FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook

FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency

FOR RELEASE
July 24, 2019

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security


Participants included: FTC Chairman Joe Simons, FTC Commissioners Noah Joshua Phillips and Christine S. Wilson, and Gustav W. Eyler, Director of the Department of Justice Civil Division’s Consumer Protection Branch.

Facebook, Inc. will pay a record-breaking $5 billion penalty, and submit to new restrictions and a modified corporate structure that will hold the company accountable for the decisions it makes about its users’ privacy, to settle Federal Trade Commission charges that the company violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information.

The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers’ privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide. It is one of the largest penalties ever assessed by the U.S. government for any violation.

The settlement order announced today also imposes unprecedented new restrictions on Facebook’s business operations and creates multiple channels of compliance. The order requires Facebook to restructure its approach to privacy from the corporate board-level down, and establishes strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy, and that those decisions are subject to meaningful oversight.

“Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers’ choices,” said FTC Chairman Joe Simons. “The magnitude of the $5 billion penalty and sweeping conduct relief are unprecedented in the history of the FTC. The relief is designed not only to punish future violations but, more importantly, to change Facebook’s entire privacy culture to decrease the likelihood of continued violations. The Commission takes consumer privacy seriously, and will enforce FTC orders to the fullest extent of the law.”
“The Department of Justice is committed to protecting consumer data privacy and ensuring that social media companies like Facebook do not mislead individuals about the use of their personal information,” said Assistant Attorney General Jody Hunt for the Department of Justice’s Civil Division. “This settlement’s historic penalty and compliance terms will benefit American consumers, and the Department expects Facebook to treat its privacy obligations with the utmost seriousness.”

More than 185 million people in the United States and Canada use Facebook on a daily basis. Facebook monetizes user information through targeted advertising, which generated most of the company’s $55.8 billion in revenues in 2018. To encourage users to share information on its platform, Facebook promises users they can control the privacy of their information through Facebook’s privacy settings.

Following a yearlong investigation by the FTC, the Department of Justice will file a complaint on behalf of the Commission alleging that Facebook repeatedly used deceptive disclosures and settings to undermine users’ privacy preferences in violation of its 2012 FTC order. These tactics allowed the company to share users’ personal information with third-party apps that were downloaded by the user’s Facebook “friends.” The FTC alleges that many users were unaware that Facebook was sharing such information, and therefore did not take the steps needed to opt-out of sharing.

In addition, the FTC alleges that Facebook took inadequate steps to deal with apps that it knew were violating its platform policies.

In a related, but separate development, the FTC also announced today separate law enforcement actions against data analytics company Cambridge Analytica, its former Chief Executive Officer Alexander Nix, and Aleksandr Kogan, an app developer who worked with the company, alleging they used false and deceptive tactics to harvest personal information from millions of Facebook users. Kogan and Nix have agreed to a settlement with the FTC that will restrict how they conduct any business in the future.

New Facebook Order Requirements

To prevent Facebook from deceiving its users about privacy in the future, the FTC’s new 20-year settlement order overhauls the way the company makes privacy decisions by boosting the transparency of decision making and holding Facebook accountable via overlapping channels of compliance.

The order creates greater accountability at the board of directors level. It establishes an independent privacy committee of Facebook’s board of directors, removing unfettered control by Facebook’s CEO Mark Zuckerberg over decisions affecting user privacy. Members of the privacy committee must be independent and will be appointed by an independent nominating committee. Members can only be fired by a supermajority of the Facebook board of directors.

The order also improves accountability at the individual level. Facebook will be required to designate compliance officers who will be responsible for Facebook’s privacy program. These compliance officers will be subject to the approval of the new board privacy committee and can be removed only by that committee—not by Facebook’s CEO or Facebook employees. Facebook CEO Mark Zuckerberg and designated compliance officers must independently submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, as well as an annual certification that the company is in overall compliance with the order. Any false certification will subject them to
individual civil and criminal penalties.

The order also strengthens external oversight of Facebook. The order enhances the independent third-party assessor’s ability to evaluate the effectiveness of Facebook’s privacy program and identify any gaps. The assessor’s biennial assessments of Facebook’s privacy program must be based on the assessor’s independent fact-gathering, sampling, and testing, and must not rely primarily on assertions or attestations by Facebook management. The order prohibits the company from making any misrepresentations to the assessor, who can be approved or removed by the FTC. Importantly, the independent assessor will be required to report directly to the new privacy board committee on a quarterly basis. The order also authorizes the FTC to use the discovery tools provided by the Federal Rules of Civil Procedure to monitor Facebook’s compliance with the order.

As part of Facebook’s order-mandated privacy program, which covers WhatsApp and Instagram, Facebook must conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy. The designated compliance officers must generate a quarterly privacy review report, which they must share with the CEO and the independent assessor, as well as with the FTC upon request by the agency. The order also requires Facebook to document incidents when data of 500 or more users has been compromised and its efforts to address such an incident, and deliver this documentation to the Commission and the assessor within 30 days of the company’s discovery of the incident.

Additionally, the order imposes significant new privacy requirements, including the following:

- Facebook must exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook’s platform policies or fail to justify their need for specific user data;
- Facebook is prohibited from using telephone numbers obtained to enable a security feature (e.g., two-factor authentication) for advertising;
- Facebook must provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users;
- Facebook must establish, implement, and maintain a comprehensive data security program;
- Facebook must encrypt user passwords and regularly scan to detect whether any passwords are stored in plaintext; and
- Facebook is prohibited from asking for email passwords to other services when consumers sign up for its services.
Alleged Violations of 2012 Order

The settlement stems from alleged violations of the FTC’s 2012 settlement order with Facebook. Among other things, the 2012 order prohibited Facebook from making misrepresentations about the privacy or security of consumers’ personal information, and the extent to which it shares personal information, such as names and dates of birth, with third parties. It also required Facebook to maintain a reasonable privacy program that safeguards the privacy and confidentiality of user information.

The FTC alleges that Facebook violated the 2012 order by deceiving its users when the company shared the data of users’ Facebook friends with third-party app developers, even when those friends had set more restrictive privacy settings.

In May 2012, Facebook added a disclosure to its central “Privacy Settings” page that information shared with a user’s Facebook friends could also be shared with the apps used by those friends. The FTC alleges that four months after the 2012 order was finalized in August 2012, Facebook removed this disclosure from the central “Privacy Settings” page, even though it was still sharing data from an app user’s Facebook friends with third-party developers.

Additionally, Facebook launched various services such as “Privacy Shortcuts” in late 2012 and “Privacy Checkup” in 2014 that claimed to help users better manage their privacy settings. These services, however, allegedly failed to disclose that even when users chose the most restrictive sharing settings, Facebook could still share user information with the apps of the user’s Facebook friends—unless they also went to the “Apps Settings Page” and opted out of such sharing. The FTC alleges the company did not disclose anywhere on the Privacy Settings page or the “About” section of the profile page that Facebook could still share information with third-party developers on the Facebook platform about an app users Facebook friends.

Facebook announced in April 2014 that it would stop allowing third-party developers to collect data about the friends of app users (“affected friend data”). Despite this promise, the company separately told developers that they could collect this data until April 2015 if they already had an existing app on the platform. The FTC alleges that Facebook waited until at least June 2018 to stop sharing user information with third-party apps used by their Facebook friends.

In addition, the complaint alleges that Facebook improperly policed app developers on its platform. The FTC alleges that, as a general practice, Facebook did not screen the developers or their apps before granting them access to vast amounts of user data. Instead, Facebook allegedly only required developers to agree to Facebook’s policies and terms when they registered their app with the Facebook Platform. The company claimed to rely on administering consequences for policy violations that subsequently came to its attention after developers had already received data about Facebook users. The complaint alleges, however, that Facebook did not enforce such policies consistently and often based enforcement of its policies on whether Facebook benefited financially from its arrangements with the developer, and that this practice violated the 2012 order’s requirement to maintain a reasonable privacy program.

The FTC also alleges that Facebook misrepresented users’ ability to control the use of facial recognition technology with their accounts. According to the complaint, Facebook’s data policy, updated in April 2018, was deceptive to tens of thousands of users.

millions of users who have Facebook’s facial recognition setting called “Tag Suggestions” because that setting was turned on by default, and the updated data policy suggested that users would need to opt-in to having facial recognition enabled for their accounts.

In addition to these violations of its 2012 order, the FTC alleges that Facebook violated the FTC Act’s prohibition against deceptive practices when it told users it would collect their phone numbers to enable a security feature, but did not disclose that it also used those numbers for advertising purposes.

The Commission vote to refer the complaint and stipulated final order to the Department of Justice for filing was 3-2. The Department will file the complaint and stipulated final order in the U.S. District Court for the District of Columbia. Chairman Simons along with Commissioners Noah Joshua Phillips and Christine S. Wilson issued a statement on this matter. Commissioners Rohit Chopra and Rebecca Kelly Slaughter issued separate statements on this matter.

NOTE: The Commission files a complaint when it has “reason to believe” that the named defendants are violating or are about to violate the law and it appears to the Commission that a proceeding is in the public interest. Stipulated final orders have the force of law when approved and signed by the district court judge.

The Federal Trade Commission works to promote competition, and protect and educate consumers. You can learn more about consumer topics and file a consumer complaint online or by calling 1-877-FTC-HELP (382-4357). Like the FTC on Facebook, follow us on Twitter, read our blogs, and subscribe to press releases for the latest FTC news and resources.

PRESS RELEASE REFERENCE:
FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer
FTC Approves Final Settlement With Facebook

Contact Information

MEDIA CONTACTS:
Juliana Gruenwald Henderson
Office of Public Affairs
202-326-2924

Peter Kaplan
Office of Public Affairs
202-326-2334

STAFF CONTACT:
James Kohm
Bureau of Consumer Protection
202-326-2640
Assembly Bill No. 375

CHAPTER 55

An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy.

[Approved by Governor June 28, 2018. Filed with Secretary of State June 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST


The California Constitution grants a right of privacy. Existing law provides for the confidentiality of personal information in various contexts and requires a business or person that suffers a breach of security of computerized data that includes personal information, as defined, to disclose that breach, as specified.

This bill would enact the California Consumer Privacy Act of 2018. Beginning January 1, 2020, the bill would grant a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared. The bill would require a business to make disclosures about the information and the purposes for which it is used. The bill would grant a consumer the right to request deletion of personal information and would require the business to delete upon receipt of a verified request, as specified. The bill would grant a consumer a right to request that a business that sells the consumer’s personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed. The bill would require a business to provide this information in response to a verifiable consumer request. The bill would authorize a consumer to opt out of the sale of personal information by a business and would prohibit the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data. The bill would authorize businesses to offer financial incentives for collection of personal information. The bill would prohibit a business from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized, as specified, to be referred to as the right to opt in. The bill would prescribe requirements for receiving, processing, and satisfying these requests from consumers. The bill would prescribe various definitions for its purposes and would
define “personal information” with reference to a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information. The bill would prohibit the provisions described above from restricting the ability of the business to comply with federal, state, or local laws, among other things.

The bill would provide for its enforcement by the Attorney General, as specified, and would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information, as defined. The bill would prescribe a method for distribution of proceeds of Attorney General actions. The bill would create the Consumer Privacy Fund in the General Fund with the moneys in the fund, upon appropriation by the Legislature, to be applied to support the purposes of the bill and its enforcement. The bill would provide for the deposit of penalty money into the fund. The bill would require the Attorney General to solicit public participation for the purpose of adopting regulations, as specified. The bill would authorize a business, service provider, or 3rd party to seek the Attorney General’s opinion on how to comply with its provisions. The bill would void a waiver of a consumer’s rights under its provisions. The bill would condition its operation on the withdrawal of a specified initiative from the ballot.

The people of the State of California do enact as follows:

SECTION 1. This measure shall be known and may be cited as “The California Consumer Privacy Act of 2018.”
SEC. 2. The Legislature finds and declares that:
(a) In 1972, California voters amended the California Constitution to include the right of privacy among the “inalienable” rights of all people. The amendment established a legal and enforceable 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 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, a California law intended to give Californians the ‘who, what, where, and when’ of how businesses handle consumers’ personal information.
(c) At the same time, California is one of the world’s leaders in the development of new technologies and related industries. Yet the proliferation of personal information has limited Californians’ ability to properly protect and safeguard their privacy. It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information.
As the role of technology and data in the everyday lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information.

Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer’s personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories.

The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.

In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.

People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information. It is possible for businesses both to respect consumers’ privacy and provide a high level transparency to their business practices.

Therefore, it is the intent of the Legislature to further Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

1. The right of Californians to know what personal information is being collected about them.
2. The right of Californians to know whether their personal information is sold or disclosed and to whom.
3. The right of Californians to say no to the sale of personal information.
4. The right of Californians to access their personal information.
5. The right of Californians to equal service and price, even if they exercise their privacy rights.

SEC. 3. Title 1.81.5 (commencing with Section 1798.100) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.5. CALIFORNIA CONSUMER PRIVACY ACT OF 2018

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 collects a consumer’s personal information 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 shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(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.

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 subparagraph (A) of paragraph (5) of subdivision (a) of Section 1798.130, the consumer’s rights to request the deletion of the consumer’s personal information.

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

(d) A business or a service provider shall not be required to comply with a consumer’s request to delete the consumer’s personal information if it is necessary for the business or service provider to maintain the consumer’s personal information in order to:
(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated 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.

(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 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 adheres to all other applicable ethics and privacy laws, when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of 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.

(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.

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 personal information.

(4) The categories of third parties with whom the business shares 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 paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable request from the consumer.

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

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

(5) 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.

1798.115. (a) A consumer shall have the right to request that a business that sells 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 about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells 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 request from the consumer.

(c) A business that sells 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 if the business has not sold 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 personal information about a consumer that has been sold to 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 1798.120.

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. This right may be referred to as the right to opt out.

(b) A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the right to opt out of the sale of their personal information.

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

(d) Notwithstanding subdivision (a), a business shall not sell 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 13 and 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 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.”

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, if the consumer exercises the consumer’s rights under this title.

   (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.

   (2) Nothing in this subdivision prohibits a business 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 by the consumer’s data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion 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 related to the value provided to the consumer by the consumer’s data.
(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.

(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 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

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

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

(1) 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, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable request, but this shall not extend the business’s duty to disclose and deliver the information within 45 days of receipt of the consumer’s request. The time period to provide the required 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 shall cover the 12-month period preceding the business’s receipt of the verifiable 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 shall not require the consumer to create an account with the business in order to make a verifiable request.

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

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

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(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 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 in the preceding 12 months 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 in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. 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 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 to whom the consumer’s personal information was disclosed for a business purpose in the preceding 12 months 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, and update that information at least once every 12 months:

(A) A description of a consumer’s rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, 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.

(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 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 if the business has not sold consumers’ personal information in the preceding 12 months, the business shall disclose that fact.

(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 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 1798.110, 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.

(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 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

1. Provide a clear and conspicuous link on the business’ Internet homepage, titled “Do Not Sell My Personal Information,” to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer’s personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer’s personal information.

2. Include a description of a consumer’s rights pursuant to Section 1798.120, along with a separate link to the “Do Not Sell My Personal Information” Internet Web page 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 1798.120 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 of their personal information, refrain from selling personal information collected by the business about the consumer.

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.

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) 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) A consumer may authorize another person solely to opt out of the sale of the consumer's personal information on the consumer's behalf, 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.

1798.140. For purposes of this title:

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

(c) “Business” means:

1. A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that 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) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
   (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
   (C) Derives 50 percent or more of its annual revenues from selling 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. “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.

(d) “Business purpose” means the use of personal information for the business’ or a service provider’s operational purposes, or other notified purposes, 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.

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

(4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, 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, or providing similar services on behalf of the business or service provider.

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

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

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

(g) “Consumer” means a natural person who is a 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.

(h) “Deidentified” means information that cannot reasonably identify, relate to, describe, or 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) “Designated methods for submitting requests” means a mailing address, email address, Internet Web page, 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) “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) “Homepage” means the introductory page of an Internet Web site and any Internet Web page 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 required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.

(m) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) “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) (1) “Personal information” means information that identifies, relates to, describes, is 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:

(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 (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, 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, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) “Personal information” does not include publicly available information. For these purposes, “publicly available” means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. “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” does not include consumer information that is deidentified or aggregate consumer information.

(p) “Probabilistic identifier” means the identification of a consumer or a 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) “Processing” means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) “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) “Research” means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or 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’ 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.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(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 limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (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 intentionally disclose personal information or uses the business to intentionally interact with a third party, 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 for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s personal information.

(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: services that the service provider performs on the business’ behalf, provided that the service provider also does not sell the personal information.

(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) 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. 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 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).

(u) “Service” or “services” means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) “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, that processes information on behalf of a business and to which 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 from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) “Third party” means a person who is not any of the following:
(1) The business that collects personal information from consumers under this title.

(2) 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:

(A) 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.

(B) 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.

A person covered by paragraph (2) 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 paragraph (2) in compliance with paragraph (2) 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) “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. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, 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 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.

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.
2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
3. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
4. Exercise or defend legal claims.
5. Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
6. Collect or sell 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 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 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) This act shall not apply to protected or health information that is collected by a covered entity governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56 of Division 1)) or governed by the privacy, security, and breach notification rules issued by the federal 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 Availability Act of 1996. For purposes of this subdivision, the definition of “medical information” in Section 56.05 shall apply and the definitions of “protected health information” and “covered entity” from the federal privacy rule shall apply.

(d) 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.).
(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, if it is in conflict with that law.

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

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

1. A time period for a business to respond to any verified consumer request may be extended by up to 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 consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service provider 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 intends to commit such a violation. A service provider 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.

(i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

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

1798.150. (a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ 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 all of the following requirements are met:

(1) Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide 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. 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.

(2) A consumer bringing an action as defined in paragraph (1) of subdivision (c) shall notify the Attorney General within 30 days that the action has been filed.

(3) The Attorney General, upon receiving such notice shall, within 30 days, do one of the following:

(A) Notify the consumer bringing the action of the Attorney General’s intent to prosecute an action against the violation. If the Attorney General does not prosecute within six months, the consumer may proceed with the action.

(B) Refrain from acting within the 30 days, allowing the consumer bringing the action to proceed.

(C) Notify the consumer bringing the action that the consumer shall not proceed with the action.

(c) Nothing in this act 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.

1798.155. 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.

(a) 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, or other person that violates this title shall be liable for a civil penalty as provided in Section 17206 of the Business and Professions Code 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.

(b) Notwithstanding Section 17206 of the Business and Professions Code, any person, business, or service provider that intentionally violates this title may be liable for a civil penalty of up to seven thousand five hundred dollars ($7,500) for each violation.

(c) Notwithstanding Section 17206 of the Business and Professions Code, any civil penalty assessed pursuant to Section 17206 for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (a), shall be allocated as follows:

(1) Twenty percent to the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.109, with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) Eighty percent to the jurisdiction on whose behalf the action leading to the civil penalty was brought.

(d) It is the intent of the Legislature that the percentages specified in subdivision (c) be adjusted as necessary to ensure that any civil penalties assessed for a violation of this title fully offset any costs incurred by the state courts and the Attorney General in connection with this title, including a sufficient amount to cover any deficit from a prior fiscal year.

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 to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General’s duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds 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.
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.

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.

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

1. Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) 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 of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional 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.

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.

4. Establishing rules and procedures for the following, within one year of passage of this title and as needed thereafter:

   A. To facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145.

   B. To govern business compliance with a consumer’s opt-out request.

   C. 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 in subparagraph (A) of paragraph (1) of subdivision (b) of Section 1798.106 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 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 1798.110 and 1798.115 and to facilitate a consumer’s or the consumer’s authorized agent’s ability to 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’ determination that a request for information received by a consumer is a verifiable 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 request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business’ authentication of the consumer’s identity, within one year of passage of this title and as needed thereafter.

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

1798.190. 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, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

1798.192. Any provision of a contract or agreement of any kind 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’ sale of the consumer’s personal information, or authorizing a business to sell the consumer’s personal information after previously opting out.

1798.194. This title shall be liberally construed to effectuate its purposes.

1798.196. This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the California Constitution.

1798.198. (a) Subject to limitation provided in subdivision (b), this title shall be operative January 1, 2020.

(b) This act shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

SEC. 4. (a) The provisions of this bill are severable. If any provision of this bill or its application is held invalid, that invalidity shall not affect
other provisions or applications that can be given effect without the invalid provision or application.