determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising. For purposes of this subsection, the use of an internet protocol address to estimate the consumer's location shall be considered sufficient to reasonably determine residency.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this subdivision conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's financial incentive program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by

informing the consumer of a change in the price, rate, level, quality, or selection of goods or services, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, processing, sale or transfer of the consumer's personal data.

Section 7. Responsibilities of processors and controllers.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance shall include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

(2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor, in order to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The processor shall adhere to the instructions of the controller and only process and transfer the data it receives from the controller to the extent necessary to provide a service requested by the controller, as set out in the contract. The contract shall also require that the processor:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to

demonstrate the processor's compliance with the obligations in this chapter;

(4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data;

(5) be prohibited from combining personal data that the processor receives from or on behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual; and

(6) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

The prohibition on combining personal data is intended to prevent large processors (e.g. Google) from leveraging their position to further bolster their capacity to surveil individuals across contexts beyond the reasonable expectations or control of consumers. Processors may combine data if necessary to conduct one of the excepted purposes in Section 10 but not for their own profit or business advantage.

(c) A processor shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

(d) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in this chapter.

(e) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under this chapter.

Section 8. Data Protection Assessments.

(a) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment for each of the controller's processing activities that presents such heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(1) The collection or processing of personal data for the purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

(B) financial, physical or reputational injury to consumers,

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or

(D) other substantial injury to consumers; and

(4) the collection or processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify the categories of personal data collected, the purposes for collecting such personal data, whether personal data is being transferred, and identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that are employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) No later than 30 days after completing a data protection assessment under this section, a controller shall submit a report of the data protection assessment or evaluation to the Attorney General. The report must include a summary of the data protection assessment and the controller shall make the summary publicly available in a place that is easily accessible to consumers. Controllers may redact trade secrets or other confidential or proprietary information from the report. The Attorney General may require that a controller disclose any data protection

Requiring controllers to conduct data protection assessments before engaging in certain processing activities protects consumers from potential privacy harms from more risky processing activities. This language is from the Colorado Privacy Act.

Requiring controllers to make a summary of their data protection assessments public allows consumers to review businesses' self-assessments of the risks and benefits of their processing activities. California has endorsed a similar concept through CCPA rulemaking.

assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) A controller shall conduct and document a data protection assessment before initiating a processing activity that presents a heightened risk of harm to a consumer and shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data collected or processed and level of risk presented by the processing, throughout the processing activity's lifecycle in order to: 1) monitor for harm caused by the processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

Section 9. De-identified data.

(a) Any controller in possession of de-identified data shall:

(1) Take technical measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) Nothing in this chapter shall be construed to:

(1) Require a controller or processor to re-identify de-identified data; or

(2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; and

(2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer;

(d) A controller that transfers de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Section 10. Limitations.

(a) Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

This placeholder for state law exemptions helps avoid conflicts with state shield laws.

(1) Comply with federal, state or municipal ordinances or regulations, except as prohibited by [state] law;

(2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;

(4) investigate, establish, exercise, prepare for or defend legal claims;

(5) provide a product or service specifically requested by the consumer;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;

(9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity targeted at or involving the controller or processor or its services, preserve the integrity or

security of systems or investigate, report or prosecute those responsible for any such action;
(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all relevant laws and regulations governing such research, if applicable, and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine,

(A) whether the deletion of personal data requested by a consumer under section 4, subsection (a), subparagraph (4)is likely to provide substantial benefits that do not exclusively accrue to the controller,

(B) the expected benefits of the research outweigh the privacy risks, and

(C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) assist another controller, processor or third party with any of the obligations under this chapter;
(12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is

(A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and

(B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law;

(13) ensure the data security and integrity of personal data as required by this chapter, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;
(14) transfer assets to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the controller's assets, only if the controller, in a reasonable time prior to the transfer, provides an affected consumer with:

(A) A notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies of such entity and

(B) a reasonable opportunity to:

(i) withdraw previously provided consent related to the consumer's personal data, and

(ii) request the deletion of the consumer's personal data;

(15) effectuate a product recall pursuant to federal or state law, or to fulfill a warranty;

(16) conduct medical research in compliance with part 46 of title 45, Code of Federal Regulations, or parts 50 and 56 of title 21, Code of Federal Regulations; or

(17) process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data, including to:

(A) Conduct internal research to develop, improve or repair products, services or technology;

(B) identify and repair technical errors that impair existing or intended functionality; or

(C) perform solely internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(b) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(c) A controller or processor that discloses personal data to a processor or third-party controller in accordance with this chapter shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(d) Nothing in this chapter shall be construed to:

(1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person

(A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or

(B) under *[insert reference to state journalist shield law]*;

(2) apply to any person's collection or processing of personal data in the course of such person's purely personal or household activities;

(3) for private school as defined *[insert reference to state statute defining private school]* and private institutions of higher education as defined by title I of the Higher Education Act of 1965, 20 United States Code, Section 1001 et seq., require deletion of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution; or

Adding this exemption for private schools is necessary because we have removed the nonprofit exemption, so nonprofits are covered under this bill. Private schools need an exemption from the deletion right so that students cannot delete personal data necessary for the functioning of the institution (e.g. grades, test scores).

(4) require the affirmative collection of any personal data with respect to the age of users that a controller is not already collecting in the normal course of business, or require a controller to implement an age gating or age verification functionality.

(e) Personal data collected or processed by a controller pursuant to this section may be collected or processed to the extent that such collection and processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section, or, in the case of sensitive data, strictly necessary to the purposes listed in this section;

(2) limited to what is necessary in relation to the specific purposes listed in this section. Personal data processed pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such processing. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such processing of personal data; and

(3) compliant with section 4, subsection (f).

Adding this reference to Section 4, subsection (f) ensures that collection and processing activities under this Section must also comply with the bill's civil rights protections.

(f) If a controller collects or processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such collection or processing qualifies for the exemption and complies with the requirements in subsection (e) of this section.

Section 11. Rulemaking.

The Attorney General may adopt rules and regulations to implement this Act.

Granting rulemaking authority to the Attorney General helps clarify the scope of the statute when there is ambiguity and allows for updates to interpretations of the statute as technology inevitably evolves.

Section 12. Enforcement.

(a) The Attorney General, a district attorney, or a counsel for a municipality may bring a civil action in the name of the State or on behalf of the residents of the State against a controller or processor that violates this chapter to:

(1) Enjoin the act or practice that is in violation of this chapter;

(2) enforce compliance with this chapter or a rule adopted under this chapter;

(3) obtain damages, civil penalties, restitution or other compensation on behalf of the residents of the State; or

(4) obtain reasonable attorney's fees and other litigation costs reasonably incurred.

(b) A violation of this chapter or a rule adopted under this chapter with respect to the personal data of a consumer constitutes an injury to that consumer. The injured consumer may bring a civil action against the party that commits the violation, provided such party is not a small business. In a civil action brought under this subsection in which a plaintiff prevails, the court may award the plaintiff:

Adding a private right of action ensures that consumers have a way to hold businesses accountable for violating the law. We exempt small businesses here as a compromise position.

(1) Damages in an amount not less than $5,000 per individual per violation, as adjusted annually to reflect an increase in the Consumer Price Index, or actual damages, whichever is greater;

(2) punitive damages;

(3) injunctive relief, including an order that an entity retrieve any personal data transferred in violation of this title;

(4) declaratory relief; and

(5) reasonable attorney's fees and litigation costs.

(c) During the period beginning on X, and ending on X, the Attorney General may, prior to initiating any action for a violation of any provision of this chapter, issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section without further notice. Not later than X, the Attorney General shall submit a report to the X disclosing:

(1) The number of notices of violation the Attorney General has issued;

(2) the nature of each violation;

(3) the number of violations that were cured during the sixty-day cure period; and

(4) any other matter the Attorney General deems relevant for the purposes of such report.

(d) The Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (c) of this section, consider:

(1) The number of violations;

(2) the size and complexity of the controller or processor;

(3) the nature and extent of the controller's or processor's processing activities;

(4) the substantial likelihood of injury to the public;

(5) the safety of persons or property;

(6) whether such alleged violation was likely caused by human or technical error; and

(7) the sensitivity of the data.

(e) A violation of the requirements of this chapter shall constitute an unfair trade practice for purposes of X.

Section 13. Severability.

If any provision of this Act or the application thereof to any person or circumstance is held invalid for any reason in a court of competent jurisdiction, the invalidity does not affect other provisions or any other application of this Act that can be given effect without the invalid provision or application, and for this purpose, the provisions of this Act are declared severable.

Section 14. Deadlines for certain actions.

The first data protection assessments required by Section 8 are required to be completed not later than the first anniversary of the effective date of this Act.

Section 15. Effective date.

This Act takes effect 180 days after enactment.