The Road to A Federal Privacy Law

Last Stop on the American Privacy Revolution’s Cross-Country Road Trip

The Journey Continues

- Especially during the pandemic, data privacy and security has remained a top legislative priority in many states.
- Several bills were introduced last year, many of which could be brought back for consideration this year.
- Top Issues were:
  - Regulating the Sale of Personal Information
  - Regulating Biometrics, including Voice and Facial Recognition Technology

Virginia Consumer Data Protection Act

Virginia Consumer Data Protection Act

- **Signed into law on March 2, 2021**
- **Effective January 1, 2023 (same day as CPRA) but may be amended before it becomes effective**
- **Imports concepts from CCPA and GDPR, but has its own idiosyncrasies**
- **No private right of action (all enforcement through Attorney General)**

Who is Subject to the VCDPA?

- **Those conducting business in Virginia or marketing to Virginians a*nd that meet a personal data threshold***
  - **In a calendar year, control or process personal data of at least 100,000 Virginia consumers, or**
  - **Control or process personal data of at least 25,000 Virginia consumers and derive over 50 percent of gross revenue from the sale of personal data**

- **Does not apply to**
  - **Entities subject to federal privacy laws (GLBA, HIPAA, HITECH)**
  - **Nonprofit organizations**
  - **Institutions of Higher Education**

What Information Is Covered?

Obligations and limitations relate to all **personal data** of the consumer

Personal data = any information that is linked or reasonably linkable to an identifiable natural person

Does not include deidentified or publicly available information

Excludes health and medical information and businesses covered by HIPAA and other state and federal laws

Also differentiates sensitive data:

Personal data REVEALING:

Racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status

Processing of genetic or biometric data for purposes of identifying a person

Personal data collected from a known child

Precise geolocation data

Data Controller Responsibilities

- **Notice**
- **Data Minimization**
- **Reasonable and adequate security safeguards**
- **Data protection assessments**
- **Data processing agreements**

Consumer Privacy Rights Under the VCDPA

- **Access, Correct, Delete, Data Portability**
- **Opt-In**
  - **No processing of sensitive personal data without consent**
- **Opt-out**
  - **Targeted advertising (displaying ads based on personal data obtained across time and nonaffiliated sites/apps)**
  - **Sale of Personal Data (for monetary consideration to a third party)**
  - **Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer**
- **Appeal**

Federal Privacy Laws and Bills

Existing Federal Privacy Bills

A long history …

- 1970: Fair Credit Reporting Act
  - Consumer protection re inaccurate/arbitrary information from credit reporting agencies.
  - No restriction on amount or type of data collected.
- 1974: U.S. Privacy Act
  - Limits federal government collection, use, and dissemination of sensitive personal information

Michael E. Sander
Founder Docket Alarm.; *VP of Analytics*, Fastcase
Twitter: @speedplane
Linked In: linkedin.com/in/speedplane/

(Existing Federal Privacy Bills continued)

• 1974: Family Education Rights and Privacy Act	**Student Records**
• 1978: Right to Financial Privacy Act	**Warrants for Bank Records**
• 1980: Privacy Protection Act	**1st Amendment Privacy Rights**
• 1984: Cable Communications Policy Act	**Cable Subscriber Data**
• 1986: The Electronic Communications Privacy Act	**Wiretap Privacy**
• 1988: Video Privacy Protection Act	**Video Rental History**
– Robert Bork	
• 1991: Telephone Consumer Protection Act	**Telemarketing**
• 1994: Driver's Privacy Protection Act	**DMV Records**
• 1996: Health Ins. Portability and Acc. Act of (HIPAA)	**Medical Records**
• 1998: Children's Online Privacy Protection Act (COPPA)	**12 and Under**
• 1999: Gramm-Leach Bliley Act	**Financial Institutions**
• 2003: CAN-SPAM	**Spam**
• 2003: Fair and Accurate Credit Transactions Act	**Identify Theft / Credit Reports**
• 2003: Do-Not-Call Implementation Act	**Telemarketing**

Federal Privacy Bills

- Many Recent Attempts
  - 2019 S.2637: Mind Your Own Business Act
  - 2019 S.1214: Privacy Bill of Rights Act
  - 2019 S.2968: Consumer Online Privacy Rights Act
  - 2020 S.3456: Consumer Data Privacy and Security Act
  - 2020 S.4626: SAFE DATA Act
- Could 2021 be the year of the Federal Privacy Act?
  - See https://www.natlawreview.com/article/new-federal-privacy-bill-introduced-could-2021-be-year

Michael E. Sander
Founder Docket Alarm.; *VP of Analytics*, Fastcase
Twitter: @speedplane
Linked In: linkedin.com/in/speedplane/

Information Transparency and Personal Data Control Act ("ITPDCA")

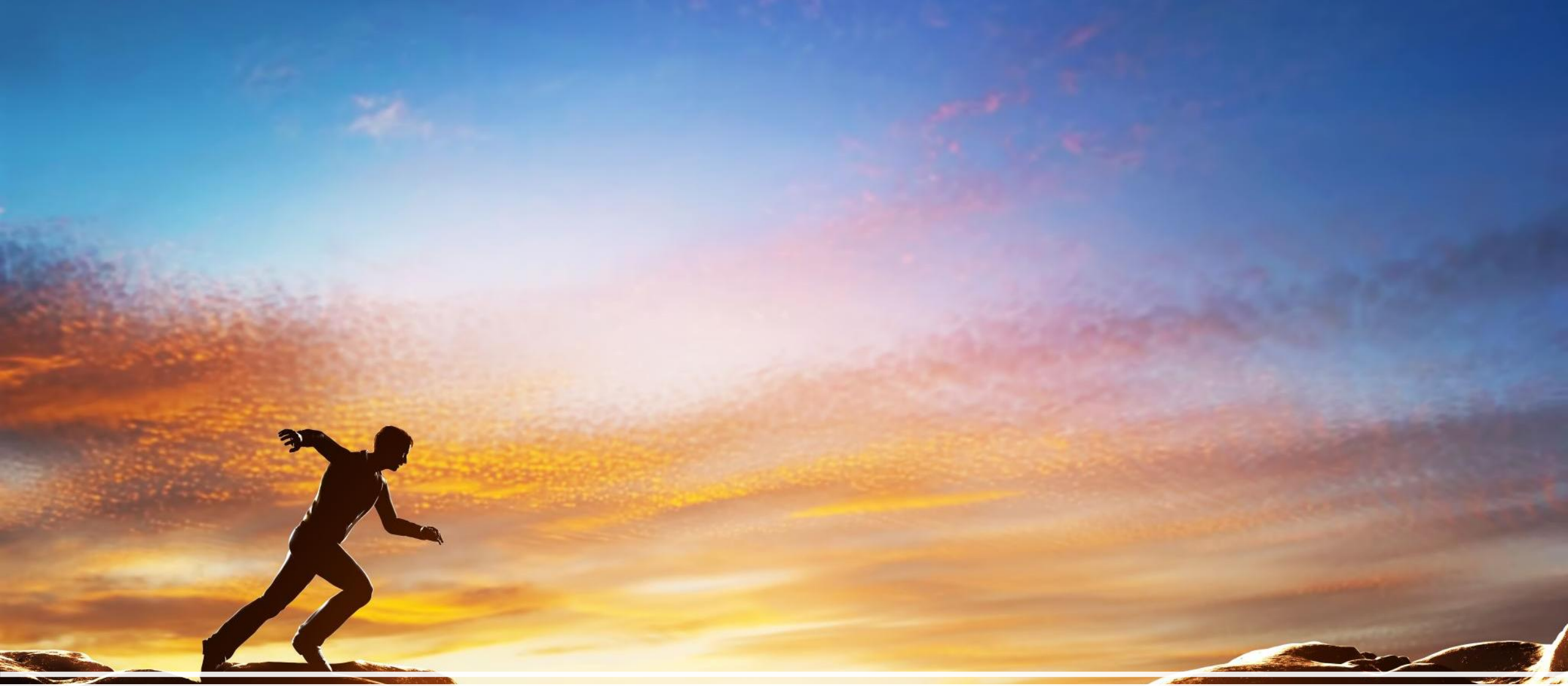
Introduced Mar. 18, 2021 by Rep. Suzan DelBene (D-WA)

- Follows provisions of previous bills:
  - Opt-in prior to sharing PII with third-party;
  - Honor opt-outs;
  - Public privacy policy written in "plain English";
  - Privacy audits if holding >250k individuals' personal data;
  - FTC is regulatory enforcer ($350M funding, 500 new staff);
  - Cannot contract out of obligations.
  - Liability shield for down-stream data misuse.

- Considered more "business friendly" provisions:
  - Preempts stronger state laws
  - No private right of action

See, e.g.,
- DelBene Introduces National Consumer Data Privacy Legislation. Press Release (Mar. 10, 2021);
- Information Transparency and Personal Data Control Act Introduced in Congress, National Law Review, Vol. XI, No. 115 (Apr. 2, 2021)

Michael E. Sander
Founder Docket Alarm.; *VP of Analytics*, Fastcase
Twitter: @speedplane
Linked In: linkedin.com/in/speedplane/

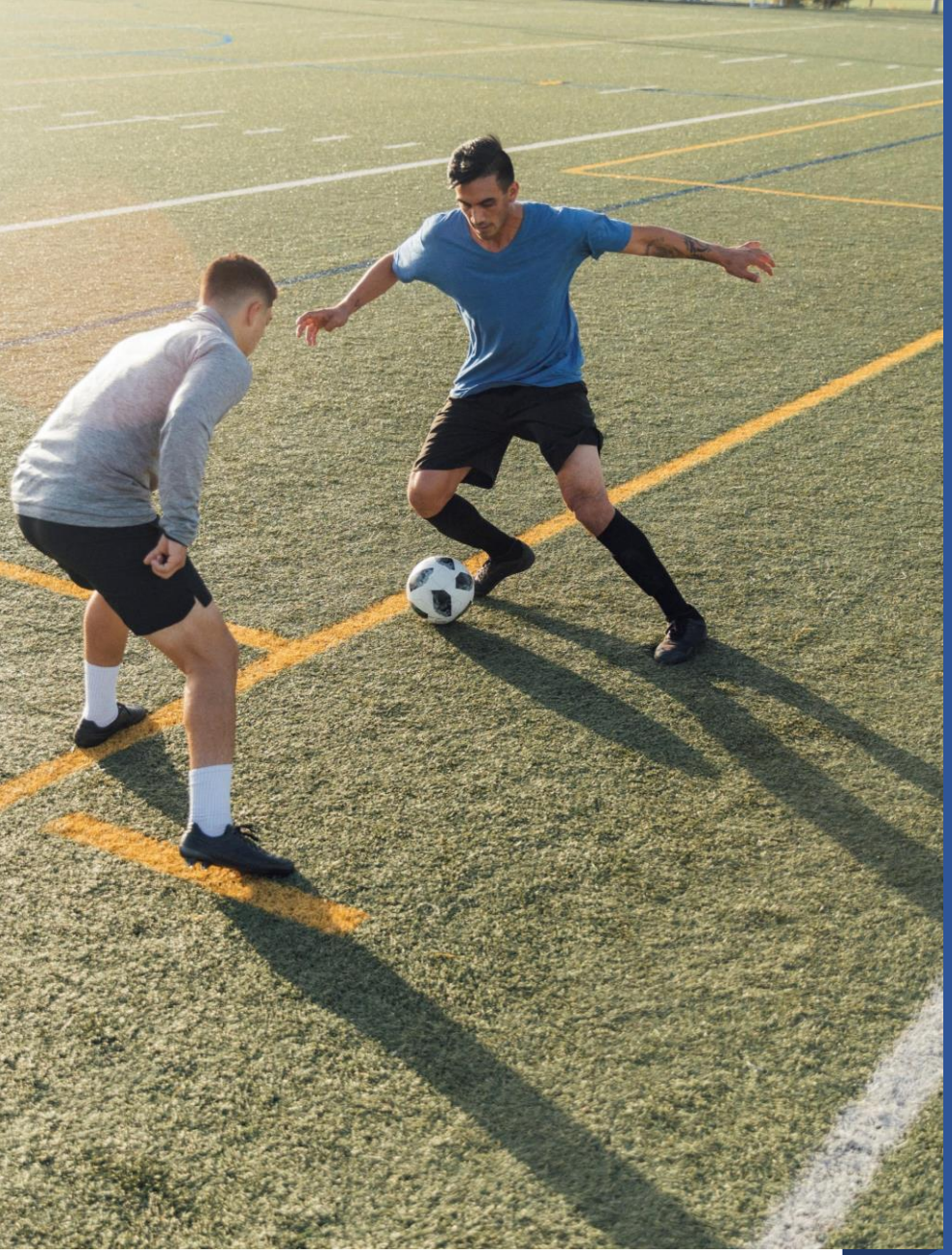


Potential Hurdles for a Federal Privacy Law this year

Artificial Intelligence

- National Security Commission on Artificial Intelligence
  - Final report issued on March 1, 2021.
  - Congressional Hearing held on March 12, 2021, to discuss the findings and recommendations contained in the final report.
  - "The United States retains advantages in critical areas, but current trends are concerning. While a competitive response is complicated by deep academic and commercial interconnections, the United States must do what it takes to retain its innovation leadership and position in the work. The U.S. government must embrace the AI competition and organize to win it by orchestrating and aligning U.S. strengths."*

* Joint Written Testimony of Chair Dr. Eric Schmidt, Vice Chair HON Robert Work, HON Mignon Clyburn, and Mr. Gilman Louie, p. 5, U.S. House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems and the U.S. House Committee on Oversight and Reform Subcommittee on National Security, Joint Hearing Titled: "Final Recommendations of the National Security Commission on Artificial Intelligence", March 12, 2021, available at: https://docs.house.gov/meetings/GO/GO06/20210312/111311/HHRG-117-GO06-Wstate-SchmidtE-20210312.pdf, last visited on 4/27/21.



Artificial Intelligence

- AI needs big data to develop, learn, and grow.
- There is a tension between protecting privacy and ensuring that the US leads in AI.
- "AI tools are critical for U.S. intelligence, homeland security, and law enforcement agencies. Public trust will hinge on justified assurance that government use of AI will respect privacy, civil liberties, and civil rights."**

** Joint Written Testimony of Chair Dr. Eric Schmidt, Vice Chair HON Robert Work, HON Mignon Clyburn, and Mr. Gilman Louie, p. 5, U.S. House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems and the U.S. House Committee on Oversight and Reform Subcommittee on National Security, Joint Hearing Titled: "Final Recommendations of the National Security Commission on Artificial Intelligence", March 12, 2021, available at: https://docs.house.gov/meetings/GO/GO06/20210312/111311/HHRG-117-GO06-Wstate-SchmidtE-20210312.pdf, last visited on 4/27/21.

Cryptocurrency

- Central Bank Digital Currency ("CBDC") is the future of money and another national security issue that has serious privacy implications.
- MIT is currently working with the Boston Fed to construct and test U.S. CBDC or a "digital dollar."
- Several other countries are testing CBDC as well, and China just recently released a digital Yuan.
- On February 24, the Federal Reserve's blog Fed Notes posted an article about the preconditions necessary for a general-purpose CBDC. The post noted 5 "preconditions" which were 1) clear policy objectives, 2) broad stakeholder support, 3) strong legal framework, 4) robust technology, and 5) market readiness.***
- One of the major concerns of CBDC is the lack of privacy and allowing the government to track spending. Issues such as the ability to program the currency for certain purposes (like giving assistance for food that can only be used for food, like a digital food stamp) and issues of access, such as needing a smartphone to be able to access your cash, are being discussed.

***https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm, last visited 4/27/21.

Taxes

- Privacy Laws can create ideal conditions for taxing of digital services, including the sale of data, and establishing the monetary value of data held.
- Namely, by requiring companies to document the data they use from collection to destruction, it provides a road map of how the data trade operates and its value.
- Digital Taxation is a hotly debated issue worldwide. The U.S. is seeking to pursue a global agreement on a digital services tax through the Organization for Economic Cooperation and Development.

Giblin Law PLLC

Annmarie Giblin
AGiblin@GiblinLawPLLC.com
www.GiblinLawPLLC.com

LEGAL INFORMATION

This presentation and its contents may be considered attorney advertising under the rules of certain jurisdictions. Prior results do not guarantee a similar outcome.

This presentation and, the information and materials presented. are for general informational purposes only. Nothing presented constitutes, was meant to constitute, and should not be considered to be legal advice. The material and information is being presented without any representation or warranty whatsoever, including as to the accuracy or completeness of the information. No one should, or is entitled to, rely in any manner on any of the information presented. Parties seeking advice should consult with legal counsel familiar with their specific situation.

This presentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way without the prior written permission of the attorneys presenting it, except that you may download one copy of the materials on a single computer for your personal, non-commercial use, provided you keep all copyright and other proprietary notices intact. We assume no liability or responsibility for any errors or omissions in the content of this presentation and are not responsible for any third-party content that may be accessed through or linked to this presentation.

A00680 Summary:

BILL NO A00680

SAME AS No Same As

SPONSOR Rosenthal L

COSPNSR Quart, Weprin, Rosenthal D, Simon

MLTSPNSR

Add Art 42 1100 - 1110, Gen Bus L

Enacts the NY privacy act to require companies to disclose their methods of de-identifying personal information, to place special safeguards around data sharing and to allow consumers to obtain the names of all entities with whom their information is shared; creates a special account to fund a new office of privacy and data protection.

A00680 Memo:

NEW YORK STATE ASSEMBLY

MEMORANDUM IN SUPPORT OF LEGISLATION

submitted in accordance with Assembly Rule III, Sec 1(f)

BILL NUMBER: A680

SPONSOR: Rosenthal L

TITLE OF BILL:

An act to amend the general business law, in relation to the management and oversight of personal data

PURPOSE:

The purpose of the bill is to address how online platform/social media firms process personal data. The bill, cited as NY Privacy Act, will require the companies to attain consent from consumers before they share and/or sell their information by acting as fiduciary entities.

SUMMARY OF SPECIFIC PROVISIONS:

Section 1 of the bill defines the act as the "New 'York Privacy Act".

Section 2 of the general business law is amended by adding a new article 42.

Section 1100 of the new article 42 provides definitions of relevant terms to be used in this act.

Section 1101 of the new article 42 defines jurisdictional scope as it applies to legal entities that conduct business in New York State or produce products or services intentionally targeted to residents in New York State.

Section 1102 of the new article 42 defines data fiduciary stating that personal data of consumers shall not be used, processed or transferred to a third party, unless the consumer provides express and documented consent.

Section 1103 of the new article 42 defines consumer rights stating that any entity subject to the provisions of this article shall provide notice to consumers of their rights.

Section 1104 of the new article 42 defines transparency stating that controllers shall be transparent and accountable for their personal data by making it available in a form that is reasonably accessible to consumers.

Section 1105 of the new article 42 defines responsibility according to role stating controllers and brokers to be responsible for meeting obligations.

Section 1106 of the new article 42 defines de-identified data stating controller or processor shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject.

Section 1107 of the new article 42 defines exemptions stating the obligations imposed on controllers or processors.

Section 1108 of the new article 42 defines liability stating that it shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

Section 1109 of the new article 42 defines enforcement providing consumer protection from deceptive acts and practices under article twenty-two of this chapter.

Section 1110 of the new article 42 defines preemption stating this article supersedes and preempts laws adopted by any local entity regarding the processing of personal data by controllers and processors.

JUSTIFICATION:

According to a Pew survey from 2018, 69% of American Adults use at least one social media platform, up from 5% in 2005. Americans use these platforms to engage with friends and family, to connect with social and political organizations, and to follow news and current events. Despite the platforms' usefulness, however, many social media users have reservations about how their personal information is used. A 2014 Pew survey found that 91% of Americans believe that people have lost control over how their personal information is collected and used. Some 80% of social media users said they were concerned about advertisers and businesses accessing and using data that they share on social media platforms. Around 64% of people surveyed in this survey also said that government should do more to address this issue. Social media companies' revenues are obtained through targeted advertising based on users' likes, shares, searches, phone numbers, emails, and other information provided while they use these platforms. According to The New York Times, some of the largest social media companies fail to inform or obtain consent from users regarding the sharing of their personal data. It found that in some instances these social media companies share the information of hundreds of millions of users without notifying their consumers. If a user were to choose the most restrictive privacy settings made available, that user's personal data could still be shared with certain external companies or affiliates. What's more, according to these large social media companies, any information share with others on these platforms could be provided to other companies without any additional consent. Currently, there are no federal regulations addressing this privacy issue, and few attempts of self-regulation by these companies have been frail and falls well short of addressing consumers' concerns. Hence, it is imperative that New York joins the increasing number of other states to fill this void.

LEGISLATIVE HISTORY:

2019-20: A.8526- Referred to Consumer Affairs and Protection; S.5642 Referred to Consumer Protection

FISCAL IMPLICATIONS:

None to the State.

EFFECTIVE DATE:
This act shall take effect on the one hundred eightieth day after it shall have become law.

A00680 Text:

STATE OF NEW YORK

680

2021-2022 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 6, 2021

Introduced by M. of A. L. ROSENTHAL, QUART, WEPRIN, D. ROSENTHAL -- read once and referred to the Committee on Consumer Affairs and Protection

AN ACT to amend the general business law, in relation to the management and oversight of personal data

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. Short title. This act may be known and cited as the "New York privacy act".

§ 2. The general business law is amended by adding a new article 42 to read as follows:

ARTICLE 42

NEW YORK PRIVACY ACT

§ 1100. Definitions. The definitions in this article apply unless the context clearly requires otherwise:

1. "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, another legal entity, where the entity holds itself out as affiliated or under common ownership such that a consumer acting reasonably under the circumstances would anticipate their personal data being provided to an affiliate.

EXPLANATION--Matter in ***italics*** (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD00516-01-1

2. "Consent" means a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

3. "Consumer" means a natural person who is a New York resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

4. "Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

5. "Data broker" means a business, or unit or units of a business, separately or together, that earns its primary revenue from supplying data or inferences about people gathered mainly from sources other than the data sources themselves.

6. "De-identified data" means:

(a) data that cannot be linked to a known natural person without additional information not available to the controller; or

(b) data (i) that has been modified to a degree that the risk of re-identification is small as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data, (ii) that is subject to a public commitment by the controller not to attempt to re-identify the data, and (iii) to which one or more enforceable controls to prevent re-identification has been applied. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

7. "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

8. "Identified or identifiable natural person" means a person who can be identified, directly or indirectly, in particular by reference to specific information including, but not limited to, a name, an identification number, specific geolocation data, or an online identifier.

9. "Minor" means any person under eighteen years of age.

10. "Personal data" means information relating to an identified or identifiable natural person.

(a) "Personal data" includes:

(i) an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifier;

(ii) information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other financial information, medical information, mental health information, or health insurance information;

(iii) commercial information, including a record of personal property, income, assets, leases, rentals, products or services purchased, obtained, or considered, or other purchasing or consuming history;

(iv) biometric information, including a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry;

(v) internet or other electronic network activity information, including browsing history, search history, content, including text, photographs, audio or video recordings, or other user generated-content,

non-public communications, and information regarding an individual's interaction with an internet website, mobile application, or advertisement;

(vi) historical or real-time geolocation data;

(vii) audio, electronic, visual, thermal, olfactory, or similar information;

(viii) education records, as defined in section thirty-three hundred two of the education law;

(ix) political information or information on criminal convictions or arrests;

(x) any required security code, access code, password, or username necessary to permit access to the account of an individual;

(xi) characteristics of protected classes under the human rights law, including race, color, national origin, religion, sex, age, or disability; or

(xii) an inference drawn from any of the information described in this paragraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

(b) The term personal data does not include publicly available information. "Publicly available information":

(i) means information that is lawfully made available from federal, state, or local government records; and

(ii) does not include biometric information collected by a covered entity about an individual without the individual's knowledge, or information used for a purpose that is not compatible with the purpose for which the information is maintained and made available in government records.

(c) Personal data does not include de-identified data.

11. "Process" or "processing" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion, or destruction.

12. "Processor" means a natural or legal person who processes personal data on behalf of the controller.

13. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

14. "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

15.(a) "Sale", "sell" or "sold" means the exchange of personal data for consideration by the controller to a third party.

(b) "Sale" does not include the following: (i) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations

considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets, if consumers are notified of the transfer of their data and of their rights under this article and affirmatively consent to the disclosure and transfer of data.

16. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's activities across web sites, applications or online services. It does not include advertising to a consumer based upon the consumer's current visit to a web site, application, or online service, or in response to the consumer's request for information or feedback.

17. "Opt-in" means affirmative, express consent of an individual for a covered entity to use, disclose, or permit access to the individual's personal data after the individual has received explicit notification of the request of the covered entity with respect to that data.

§ 1101. Jurisdictional scope. 1. This article applies to legal entities that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state.

2. This article does not apply to:

(a) state and local governments;

(b) personal data sets to the extent that they are regulated by the federal health insurance portability and accountability act of 1996, the federal health information technology for economic and clinical health act, or the Gramm-Leach-Bliley act of 1999; or

(c) data sets maintained for employment records purposes.

§ 1102. Data fiduciary. 1. Personal data of consumers shall not be used, processed or transferred to a third party, unless the consumer provides express and documented consent. Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.

(a) Every legal entity, or affiliate of such entity, and every controller and data broker to which this article applies shall:

(i) reasonably secure personal data from unauthorized access; and

(ii) promptly inform a consumer of any breach of the duty described in this paragraph with respect to personal data of such consumer.

(b) A legal entity, an affiliate of such entity, controller or data broker may not use personal data, or data derived from personal data, in any way that:

(i) will benefit the online service provider to the detriment of an end user; and

(ii) (A) will result in reasonably foreseeable and material physical or financial harm to a consumer; or

(B) would be unexpected and highly offensive to a reasonable consumer.

(c) A legal entity, or affiliate of such entity, controller or data broker:

(i) may not disclose or sell personal data to, or share personal data with, any other person except as consistent with the duties of care and loyalty under paragraphs (a) and (b) of this subdivision;

(ii) may not disclose or sell personal data to, or share personal data with, any other person unless that person enters into a contract that imposes the same duties of care, loyalty, and confidentially toward the consumer as are imposed under this section; and

(iii) shall take reasonable steps to ensure that the practices of any person to whom the entity, or affiliate of such entity, controller or data broker discloses or sells, or with whom the entity, or affiliate of such entity, controller or data broker shares. Personal data fulfills the duties of care, loyalty, and confidentiality assumed by the person under the contract described in subparagraph (ii) of this paragraph, including by auditing, on a regular basis, the data security and data information practices of any such entity, or affiliate of such entity, controller or data broker.

2. For the purposes of this section the term "privacy risk" means potential adverse consequences to consumers and society arising from the processing of personal data, including, but not limited to:

(a) direct or indirect financial loss or economic harm;

(b) physical harm;

(c) psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

(d) significant inconvenience or expenditure of time;

(e) adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(f) stigmatization or reputational harm;

(g) disruption and intrusion from unwanted commercial communications or contacts;

(h) price discrimination;

(i) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the controller assessing privacy risk, that:

(A) alters that individual's experiences;

(B) limits that individual's choices;

(C) influences that individual's responses; or

(D) predetermines results; or

(j) other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used.

3. The fiduciary duty owed to a consumer under this section shall supersede any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker, to whom this article apples.

§ 1103. Consumer rights. Any entity subject to the provisions of this article shall provide notice to consumers of their rights under this article and shall provide consumers the opportunity to opt in or opt out of processing their personal data in such a manner that the consumer

must select and clearly indicate their consent or denial of consent. Controllers shall facilitate requests to exercise the consumer rights set forth in subdivisions one through six of this section. 1. On request from a consumer, a controller shall confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data concerning the consumer and the names of third parties to whom personal data is sold or licensed. On request from a consumer, a controller shall provide a copy of the personal data undergoing processing free of charge, up to twice annually. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information shall be provided in a commonly used electronic form.

2. On request from a consumer, the controller, without undue delay, shall correct inaccurate personal data concerning the consumer. Taking into account the purposes of the processing, the controller shall complete incomplete personal data, including by means of providing a supplementary statement.

3. (a) On request from a consumer, a controller shall delete the consumer's personal data without undue delay where one of the following grounds applies:

(i) The personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed;

(ii) For processing that requires consent under section eleven hundred five of this article, the consumer withdraws consent to processing;

(iii) The personal data has been unlawfully processed;

(iv) To comply with a legal obligation under federal, state, or local law to which the controller is subject; or

(v) The consumer otherwise requests that the data be deleted.

(b) Where the controller is obliged to delete personal data under this section that has been disclosed to third parties by the controller, including data brokers that received the data through a sale, the controller shall take reasonable steps, which may include technical measures, to inform other controllers that are processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation shall take into account available technology and cost of implementation.

(c) This subdivision does not apply to the extent processing is necessary:

(i) for exercising the right of free speech;

(ii) for compliance with a legal obligation that requires processing by federal, state, or local law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) for reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is processed by or under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(iv) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the

deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing; or

(v) for the establishment, exercise, or defense of legal claims.

4. (a) The controller shall cease processing if one of the following grounds applies:

(i) The accuracy of the personal data is contested by the consumer, for a period enabling the controller to verify the accuracy of the personal data;

(ii) The processing is unlawful and the consumer opposes the deletion of the personal data and requests the restriction of processing instead;

(iii) The controller no longer needs the personal data for the purposes of the processing, but such personal data is required by the consumer for the establishment, exercise, or defense of legal claims; or

(iv) The consumer otherwise requests that the controller cease processing.

(b) Where personal data is subject to a restriction or processing under this subdivision, the personal data shall, with the exception of storage, only be processed (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; or (iii) for reasons of important public interest under federal, state, or local law.

(c) Where a consumer has taken steps by the online selection of options related to sharing personal data a controller is obligated to adhere to such selections.

5. (a) On request from a consumer, the controller shall provide the consumer any personal data concerning such consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i)(A) the processing of such personal data requires consent under section eleven hundred five of this article, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.

(b) Controllers shall transmit the personal data requested under this subdivision directly from one controller to another, where technically feasible, and transmit the personal data to another controller without hindrance from the controller to which the personal data was provided.

(c) Requests for personnel data under this subdivision shall be without prejudice to subdivision three of this section.

(d) The rights provided in this subdivision do not apply to processing necessary for the performance of a task carried out in the public interest and shall not adversely affect the rights of consumers.

6. A consumer shall not be subject to a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer. Legal or similarly significant effects include, but are not limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

(a) This subdivision does not apply if the decision is authorized by federal or state law to which the controller is subject and which incorporates suitable measures to safeguard the consumer's rights and legitimate interests, as indicated by the risk assessments required by section eleven hundred five of this article.

(b) Notwithstanding paragraph (a) of this subdivision, the controller shall implement suitable measures to safeguard consumer's rights and legitimate interests with respect to decisions based solely on profil-

ing, including providing human review of the decision, to express the consumer's point of view with respect to the decision, and to contest the decision.

7. A controller shall communicate any correction, deletion, or restriction of processing carried out in accordance with subdivisions two, three or four of this section to each third-party recipient to whom the personal data has been disclosed, including third parties that received the data through a sale, unless this proves impossible. The controller shall inform the consumer about such third-party recipients, if any, if the consumer requests such information.

8. A controller shall provide information on action taken on a request under subdivisions one through six of this section without undue delay and in any event within thirty days of receipt of the request. That period may be extended by sixty additional days where necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of any such extension within thirty days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the consumer.

(a) If a controller does not take action on the request of a consumer, the controller shall inform the consumer without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) Information provided under this section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request under subdivisions one through six of this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

(d) A controller shall conduct an internal review on any action taken upon request of a consumer under subdivisions one through six of this section.

§ 1104. Transparency. 1. Controllers shall be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that is easily understood and which includes:

(a) the categories of personal data collected by the controller;

(b) the purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) the rights that consumers may exercise pursuant to section eleven hundred three of this article, if any;

(d) the categories of personal data that the controller shares with third parties, if any; and

(e) the names and categories of third parties, if any, with whom the controller shares personal data.

2. Controllers that engage in profiling shall disclose such profiling to the consumer at or before the time personal data is obtained, includ-

ing meaningful information about the logic involved and the significance and envisaged consequences of the profiling.

3. If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, including targeted marketing and profiling to the extent that it is related to such direct marketing, it shall disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and prominent manner.

§ 1105. Responsibility according to role. 1. Controllers and brokers shall be responsible for meeting the obligations set forth under this article.

2. Processors and brokers are responsible under this article for adhering to the instructions of the controller and assisting the controller to meet its obligations under this article.

3. Processing by a processor shall be governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

§ 1106. De-identified data. A controller or processor that uses 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 contractual commitments.

§ 1107. Exemptions. 1. The obligations imposed on controllers or processors under this article do not restrict a controller's or processor's ability to:

(a) comply with federal, state, or local laws;

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

(c) disclose personal data to a law enforcement agency if such information:

(i) was inadvertently obtained by the controller or data broker; and

(ii) appears to pertain to the commission of a crime;

(d) cooperate with a governmental entity if the controller or data broker, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure of personal data without delay;

(e) investigate, exercise, or defend legal claims; or

(f) prevent or detect identity theft, fraud, or other criminal activity or verify identities.

2. The obligations imposed on controllers or processors under this article do not apply where compliance by the controller or processor with this article would violate an evidentiary privilege under New York law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under New York law as part of a privileged communication.

3. A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this article is not in violation of this article, including under section eleven hundred eight of this article, if the third-party recipient processes such personal data in violation of this article, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the third-party recipient intended to commit a violation. A third-party recipient receiving personal data from a controller or processor is likewise not

liable under this article, including under section eleven hundred eight of this article, for the obligations of a controller or processor to whom it provides services.

4. This article does not require a controller or processor to do the following:

(a) re-identify de-identified data;

(b) retain personal data concerning a consumer that he or she would not otherwise retain in the ordinary course of business; or

(c) comply with a request to exercise any of the rights under subdivisions one through six of section eleven hundred three of this article if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

5. Obligations imposed on controllers and processors under this article do not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

§ 1108. Liability. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this article, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

§ 1109. Enforcement. 1. The legislature finds that the practices covered by this article are matters vitally affecting the public interest for the purpose of providing consumer protection from deceptive acts and practices under article twenty-two-A of this chapter. A violation of this article is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying article twenty-two-A of this chapter.

2. The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this article.

3. In addition to any right of action granted to any governmental body pursuant to this section, any person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions. The court may award reasonable attorney's fees to a prevailing plaintiff.

4. Any controller or processor who violates this article is subject to an injunction and liable for damages and a civil penalty. When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity. Each individual whose information was unlawfully processed counts as a separate violation. Each provision of this article that was violated counts as a separate violation.

§ 1110. Preemption. This article supersedes and preempts laws adopted by any local entity regarding the processing of personal data by controllers or processors.

§ 3. This act shall take effect on the one hundred eightieth day after it shall have become a law.

19-0021 Amdt. # 1

November 4, 2019

VIA MESSENGER

RECEIVED

NOV 13 2019

INITIATIVE COORDINATOR
ATTORNEY GENERAL'S OFFICE

Office of the Attorney General
1300 "I" Street, 17th Floor
Sacramento, CA 95814

Attention: Initiative Coordinator

Re: *Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, and Request to Prepare Circulating Title and Summary (Amendment)*

Dear Initiative Coordinator:

On October 9, 2019, I submitted a proposed statewide initiative titled "*The California Privacy Rights and Enforcement Act of 2020,*" Version 3 ("Initiative") and submitted a request that the Attorney General prepare a circulating title and summary pursuant to section 10(d) of Article II of the California Constitution.

Pursuant to Elections Code section 9002(b), I hereby submit timely amendments to the text of the Initiative. As the proponent of the Initiative, I approve the submission of the amended text to the Initiative and I declare that the amendment is reasonably germane to the theme, purpose, and subject of the Initiative. I respectfully request that the Attorney General prepare a circulating title and summary using the amended Initiative (Amendment).

Sincerely,

Alastair Mactaggart

Enclosures
(00393930)

THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Table of Contents

Section 24: ***Establishment of California Privacy Protection Agency***

Section 25: ***Amendment***

Section 26: ***Severability***

Section 27: ***Conflicting Initiatives***

Section 28: ***Standing***

Section 29: ***Construction***

Section 30: ***Savings Clause***

Section 31: ***Effective and Operative Dates***

SEC. 1. Title.

This measure shall be known and may be cited as "The California Privacy Rights Act of 2020."

SEC. 2. Findings and Declarations.

The People of the State of California hereby find and declare all of the following:

A. In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. Voters acted in response to the accelerating encroachment on personal freedom and security caused by increased data collection and usage in contemporary society. The amendment established a legal and enforceable constitutional right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.

B. Since California voters approved the constitutional right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians' privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, but consumers had no right to learn what personal information a business had collected about them and how they used it or to direct businesses not to sell the consumer's personal information.

C. That changed in 2018, when more than 629,000 California voters signed petitions to qualify the California Consumer Privacy Act of 2018 for the ballot. In response to the measure's qualification, the Legislature enacted the California Consumer Privacy Act of 2018 (CCPA) into law. The CCPA gives California consumers the right to learn what information a business has collected about them, to delete their personal information, to stop businesses from selling their personal information, including using it to target them with ads that follow them as they browse the internet from one website to another, and to hold businesses accountable if they do not take reasonable steps to safeguard their personal information.

D. Even before the CCPA had gone into effect, the Legislature considered many bills in 2019 to amend the law, some of which would have significantly weakened it. Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation.

E. Rather than diluting privacy rights, California should strengthen them over time. Many businesses collect and use consumers' personal information, sometimes without consumers' knowledge regarding the business's use and retention of their personal information. In practice, consumers are often entering into a form of contractual arrangement in which while they do not pay money for a good or service, they exchange access to that good or service in return for access to their attention, or access to their personal information. Because the value of the personal information they are exchanging for the good or service is often opaque, depending on the practices of the business, consumers often have no good way to value the transaction. In addition, the terms of agreement or policies in which the arrangements are spelled out, are often complex, unclear, and as a result most consumers never have the time to read or understand them.

F. This asymmetry of information makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses. Unlike in other areas of the economy where consumers can comparison shop, or can understand at a glance if a good or

service is expensive or affordable, it is hard for the consumer to know how much his or her information is worth to any given business, when data use practices vary so widely between businesses.

G. The State therefore has an interest in mandating laws that will allow consumers to understand more fully how their information is being used, and for what purposes. In the same way that ingredient labels on foods help consumers shop more effectively, disclosure around data management practices will help consumers become more informed counterparties in the data economy, and promote competition. Additionally, if a consumer can tell a business not to sell his or her data, then that consumer will not have to scour a privacy policy to see whether the business is, in fact, selling that data, and the resulting savings in time is worth, in the aggregate, a tremendous amount of money.

H. Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights. Consumers should be entitled to a clear explanation of the uses of their personal information, including how it is used for advertising, and to control, correct, or delete it, including by allowing consumers to limit businesses' use of their sensitive personal information to help guard against identity theft, to opt-out of the sale and sharing of their personal information, and to request that businesses correct inaccurate information about them.

I. California is the world leader in many new technologies that have reshaped our society. The world today is unimaginable without the internet, one of the most momentous inventions in human history, and the new services and businesses that arose on top of it -- many of which were invented here in California. One of the most successful business models for the internet has been services that rely on advertising to make money as opposed to charging consumers a fee. Advertising-supported services have existed for generations, and can be a great model for consumers and businesses alike. However, some advertising businesses today use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests. Some companies that do not charge consumers a fee, subsidize these services by monetizing consumers' personal information. Consumers should have the information and tools necessary to limit the use of their information to non-invasive, pro-privacy advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of, if they choose to do so. Absent these tools, it will be virtually impossible for consumers to fully understand these contracts they are essentially entering into when they interact with various businesses.

J. Children are particularly vulnerable from a negotiating perspective with respect to their privacy rights. Parents should be able to control what information is collected and sold or shared about their young children and should be given the right to demand that companies erase information collected about their children.

K. Business should also be held directly accountable to consumers for data security breaches and notify consumers when their most sensitive information has been compromised.

L. An independent watchdog whose mission is to protect consumer privacy should ensure that businesses and consumers are well-informed about their rights and obligations and should vigorously enforce the law against businesses that violate consumers' privacy rights.

SEC. 3. Purpose and Intent.

In enacting this Act, it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy. The implementation of this Act shall be guided by the following principles:

A. Consumer Rights

1. Consumers should know who is collecting their personal information and that of their children, how it is being used, and to whom it is disclosed, so that they have the information necessary to exercise meaningful control over businesses' use of their personal information and that of their children.

2. Consumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to the consumer, and they should have meaningful options over how it is collected, used, and disclosed.

3. Consumers should have access to their personal information and should be able to correct it, delete it, and take it with them from one business to another.

4. Consumers or their authorized agents should be able to exercise these options through easily accessible self-serve tools.

5. Consumers should be able to exercise these rights without being penalized for doing so.

6. Consumers should be able to hold businesses accountable for failing to take reasonable precautions to protect their most sensitive personal information from hackers and security breaches.

7. Consumers should benefit from businesses' use of their personal information.

8. The privacy interests of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses. In addition, this law is not intended to interfere with the right to organize and collective bargaining under the National Labor Relations Act. It is the purpose and intent of the Act to extend the exemptions in this title for employee and business to business communications until January 1, 2023.

B. The Responsibilities of Businesses

1. Businesses should specifically and clearly inform consumers about how they collect and use personal information and how they can exercise their rights and choice.

2. Businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes, and should not further collect, use, or disclose consumers' personal information for reasons incompatible with those purposes.

3. Businesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared.

4. Businesses should provide consumers or their authorized agents with easily accessible means to allow consumers and their children to obtain their personal information, to delete it, or correct it, and to opt-out of its sale and the sharing across business platforms, services, businesses and devices, and to limit the use of their sensitive personal information.

5. Businesses should not penalize consumers for exercising these rights.

6. Businesses should take reasonable precautions to protect consumers' personal information from a security breach.

7. Businesses should be held accountable when they violate consumers' privacy rights, and the penalties should be higher when the violation affects children.

C. Implementation of the Law

1. The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy, while giving attention to the impact on business and innovation. Consumer privacy and the development of beneficial new products and services are not necessarily incompatible goals. Strong consumer privacy rights create incentives to innovate and develop new products that are privacy protective.

2. Businesses and consumers should be provided with clear guidance about their responsibilities and rights.

3. The law should place the consumer in a position to knowingly and freely negotiate with a business over the business' use of the consumer's personal information.

4. The law should adjust to technological changes, help consumers exercise their rights, and assist businesses with compliance, with the continuing goal of strengthening consumer privacy.

5. The law should enable pro-consumer new products and services and promote efficiency of implementation for business, provided that the amendments do not compromise or weaken consumer privacy.

6. The law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy, while giving attention to the impact on business and innovation.

7. Businesses should be held accountable for violating the law through vigorous administrative and civil enforcement.

8. To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.

SEC. 4. Section 1798.100 of the Civil Code is amended to read:

1798.100. General Duties of Businesses that Collect Personal Information

1798.100. (a) ~~A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.~~

~~(b)~~ A business that ***controls the collection of*** ~~collects~~ a consumer's personal information shall, at or before the point of collection, inform consumers as to*:*

(1) the categories of personal information to be collected and the purposes for which the categories of personal information ***are collected or used*** ~~shall be used~~ ***and whether such information is sold or shared.*** A business shall not collect additional categories of personal information or use personal information collected for additional purposes ***that are incompatible with the disclosed purpose for which the personal information was collected,*** without providing the consumer with notice consistent with this section.

(2) if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with notice consistent with this section.

(3) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if such business, acting as a third party, controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information are used, and whether such personal information is sold, in a clear and conspicuous manner at such location.

(c) A business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with such third party, service provider, or contractor, that: (1) specifies that the personal information is sold or disclosed by

the business only for limited and specified purposes; (2) obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title; (3) grants the business rights to take reasonable and appropriate steps to help to ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business's obligations under this title; (4) requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title; (5) grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.

(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.

~~(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.~~

~~(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.~~

~~(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.~~

SEC. 5. Section 1798.105 of the Civil Code is amended to read:

1798.105. Consumers' Right to Delete Personal Information

1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) ***(1)*** A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, ~~and direct~~ ***notify*** any service providers ***or contractors*** to delete the consumer's personal information from their records, ***and notify all third parties to whom the business has sold or shared such personal information, to delete the***

consumer's personal information, unless this proves impossible or involves disproportionate effort.

(2) The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this title.

(3) A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete, and shall notify any of its own service providers or contractors to delete, personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors or third parties who may have accessed such personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.

(d) A business, or a service provider ***or contractor, acting pursuant to its contract with the business, another service provider, or another contractor,*** shall not be required to comply with a consumer's request to delete the consumer's personal information if it is ***reasonably*** necessary for the business, ~~or~~ service provider, ***or contractor*** to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, ***fulfill the terms of a written warranty or product recall conducted in accordance with federal law,*** provide a good or service requested by the consumer, or reasonably anticipated ***by the consumer*** within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) ~~Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.~~ ***Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.***

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

(4) Exercise free speech, ensure the right of another consumer to exercise ~~his or her~~ ***that consumer's*** right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

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

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business ***and compatible with the context in which the consumer provided the information***.

(8) Comply with a legal obligation.

~~(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.~~

SEC. 6. Section 1798.106 is added to the Civil Code to read:

1798.106. Consumers' Right to Correct Inaccurate Personal Information

1798.106 (a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer correct such inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's right to request correction of inaccurate personal information.

(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information, as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.

SEC. 7. Section 1798.110 of the Civil Code is amended to read:

1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

1798.110. (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

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

(3) The business or commercial purpose for collecting, ~~or~~ selling, ***or sharing*** personal information.

(4) The categories of third parties ~~with~~ ***to*** whom the business ~~shares~~ ***discloses*** personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to ***subparagraph (B) of*** paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, ***provided that a business shall be deemed to be in compliance with paragraphs (1) through (4) of subdivision (a) of this Section to the extent that the categories of information and the business or commercial purpose for collecting or selling or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs***

(1) through (4) of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) through (4) of subdivision (c) of this Section.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph***s*** (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about ~~that consumer~~ ***consumers***.

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

(3) The business or commercial purpose for collecting, ~~or~~ selling***, or sharing*** personal information.

(4) The categories of third parties ~~with~~ ***to*** whom the business ~~shares~~ ***discloses*** personal information.

(5) ~~The~~ ***That a consumer has the right to request the*** specific pieces of personal information the business has collected about that consumer.

~~(d) This section does not require a business to do the following:~~

~~(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.~~

~~(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.~~

SEC. 8. Section 1798.115 of the Civil Code is amended to read:

1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom

1798.115. (a) A consumer shall have the right to request that a business that sells ***or shares*** the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold ***or shared*** about the consumer and the categories of third parties to whom the personal information was sold ***or shared***, by category or categories of personal information for each ***category of*** third ~~party~~ ***parties*** to whom the personal information was sold ***or shared***.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose ***and the categories of persons to whom it was disclosed for a business purpose***.

(b) A business that sells ***or shares*** personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells ***or shares*** consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold ***or shared***, or if the business has not sold ***or shared*** consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed ~~the~~ consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell ***or share*** personal information about a consumer that has been sold to, ***or shared with,*** the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

SEC. 9. Section 1798.120 of the Civil Code is amended to read:

1798.120. Consumers' Right to Opt-Out of Sale or Sharing of Personal Information

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells ***or shares*** personal information about the consumer to third parties not to sell ***or share*** the consumer's personal information. This right may be referred to as the right to opt-out ***of sale or sharing***.

(b) A business that sells consumers' personal information to, ***or shares it with,*** third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold ***or shared*** and that consumers have the "right to opt-out" of the sale ***or sharing*** of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell ***or share*** the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers ~~between~~ ***at least*** 13 ***years of age*** and ***less than*** 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale ***or sharing*** of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. ~~This right may be referred to as the "right to opt-in."~~

(d) A business that has received direction from a consumer not to sell ***or share*** the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell ***or share*** the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision ~~(a)~~ ***(c)*** of Section 1798.135, from selling ***or sharing*** the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides ~~express authorization~~ ***consent,*** for the sale ***or sharing*** of the consumer's personal information.

SEC. 10. Section 1798.121 is added to the Civil Code to read:

1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

1798.121. (a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the

goods reasonably expected by an average consumer who requests such goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction, unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information, after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.

(d) Sensitive Personal information that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this Section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100.

SEC. 11. Section 1798.125 of the Civil Code is amended to read:

1798.125. Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights

1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

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

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

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

(E) Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.

(2) Nothing in this subdivision prohibits a business, ***pursuant to subdivision (b),*** from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the ~~consumer~~ ***business*** by the consumer's data.

(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale ***or sharing*** of personal information, or the ~~deletion~~ ***retention*** of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is ~~directly~~ ***reasonably*** related to the value provided to the ~~consumer~~ ***business*** by the consumer's data.

(2) A business that offers any financial incentives pursuant to ***this*** subdivision ~~(a)~~, shall notify consumers of the financial incentives pursuant to Section ~~1798.135~~ ***1798.130***.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section ~~1798.135~~ ***1798.130*** ~~which~~ ***that*** clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. ***If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.***

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

SEC. 12. Section 1798.130 of the Civil Code is amended to read:

1798.130. Notice, Disclosure, Correction, and Deletion Requirements

1798.130. (a) In order to comply with Sections 1798.100, 1798.105, ***1798.106,*** 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) ***(A)*** Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, ***or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively,*** including, at a minimum, a toll-free telephone number~~, and if the business maintains an Internet Web site, a Web site address~~. ***A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.***

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.

(2) ***(A)*** Disclose and deliver the required information to a consumer free of charge, ***or correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request,*** within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a

verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information, ***or correct inaccurate personal information or delete personal information,*** within 45 days of receipt of the consumer's request. The time period to provide the required information, ***or to correct inaccurate personal information or delete personal information,*** may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure ***of the required information*** ~~shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and~~ shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business ***may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but*** shall not require the consumer to create an account with the business in order to make a verifiable consumer request, ***provided that if the consumer has an account with the business, the business may require the consumer to use that account to submit a verifiable consumer request.***

(B) The disclosure of the required information shall cover the 12-month period preceding the business's receipt of the verifiable consumer request, provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period and the business shall be required to provide such information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business's obligation to provide such information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.

(3) ***(A) A business that receives a verifiable consumer request pursuant to sections 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent pursuant to sections 1798.110 or 1798.115 to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business's response to a verifiable consumer request, including but not limited to by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate information, or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) through (f) of Section 1798.100, taking into account the nature of the processing.***

(B) For purposes of subdivision (b) of Section 1798.110:

(~~A~~*i*) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

~~(B)~~ ***(ii)*** Identify by category or categories the personal information collected about the consumer ~~in the preceding 12 months~~ ***for the applicable period of time*** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected***; the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, or selling or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.***

(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold ***or shared*** ~~in the preceding 12 months~~ ***during the applicable period of time*** by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold ***or shared*** ~~in the preceding 12 months~~ ***during the applicable period of time*** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold ***or shared***. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose ~~in the preceding 12 months~~ ***during the applicable period of time*** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of ~~third parties~~ ***persons*** to whom the consumer's personal information was disclosed for a business purpose ~~in the preceding 12 months~~ ***during the applicable period of time*** by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its ~~Internet Web site~~ ***Internet website***, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections ***1798.100, 1798.105, 1798.106,*** 1798.110, 1798.115, and 1798.125 and ~~one~~ ***two*** or more designated methods for submitting requests***, except as provided in subparagraph (A) of paragraph (1) of subdivision (a).***

(B) For purposes of subdivision (c) of Section 1798.110~~,~~***: (i)*** a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the

enumerated category or categories in subdivision (c) that most closely describe the personal information collected***; (ii) the categories of sources from which consumers' personal information is collected; (iii) the business or commercial purpose for collecting or selling or sharing consumers' personal information; and (iv) the categories of third parties to whom the business discloses consumers' personal information.***

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold ***or shared*** about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold ***or shared***, or if the business has not sold ***or shared*** consumers' personal information in the preceding 12 months, the business shall ***prominently*** disclose that fact ***in its privacy policy***.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely ~~describe~~ ***describes*** the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections ***1798.100, 1798.105, 1798.106,*** 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

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

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections ***1798.100,*** 1798.110 and 1798.115 shall follow the ~~definition~~ ***definitions*** of personal information ***and sensitive personal information*** in Section 1798.140 ***by describing the categories of personal information using the specific terms set forth in subparagraphs (A) through (K) of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) through (9) of subdivision (ae) of Section 1798.140***.

SEC. 13. Section 1798.135 of the Civil Code is amended to read:

1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

1798.135. (a) A business that ~~is required to comply with Section 1798.120~~ ***sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121*** shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's ~~Internet~~ ***internet*** homepage***(s)***, titled "Do Not Sell ***or Share*** My Personal Information," to an ~~Internet Web page~~ ***internet webpage***

that enables a consumer, or a person authorized by the consumer, to opt-out of the sale ***or sharing*** of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business's internet homepage(s), titled "Limit the Use of My Sensitive Personal Information" that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business's discretion, utilize a single, clearly-labeled link on the business's internet homepage(s), in lieu of complying with paragraphs (1) and (2), if such link easily allows a consumer to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

(4) In the event that a business responds to opt-out requests received pursuant to paragraphs (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.

(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt-out of the business's sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

(2) A business that allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a webpage that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business's sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that: (A) the consent webpage also allows the consumer or a person authorized by the consumer to revoke such consent as easily as it is affirmatively provided; (B) the link to the webpage does not degrade the consumer's experience on the webpage the consumer intends to visit and has a similar look, feel, and size relative to other links on the same webpage; and (C) the consent webpage complies with technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185.

(3) A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

(c) A business ***that is subject to this Section*** shall:

(1) ~~not~~***Not*** require a consumer to create an account ***or provide additional information beyond what is necessary*** in order to direct the business not to sell ***or share*** the consumer's personal information ***or to limit use or disclosure of the consumer's sensitive personal information***.

(2) Include a description of a consumer's rights pursuant to ~~Section~~ ***Sections*** 1798.120 ***and 1798.121***, along with a separate link to the "Do Not Sell ***or Share*** My Personal Information" ***internet webpage and a separate link*** ~~Internet Web page~~ ***to the "Limit the Use of My Sensitive***

Personal Information" internet webpage, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in ~~Section~~ ***Sections*** 1798.120, ***1798.121,*** and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale ***or sharing*** of their personal information ***or limit the use or disclosure of their sensitive personal information***, refrain from selling ***or sharing the consumer's*** personal information ***or using or disclosing the consumer's sensitive personal information*** ~~collected by the business about the consumer~~ ***and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.***

(5) For ~~a consumer who has opted out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information~~ ***consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age, and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age.***

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

~~(b)~~ ***(d)*** Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

~~(c)~~ ***(e)*** A consumer may authorize another person ~~solely~~ to opt-out of the sale ***or sharing*** of the consumer's personal information, ***and to limit the use of the consumer's sensitive personal information,*** on the consumer's behalf, ***including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b) of this Section, indicating the consumer's intent to opt-out,*** and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General, ***regardless of whether the business has elected to comply with subdivision (a) or (b) of this Section. For purposes of clarity, a business that elects to comply with subdivision (a) of this Section may respond to the consumer's opt-out consistent with Section 1798.125.***

(f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use such consumer's

personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from: (1) selling or sharing the personal information; or (2) retaining, using, or disclosing such consumer's personal information: (A) for any purpose other than for the specific purpose of performing the services offered to the business, (B) outside of the direct business relationship between the person and the business, or (C) for a commercial purpose other than providing the services to the business.

(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title, provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.

SEC. 14. Section 1798.140 of the Civil Code is amended to read:

1798.140. Definitions

1798.140. For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business's behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

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

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

~~(c)~~ ***(d)*** "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) ***As of January 1 of the calendar year,*** ~~Has~~ ***had*** annual gross revenues in excess of twenty-five million dollars ($25,000,000) ***in the preceding calendar year***, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys ***or,*** ~~receives for the business's commercial purposes,~~ sells, or shares ~~for commercial purposes, alone or in combination~~ the personal information of ~~50,000~~ ***100,000*** or more consumers ***or,*** households~~, or devices~~.

(C) Derives 50 percent or more of its annual revenues from selling***, or sharing*** consumers' personal information.

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

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

(4) A person that does business in California, that is not covered by paragraphs (1), (2), or (3) and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

~~(d)~~ ***(e)*** "Business purpose" means the use of personal information for the business's ~~or a service provider's~~ operational purposes, or other notified purposes, ***or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185,*** provided that the use of personal information shall be reasonably necessary and proportionate to achieve the ~~operational~~ purpose for which the personal information was collected or processed or for another ~~operational~~ purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to ~~a current interaction with the consumer and concurrent transactions, including, but not limited to,~~ counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) ~~Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.~~ ***Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.***

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

(4) Short-term, transient use, ***including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business,*** provided ***that*** the ***consumer's*** personal information ~~that~~ is not disclosed to another third party and is not used to build a profile about ~~a~~ ***the*** consumer or otherwise alter ~~an individual~~ ***the*** consumer's experience outside the current interaction ***with the business.~~, including, but not limited to, the contextual customization of ads shown as part of the same interaction.~~

(5) Performing services on behalf of the business, ~~or service provider,~~ including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, ~~providing advertising or marketing services,~~ providing analytic services, ***providing storage,*** or providing similar services on behalf of the business ~~or service provider~~.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

~~(6)~~ ***(7)*** Undertaking internal research for technological development and demonstration.

~~(7)~~ ***(8)*** Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

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

~~(f)~~ ***(g)*** "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. ~~"Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.~~

(h) "Consent" means any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

~~(g)~~ ***(i)*** "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

(iii) Retaining, using, or disclosing the information outside of the direct business relationship between the contractor and the business.

(iv) Combining the personal information which the contractor receives pursuant to a written contract with the business with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) "Cross-context ***behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.***

(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation.

~~(h)~~ ***(m)*** "Deidentified" means information that cannot reasonably ***be used to infer information about, or otherwise be linked to, a particular consumer, provided that the business that possesses the information:***

(A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;

(B) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision; and

(C) contractually obligates any recipients of the information to comply with all provisions of this subdivision. ~~Identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:~~

~~(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.~~

~~(2) Has implemented business processes that specifically prohibit reidentification of the information.~~

~~(3) Has implemented business processes to prevent inadvertent release of deidentified information.~~

~~(4) Makes no attempt to reidentify the information.~~

~~(i)~~ ***(n)*** "Designated methods for submitting requests" means a mailing address, email address, ~~Internet Web page~~ ***internet webpage***, ~~Internet Web~~ ***internet web*** portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

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

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

~~(l)~~ ***(p)*** "Homepage" means the introductory page of an ~~Internet Web site~~ ***internet website*** and any ~~Internet Web page~~ ***internet webpage*** where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the ~~notice~~ ***notices*** required by ~~subdivision (a) of Section 1798.145~~ ***this title***, including, but not limited to, before downloading the application.

(q) "Household" means a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s).

~~(m)~~ ***(r)*** "Infer" or "inference" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

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

(t) "Non-personalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation.

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

~~(o)~~ ***(v)*** (1) "Personal Information" means information that identifies, relates to, describes, is ***reasonably*** capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is ***reasonably*** capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any ~~categories of~~ personal information described in subdivision ~~i~~ (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an ~~Internet Web site~~ ***Internet website***, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(2) "Personal information" does not include publicly available information ***or lawfully obtained, truthful information that is a matter of public concern***. For ~~these~~ purposes ***of this paragraph***, "publicly available" means: information that is lawfully made available from federal, state, or local government records, ***or*** ~~if any conditions associated with such~~ information ***that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience***. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. ~~Information is not "publicly available" if that data is used for a purpose that is not~~

~~compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained~~. ~~"Publicly available~~ ***"Personal information"*** does not include consumer information that is deidentified or aggregate consumer information.

(w) "Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations.

~~(p)~~ ***(x)*** "Probabilistic identifier" means the identification of a consumer or a ***consumer's*** device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

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

(z) "Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

~~(r)~~ ***(aa)*** "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

~~(s)~~ ***(ab)*** "Research" means scientific ***analysis***, systematic study and observation, including basic research or applied research that is ***designed to develop or contribute to public or scientific knowledge*** ~~in the public interest~~ and that adheres ***or otherwise conforms*** to all other applicable ethics and privacy laws, ~~or~~ ***including but not limited to*** studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, ***by a business***.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, ***other than as needed to support the research***.

(4) Subject to business processes that specifically prohibit reidentification of the information, ***other than as needed to support the research***.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) ~~Not be used for any commercial purpose.~~

~~(9)~~ Subjected by the business conducting the research to additional security controls ***that*** limit access to the research data to only those individuals ~~in a business~~ as are necessary to carry out the research purpose.

(ac) "Security and Integrity" means the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; (2) to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; and (3) a business to ensure the physical safety of natural persons.

~~(t)~~ ***(ad)*** (1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to ~~another business or~~ a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to***: (i)*** intentionally disclose personal information***;*** or ***(ii)*** ~~uses the business to~~ intentionally interact with a ***one or more*** third ~~party~~ ***parties;*** ~~provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.~~

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information ***or limited the use of the consumer's sensitive personal information*** for the purposes of alerting ~~third parties~~ ***persons*** that the consumer has opted out of the sale of the consumer's personal information ***or limited the use of the consumer's sensitive personal information.; or***

~~(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:~~

~~(i) The business has provided notice that information being used or shared in its terms and conditions consistent with *Section* 1798.135.~~

~~(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.~~

~~(D)~~ ***(C)*** The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with ~~Sections 1798.110 and 1798.115~~ ***this title***. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with ~~Section~~

~~1798.120~~ ***this title***. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(ae) "Sensitive personal information" means: (1) personal information that reveals (A) a consumer's social security, driver's license, state identification card, or passport number; (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer's precise geolocation; (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer's genetic data; and (2)(A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analyzed concerning a consumer's health; or (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) of Section 1798.140 shall not be considered sensitive personal information or personal information.

~~(u)~~ ***(af)*** "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

~~(v)~~ ***(ag) (1)*** "Service provider" means a ~~sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners,~~ ***person*** that processes ***personal*** information on behalf of a business and ~~to~~ which ***receives from or on behalf of*** the business ~~discloses~~ a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the ~~entity receiving the information~~ ***person*** from***: (A) selling or sharing the personal information; (B)*** retaining, using, or disclosing the personal information for any purpose other than for the ~~specific purpose of performing the services~~ ***business purposes*** specified in the contract for the business, ~~or as otherwise permitted by this title,~~ including retaining, using, or disclosing the personal information for a commercial purpose other than ~~providing the services~~ ***the business purposes*** specified in the contract with the business***, or as otherwise permitted by this title; (C) retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business; and (D) combining the personal information which the service provider receives from or on behalf of the business, with personal information which it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this Section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months.***

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for such business purpose, it shall notify the business of such engagement, and the

engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

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

(A) A consumer uses or directs the business to: (i) intentionally disclose personal information; or (ii) intentionally interact with one or more third parties;

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.; or

(C) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this title. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

~~(w)~~ ***(ai)*** "Third party" means a person who is not any of the following:

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

(2) ***A service provider to the business; or***

(3) A contractor.

~~(A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:~~

~~(i) Prohibits the person receiving the personal information from:~~

~~(I) Selling the personal information.~~

~~(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using,~~

~~or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.~~

~~(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.~~

~~(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.~~

~~(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.~~

~~(x)~~ ***(aj)*** "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device ***that is linked to a consumer or family***. For purposes of this subdivision, "family" means a custodial parent or guardian and any ~~minor~~ children ***under 18 years of age*** over which the parent or guardian has custody.

~~(y)~~ ***(ak)*** "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, ~~or~~ by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, ***or by a person who has power of attorney or is acting as a conservator for the consumer,*** and that the business can ~~reasonably~~ verify, ***using commercially reasonable methods,*** pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115, ***to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106,*** if the business cannot verify, pursuant ***to*** this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

SEC. 15. Section 1798.145 of the Civil Code is amended to read:

1798.145. Exemptions

1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business's ability to:

(1) Comply with federal, state, or local laws ***or comply with a court order or subpoena to provide information***.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. ***Law enforcement agencies, including police and sheriff's***

departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information and upon receipt of such direction a business shall not delete the personal information for 90 days, in order to allow the law enforcement agency to obtain a court-issued subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90 day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant, unless the consumer's deletion request is subject to an exemption from deletion under this title.

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

(4) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury, provided that: (A) the request is approved by a high-ranking agency officer for emergency access to a consumer's personal information; (B) the request is based on the agency's good faith determination that it has a lawful basis to access the information on a non-emergency basis; and (C) the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

~~(4)~~ ***(5)*** Exercise or defend legal claims.

~~(5)~~ ***(6)*** Collect, use, retain, sell, ***share,*** or disclose ~~consumer~~ ***consumers' personal*** information that is deidentified or ~~in the~~ aggregate consumer information.

~~(6)~~ ***(7)*** Collect, ~~or~~ sell, ***or share*** a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not ~~permit~~ ***prohibit*** a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110, ***1798.115, 1798.120, 1798.121, 1798.130, and*** ~~to~~ 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

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

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance

Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) ***Personal*** Information collected as part of a clinical trial ***or other biomedical research study*** subject to ***or conducted in accordance with*** the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration, ***provided that such information is not sold or shared in a manner not permitted by this subparagraph, and if it is inconsistent, that participants be informed of such use and provide consent***.

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

(d) ***(1)*** This title shall not apply to ~~the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).~~ ***activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.***

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the Fair Credit Reporting Act.

(3) This subdivision (d) shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed ~~pursuant~~ ***subject*** to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), ***or the Federal Farm Credit Act of 1971 (as amended in 12 U.S.C. Sections 2001 -- 2279cc and implementing regulations, 12 Code of Federal Regulations, Parts 600, et seq.)***. This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(B) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

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

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

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

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

~~(h)~~ ***(i) (1)*** A business that discloses personal information to a service provider ***or contractor in compliance with this title*** shall not be liable under this title if the service provider ***or contractor*** receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider ***or contractor*** intends to commit such a violation. A service provider ***or contractor*** shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title, ***provided that the service provider or contractor shall be liable for its own violations of this title.***

(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt-out of the sale or sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted-in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the third party intends to commit such a violation.

~~(i)~~ ***(j)*** This title shall not be construed to require a business, ***service provider, or contractor*** to***:*** ***(1)*** reidentify or otherwise link information that, ***in the ordinary course of business,*** is not maintained in a manner that would be considered personal information***; (2) retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained; or (3) maintain information in identifiable, linkable or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.***

~~(j)~~ ***(k)*** The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other ~~consumers~~ ***natural persons. A verifiable consumer request for specific pieces of personal information pursuant to Section 1798.110, to delete a consumer's personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business's possession.***

~~(k)~~ ***(l)*** The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

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

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or an independent contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or independent contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (a) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2023.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.

(2) For purposes of this subdivision:

(A) "Independent contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2023.

(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business which the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business, and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth subdivision (b) of Section 1785.42.

(C) "Owner or owners" means a natural person that meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors, or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(C) "Director" means a natural person designated in the articles of incorporation of a business as such or elected by the incorporators and natural persons designated, elected or appointed by any other name or title to act as directors, and their successors.

(D) "Officer" means a natural person elected or appointed by the board of directors of a business to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 inclusive, shall not apply to household data.

(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose an educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment where consumer access, possession or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) "Educational standardized assessment or educational assessment" means a standardized or non-standardized quiz, test, or other assessment used to evaluate students in or for entry to K-12 schools, post-secondary institutions, vocational programs, and postgraduate programs which are accredited by an accrediting agency or organization recognized by the state of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business's use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business's use, disclosure, or sale of that information to produce a physical item such as a school yearbook containing the consumer's photograph if:

(1) The business has incurred significant expense in reliance on the consumer's consent;

(2) Compliance with the consumer's request to opt-out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable; and

(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.

SEC. 16. Section 1798.150 of the Civil Code is amended to read:

1798.150. Personal Information Security Breaches

1798.150. (a) (1) Any consumer whose nonencrypted ~~or~~ ***and*** nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, ***or whose***

email address in combination with a password or security question and answer that would permit access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

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

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. ***The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach.*** No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

SEC. 17. Section 1798.155 of the Civil Code is amended to read:

1798.155. Administrative Enforcement

1798.155. (a) ~~Any business or third-party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.~~

~~(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance~~. Any business, service provider, ***contractor*** or other person that violates this title shall be ~~subject to an injunction and~~ liable for ***an administrative fine of not more than two thousand five hundred dollars ($2,500) for each***

violation, or seven thousand five hundred dollars ($7,500) for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor or other person has actual knowledge is under 16 years of age, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency ~~a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.~~

~~(c)~~ ***(b)*** Any ~~civil penalty~~ ***administrative fine*** assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision ~~(b)~~ ***(a)***, shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts, ~~and~~ the Attorney General ***and the California Privacy Protection Agency*** in connection with this title.

SEC. 18. Section 1798.160 of the Civil Code is amended to read:

1798.160. Consumer Privacy Fund

1798.160. (a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature ***first*** to offset any costs incurred by the state courts in connection with actions brought to enforce this title, ~~and any~~ ***the*** costs incurred by the Attorney General in carrying out the Attorney General's duties under this title***, and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.***

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively ***as follows:***

(1) to offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) after satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows: (A) ninety-one percent (91%) shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk; the principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes; and (B) nine percent (9%) shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with three percent (3%) allocated to each of the following grant recipients: (i) non-profit organizations to promote and protect consumer privacy; (ii) non-profit organizations and public agencies, including school districts, to educate children in the area of online privacy; and (iii) state and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

(c) ~~These funds~~ ***Funds in the Consumer Privacy Fund*** shall not be subject to appropriation or transfer by the Legislature for any other purpose. ~~, unless the Director of Finance determines~~

~~that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.~~

SEC. 19. Section 1798.175 of the Civil Code is hereby reenacted to read:

1798.175. Conflicting Provisions

1798.175. This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

SEC. 20. Section 1798.180 of the Civil Code is hereby reenacted to read:

1798.180. Preemption

1798.180. This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

SEC. 21. Section 1798.185 of the Civil Code is amended to read:

1798.185. Regulations

1798.185. (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating ***or adding*** ~~as needed additional~~ categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision ~~(o)~~ ***(v)*** of Section 1798.140, ***and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) of Section 1798.140,*** in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the ~~definition~~ ***definitions*** of ***"deidentified" and*** ~~unique identifiers~~ ***"unique identifier"*** to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and ~~additional~~ ***adding, modifying, or deleting*** categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130. *The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal Regulations, where such information previously was "protected health information" as defined in Section 160.103 of that title.*

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

passage of this title and as needed thereafter, ***with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.***

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale ***or sharing*** of personal information pursuant to ~~paragraph (1) of subdivision (a) of~~ Section ~~1798.145~~ ***1798.120 and to limit the use of a consumer's sensitive personal information pursuant to Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt-out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.***

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

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

(5) Adjusting the monetary ~~threshold~~ ***thresholds, in January of every odd-numbered year to reflect any increase in the Consumer Price Index,*** in: subparagraph (A) of paragraph (1) of subdivision ~~(c)~~ ***(d)*** of Section 1798.140; ***subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150; subdivision (a) of Section 1798.155; Section 1798.199.25; and subdivision (a) of Section 1798.199.90*** ~~in January of every odd-numbered year to reflect any increase in the Consumer Price Index~~.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial ***incentives*** ~~incentive offerings,~~ within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections ***1798.105, 1798.106,*** 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to ***delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or*** obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received ~~by~~ ***from*** a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(8) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing: (A) how a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information; (B) how concerns regarding the accuracy of the information may be resolved; (C) the steps a business may take to prevent fraud; and (D) if a business rejects a request to

correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.

(9) Establishing the standard to govern a business's determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.

(10) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

(11) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.

(12) Issuing regulations to further define "intentionally interacts," with the goal of maximizing consumer privacy.

(13) Issuing regulations to further define "precise geolocation," such as where the size defined is not sufficient to protect consumer privacy in sparsely populated areas, or when the personal information is used for normal operational purposes, such as billing.

(14) Issuing regulations to define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, such as system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication, provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (A) perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities,

(B) submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with such processing, with the goal

of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.

(17) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

(18) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor, in the absence of a court order, warrant, or subpoena.

(19) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should: (i) ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business; (ii) ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer, and does not require that the consumer provide additional information beyond what is necessary; (iii) clearly represent a consumer's intent and be free of defaults constraining or presupposing such intent; (iv) ensure that the opt-out preference signal does not conflict with other commonly-used privacy settings or tools that consumers may employ; (v) provide a mechanism for the consumer to selectively consent to a business's sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting their preferences with respect to other businesses or disabling the opt-out preference signal globally; and (vi) state that in the case of a page or setting view which the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including (a) a global opt-out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information; (b) a choice to "Limit The Use Of My Sensitive Personal Information"; and (c) a choice titled "Do Not Sell/Do Not Share/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

(C) Issuing regulations, with the goal of strengthening consumer privacy, while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including: (i) determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information; (ii) determining the scope of activities permitted under paragraph (8) of

subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research; (iii) ensuring the functionality of the business's operations; and (iv) ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.

(20) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should: (A) strive to promote competition and consumer choice and be technology neutral; (B) ensure that the business does not respond to an opt-out preference signal by: (i) intentionally degrading the functionality of the consumer experience; (ii) charging the consumer a fee in response to the consumer's opt-out preferences; (iii) making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal; (iv) attempting to coerce the consumer to opt-in to the sale or sharing of their personal information, or the use or disclosure of their sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal, including stating or implying that the consumer will not be able to use the business's products or services, or that such products or services may not function properly or fully; or (v) displaying any notification or pop-up in response to the consumer's opt-out preference signal; and (C) ensure that any link to a webpage or its supporting content that allows the consumer to consent to opt-in: (i) is not part of a popup, notice, banner, or other intrusive design that obscures any part of the webpage the consumer intended to visit from full view, or that interferes with or impedes in any way the consumer's experience visiting or browsing the webpage or website the consumer intended to visit; (ii) does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the website; (iii) does not make use of any dark patterns; and (iv) applies only to the business with which the consumer intends to interact. The regulation should strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.

(21) Review existing California Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this Title. Upon completing its review, the Agency shall adopt a regulation that applies only the more protective provisions of this Title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

(22) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.

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

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

(d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the Act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the Agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this Act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended or reenacted by this Act shall remain in effect and shall be enforceable until the same provisions of this Act become enforceable.

SEC. 22. Section 1798.190 of the Civil Code is amended to read:

1798.190. Anti-Avoidance

1798.190. ***A court or the Agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title: (a) if*** ~~If~~ a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell ***or share,; or (b) if steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use*** ~~a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title~~.

SEC. 23. Section 1798.192 of the Civil Code is amended to read:

1798.192. Waiver

1798.192. Any provision of a contract or agreement of any kind, ***including a representative action waiver,*** that purports to waive or limit in any way ~~a consumer's~~ rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell ***or share*** the consumer's personal information after previously ~~opting out~~ ***opting-out***.

SEC. 24. Section 1798.199.10 et seq. are added to the Civil Code to read as follows:

Establishment of California Privacy Protection Agency

1798.199.10. (a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act. The Agency shall be governed by a five-member board, including the Chair. The Chair and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.

(b) The initial appointments to the Agency shall be made within 90 days of the effective date of the Act adding this section.

1798.199.15. Members of the Agency board shall:

(a) have qualifications, experience and skills, in particular in the areas of privacy and technology, required to perform the duties of the Agency and exercise its powers;

(b) maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act;

(c) remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another;

(d) refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term;

(e) have the right of access to all information made available by the Agency to the Chair;

(f) be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil action under this Title during the member's tenure or during the five-year period preceding the member's appointment; and

(g) be precluded for a period of two years after leaving office, from acting, for compensation, as an agent or attorney for, or otherwise representing any other person in a matter pending before the Agency if the purpose is to influence an action of the Agency.

1798.199.20. Members of the Agency board, including the Chair, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.

1798.199.25. For each day on which they engage in official duties, members of the Agency board shall be compensated at the rate of one hundred dollars ($100), adjusted biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.

1798.199.30. The Agency board shall appoint an executive director who shall act in accordance with Agency policies and regulations and with applicable law. The Agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The Agency may contract for services that cannot be provided by its employees.

1798.199.35. The Agency board may delegate authority to the Chair or the executive director to act in the name of the Agency between meetings of the Agency, except with respect to resolution of enforcement actions and rulemaking authority.

1798.199.40. The Agency shall perform the following functions:

(a) Administer, implement, and enforce through administrative actions, Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code.

(b) On and after the earlier of July 1, 2021, or within six months of the Agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the

purposes and provisions of the California Consumer Privacy Act, including regulations specifying record keeping requirements for businesses to ensure compliance with this title.

(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information.

(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the Agency pursuant to paragraph (15) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.

(e) Provide guidance to consumers regarding their rights under this title.

(f) Provide guidance to businesses regarding their duties and responsibilities under this title, and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.

(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.

(h) Monitor relevant developments relating to the protection of personal information, and in particular, the development of information and communication technologies and commercial practices.

(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.

(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraphs (1), (2), or (3) of subdivision (d) of section 1798.140 may voluntarily certify that they are in compliance with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of such entities available to the public.

(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.

(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction, and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

1798.199.45. Upon the sworn complaint of any person or on its own initiative, the Agency may investigate possible violations of this title relating to any business, service provider, contractor, or person. The Agency may decide not to investigate a complaint or decide to provide a business with a time-period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the Agency may consider: (a) the lack of intent to violate this title; and (b) voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the Agency of the complaint. The Agency shall notify in writing the person who made the complaint of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for such action or non-action.

1798.199.50. No finding of probable cause to believe this title has been violated shall be made by the Agency unless, at least 30 days prior to the Agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the Agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the Agency a written request that the proceeding be public.

1798.199.55. (a) When the Agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The Agency shall have all the powers granted by that chapter. If the Agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars ($2,500) for each violation, or up to seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the Agency determines that no violation has occurred, it shall publish a declaration so stating.

(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

1798.199.60. Whenever the Agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the Agency shall state the reasons in writing for rejecting the decision.

1798.199.65. The Agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records or other items material to the performance of the Agency's duties or exercise of its powers, including but not limited to its power to audit a business's compliance with this title.

1798.199.70. No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.

(b) If the person alleged to have violated this title engages in the fraudulent concealment of his or her acts or identity, the five-year period shall be tolled for the period of the

concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to their duties under this title and knowingly conceals them in performing or omitting to perform those duties, for the purpose of defrauding the public of information to which it is entitled under this title.

(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of filing of the motion to compel until the date the documents are produced.

1798.199.75. (a) In addition to any other available remedies, the Agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the Agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case, depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the Agency. In order to obtain a judgment in a proceeding under this section, the Agency shall show, following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:

(1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.

(2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.

(3) That a demand for payment has been made by the Agency and full payment has not been received.

(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.

1798.199.80. (a) If the time for judicial review of a final Agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the Agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the order or decision, or the order as modified in accordance with a decision on judicial review.

(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.

(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the Agency.

(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the same manner as any other judgment of the court in which it is entered.

(e) The Agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.

(f) The remedy available under this section is in addition to those available under any other law.

1798.199.85. Any decision of the Agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.

1798.199.90. (a) Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation and each violation involving the personal information of minor consumers, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.

(b) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.

(c) The Agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action, and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The Agency may not limit the authority of the Attorney General to enforce this title.

(d) No civil action may be filed by the Attorney General under this Section for any violation of this title after the Agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.

(e) This section shall not affect the private right of action provided for in Section 1798.150.

1798.199.95. (a) There is hereby appropriated from the General Fund of the state to the Agency the sum of five million dollars ($5,000,000) during the fiscal year 2020-2021, and the sum of ten million dollars ($10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the Agency pursuant to this title. The expenditure of funds under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate such additional amounts to the Commission and other agencies as may be necessary to carry out the provisions of this title.

(b) The Department of Finance, in preparing the state budget and the Budget Bill submitted to the Legislature, shall include an item for the support of this title, which item shall indicate all of the following: (1) the amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of such agencies; and (2) the additional amounts required to be appropriated by the Legislature to the Agency to carry out the purposes of this title, as provided for in this section; and (3) in parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars ($10,000,000), adjusted for cost-of-living changes made pursuant to this section.

(c) The Attorney General shall provide staff support to the Agency until such time as the Agency has hired its own staff. The Attorney General shall be reimbursed by the Agency for these services.

1798.199.100. The Agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the Agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.

SEC. 25. Amendment.

(a) The provisions of this Act may be amended after its approval by the voters by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor, provided that such amendments are consistent with and further the purpose and intent of this Act as set forth in Section 3, including amendments to the exemptions in Section 1798.145 if the laws upon which the exemptions are based are amended to enhance privacy and are consistent with and further the purposes and intent of this Act and amendments to address a decision of a California state or federal court holding that a provision of the Act is unconstitutional or preempted by federal law, provided that any further amendments to legislation that addresses a court holding shall be subject to this subdivision.

(b) Notwithstanding Section 1798.199.25, the Legislature may authorize additional compensation for members of the California Consumer Privacy Agency, if it determines that it is necessary to carry out the Agency's functions, by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor.

(c) This section applies to all statutes amended or reenacted as part of this Act, and all provisions of such statutes, regardless of whether this Act makes any substantive change thereto.

(d) The provisions of this Act shall prevail over any conflicting legislation enacted after January 1, 2020. Any amendments to this Act or any legislation that conflicts with any provision of this Act shall be null and void upon passage of this Act by the voters, regardless of the code in which it appears. Legislation shall be considered "conflicting" for purposes of this subdivision, unless the legislation is consistent with and furthers the purpose and intent of this Act as set forth in Section 3.

SEC. 26. Severability.

If any provision of this measure, or part of this measure, or the application of any provision or part to any person or circumstances, is for any reason held to be invalid, the remaining provisions, or applications of provisions, shall not be affected, but shall remain in full force and effect, and to this end the provisions of this measure are severable. If a court were to find in a final, unreviewable judgment that the exclusion of one or more entities or activities from the applicability of the Act renders the Act unconstitutional, those exceptions should be severed and the Act should be made applicable to the entities or activities formerly exempt from the Act. It is the intent of the voters that this Act would have been enacted regardless of whether any invalid provision had been included or any invalid application had been made.

SEC. 27. Conflicting Initiatives.

(a) In the event that this measure and another measure addressing consumer privacy shall appear on the same statewide ballot, the provisions of the other measure or measures shall be deemed to be in conflict with this measure. In the event that this measure receives a greater number of affirmative votes than a measure deemed to be in conflict with it, the provisions of this measure shall prevail in their entirety, and the other measure or measures shall be null and void.

(b) If this measure is approved by the voters but superseded by law by any other conflicting measure approved by voters at the same election, and the conflicting ballot measure is later held invalid, this measure shall be self-executing and given full force and effect.

SEC. 28. Standing.

Notwithstanding any other provision of law, if the State or any of its officials fail to defend the constitutionality of this Act, following its approval by the voters, any other government agency of this State shall have the authority to intervene in any court action challenging the constitutionality of this Act for the purpose of defending its constitutionality, whether such action is in state or federal trial court, on appeal, or on discretionary review by the Supreme Court of California and/or the Supreme Court of the United States. The reasonable fees and costs of defending the action shall be a charge on funds appropriated to the California Department of Justice, which shall be satisfied promptly.

SEC. 29. Construction.

This Act shall be liberally construed to effectuate its purposes.

SEC. 30. Savings Clause.

This Act is intended to supplement federal and state law, where permissible, but shall not apply where such application is preempted by, or in conflict with, federal law, or the California Constitution. The provisions of the Act relating to children under 16 years of age shall only apply to the extent not in conflict with Children's Online Privacy Protection Act.

SEC. 31. Effective and Operative Dates.

(a) This Act shall become effective as provided in subdivision (a) of section 10 of article II of the California Constitution. Except as provided in subdivision (b), this Act shall become operative January 1, 2023, and with the exception of the right of access, shall only apply to personal information collected by a business on or after January 1, 2022.

(b) Subdivisions (m) and (n) of Section 1798.145, Sections 1798.160, 1798.185, 1798.199.10 through 1798.199.40, and 1798.199.95, shall become operative on the effective date of the Act.

(c) The provisions of the California Consumer Privacy Act of 2018, amended or reenacted by this Act, shall remain in full force and effect and shall be enforceable until the same provisions of this Act become operative and enforceable.

(00391006)