FULLSTEAM OPERATIONS LLC

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

CONSUMER RIGHTS - RESPONSE AND VERIFICATION

POLICY AND PROCEDURES

Revised 11/6/2019

Edward R. Graf, PhD, EJD, CIPP/E, CIPM, CIPP/US
Director Compliance and Contracts
Fullsteam Operations LLC

1. Introduction.

This Consumer Rights - Response and Verification Policy and Procedures ("Policy") provides guidance to Fullsteam Operations LLC and its portfolio companies ("Fullsteam") for compliance with California consumers' rights as mandated by the California Consumer Privacy Act of 2018 ("CCPA"). Signed into law in the summer of 2018, the CCPA creates a variety of new consumer privacy rights which require companies to implement policies and procedures to manage and comply with new consumer-facing responsibilities.

The CCPA grants 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 the information, and the categories of third parties with which the information is shared. It requires a business to make disclosures about the information and the purposes for which it is used. The law grants a consumer the right to request deletion of personal information and requires the business to delete upon receipt of a verified request. The bill grants a consumer a right to request that a business that discloses the consumer's personal information for a business purpose, disclose the categories of information that it collects and categories of information and the identity of third parties to which the information was disclosed. The bill requires a business to provide this information in response to a verifiable consumer request.

When implementing processes and procedures to respond to individuals who invoke their rights under the CCPA, it is important not to overlook the requirement to verify the requestor's identity and the risk that this requirement presents. It is our intent to invoke rules which reasonably weigh the consumer's rights against the possibility of providing information or deleting information as a result of fraud.

Fullsteam does not and has no intention of selling any consumer personal information, thus that topic is not discussed in this Policy.

This Policy will be evaluated annually to ensure its adequacy and relevancy regarding our obligations and responsibilities.

2. Communication with Consumers.

In the interest of efficiency and accuracy, Edward Graf, our Director Compliance and Contracts, will handle all California consumer inquiries about our privacy practices or compliance with the CCPA and associated regulations and will direct consumers on how to exercise their rights thereunder. He was chosen for this role based upon his education, experience and training specifically on the CCPA. He is current on the CCPA and is committed to staying current as it may be amended or interpreted by regulations.

In the event that additional persons are required to meet our obligations, Edward Graf will establish and document a training policy, and monitor his assistants' compliance, to ensure that

his assistants handle all consumer requests correctly and are informed of all the requirements of the CCPA and its applicable regulations.

3. Consumer Rights to Know.

3.1 Under the CCPA, upon receipt of a *verifiable request* by a California consumer, Fullsteam will disclose, provided that it does not come under a Disclosure Exception, defined below, to that consumer the following:

(a) categories of personal information we have collected about that consumer in the 12 months preceding the date of the request.

(b) categories of sources from which the personal information was collected in the 12 months preceding the date of the request.

(c) business or commercial purpose for which the personal information was collected in the 12 months preceding the date of the request.

(d) categories of third parties with whom we shared the personal information in the 12 months preceding the date of the request.

(e) specific pieces of personal information which we have collected about that consumer.

3.2 Not Required. However, we *will not*:

(a) 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; or

(b) 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.

3.3 "Disclosure Exception" listed as follows: We do not collect the sensitive and valuable consumer personal information listed below unless it is necessary to provide the good or perform the services purchased by the consumer. Fullsteam *will never* disclose a consumer's:

(a) Social Security number;

(b) driver's license number or other government-issued identification number;

(c) financial account number or credit/debit card information;

(e) any health insurance or medical identification number;

(f) an account password;

(g) security questions and answers; or

(h) specific pieces of personal information if we believe the disclosure would create a substantial, articulable, and unreasonable risk to:

(1) security of that personal information;

(2) consumer's account with us; or

(3) security of our systems or networks.

4. Consumer Right to Obtain.

Upon receipt of a *verifiable request* by a California consumer, Fullsteam will deliver, provided that it does not come under a Disclosure Exception, free of charge to the consumer, the personal information collected from the consumer. 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.

We will provide personal information to a consumer at any time. However, we are not required to provide personal information to a consumer more than two (2) times in a twelve (12) month period.

5. Consumer Right of Deletion.

5.1 Upon receipt of a *verifiable request* by a California consumer, Fullsteam will delete, if not retained under a Deletion Exception, as listed below, the consumer's personal information from its records and *direct any service providers to delete the consumer's personal information from their records.*

5.2 "Deletion Exception" listed as follows: We *will not* delete the consumer's personal information if it is necessary for us or our service provider to maintain the consumer's personal information in order to:

(a) 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 an ongoing business relationship with the consumer, or otherwise perform a contract between us and the consumer;

(b) detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;

(c) debug to identify and repair errors that impair existing intended functionality;

(d) 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;

(e) 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 attached hereto as Exhibit A;

(f) 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;

(g) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with us;

(h) comply with a legal obligation; or

(i) 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.

6. General Response to Consumer Requests.

Upon receiving a request from a California consumer to know or a request to delete, we will confirm receipt of the request within ten (10) days and provide information about how we will process the request. The information will include our verification process and when the consumer may expect a response.

We will respond to requests to know and requests to delete within forty-five (45) days from the date that we receive the request. If necessary, we may take up to an additional forty-five (45) days to respond to the consumer's request, for a maximum total of ninety (90) days from the date we receive the request. In such instances, we will provide the consumer with notice and an explanation of the reason why we need more than forty-five (45) days to respond to the request.

If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, we will either treat the request as if it had been submitted in our designated manner or provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.

7. Responding to Requests to Know.

If a consumer requests specific pieces of information about the consumer and we cannot verify the identity of the person making the request, we will not disclose any specific pieces of personal information and will inform the consumer that we cannot verify their identity. If the request is denied in whole or in part, we will also evaluate the consumer's request as if he/she were seeking the disclosure of categories of personal information.

If the consumer request the disclosure of categories of personal information about the consumer, and we cannot verify the identity of the person making the request, we may deny the request to disclose the categories and other information requested and will inform them that we cannot verify their identity. If the request is denied in whole or in part, we will provide an individualized response to the consumer and not only direct the consumer to our privacy policy.

If we deny a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, we will inform the requestor and explain the basis for the denial. If the request is denied only in part, we will disclose the other information sought by the consumer.

We will use reasonable security measures when transmitting personal information to the consumer.

If we have a password-protected account with the consumer, we may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to receive.

In responding to a verified request to know categories of personal information collected, we will provide, in a meaningful way, the:

(a) categories of sources from which the personal information was collected;

(b) business or commercial purpose for which we collected the personal information;

(c) categories of third parties to whom we disclosed the categories of personal information; and

(d) business or commercial purpose for which we disclosed the categories of personal information.

8. Responding to Requests to Delete.

For requests to delete, if we cannot verify the identity of the consumer, we will deny the request to delete. We will inform the consumer that their identity cannot be verified and inform them that we do not sell any consumer personal information.

Upon verification and absent a Deletion Exception, we will comply with a consumer's request to delete their personal information by:

(a) permanently and completely erasing the personal information on our existing systems with the exception of archived or back-up systems;

(b) de-identifying the personal information; or

(c) aggregating the personal information.

If any personal information is on our archived or backup systems, we may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used.

In our response to a consumer's request to delete, we will specify the manner in which we deleted the personal information.

In cases in which we deny a consumer's request to delete, we will:

(a) inform the consumer that we will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor;

(b) delete the consumer's personal information that is not subject to the exception; and

(c) not use the consumer's personal information retained for any other purpose than provided for by that exception.

In responding to a request to delete, we may present the consumer with the choice to delete select portions of their personal information after first giving the consumer the option to delete all personal information. The consumer will be required to first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

We will use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

9. Requests to Access or Delete Household Information

If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and we can individually verify all

the members of the household subject to our verification requirements, we will comply with the request.

10. Request to Us Acting as a Service Provider

If we, acting as a service provider to another business, receive a request to know or a request to delete from a consumer regarding personal information that we collect and maintain on behalf of the other business, and we do not comply with the request, we will explain the basis for the denial to the consumer. We will also inform the consumer that they should submit the request directly to the business on whose behalf we are acting as a service provider and, when feasible, provide the consumer with contact information for that business.

11. General Verification Rules and Procedures.

Inasmuch as we do business in which we have direct contact and in other business, indirect contact with consumers, we utilize the method to verify the consumer's identity, which we find most applicable to the situation.

Whenever feasible, we will match the identifying information provided by the consumer to the personal information of the consumer which we have stored. If the consumer information has been de-identified, we will not provide or delete the information in response to a consumer request or re-identify individual data to verify a consumer request.

In all cases we will consider the:

(a) type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a stringent verification process;

(b) risk of harm to the consumer posed by any unauthorized access or deletion;

(c) likelihood that fraudulent or malicious actors would seek the personal information;

(d) if the personal information to be provided by the consumer to verify their identity is sufficiently robust;

(e) manner in which we interact with the consumer; and

(f) available technology for verification.

If we cannot verify the identity of the consumer from the information which we have stored, we may request additional information from the consumer, which shall only be used for the purposes

of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. We will delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required for record keeping.

We will use reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

12. Verification for Password-Protected Accounts

If we maintain a password-protected account with the consumer, if feasible, we may verify the consumer's identity through our existing authentication practices for the consumer's account, following our general verification rules and procedures. We will require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.

If we suspect fraudulent or malicious activity on or from the password-protected account, we will not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom we have collected information. We will use our general verification rules and procedures to further verify the identity of the consumer.

13. Verification for Non-Accountholders

If a consumer does not have or cannot access a password-protected account with us, we will proceed using our general verification rules and procedures, including the additional procedures below.

We will verify the identity of the consumer to a reasonable degree of certainty. A *reasonable degree* of certainty may include matching at least two data points provided by the consumer with data points maintained by us, and which we have determined to be reliable for the purpose of verifying the consumer.

If we in good faith determine that a request to know specific pieces of personal information requires that we verify the identity of the consumer making the request to a *reasonably high degree* of certainty, we may match at least three pieces of personal information provided by the consumer with personal information maintained by us that we consider to be reliable for the purpose of verifying the consumer, together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. We will maintain all signed declarations as part of our record-keeping.

Our response to a request to delete may require that we verify the identity of the consumer to a *reasonable degree* or a *reasonably high degree* of certainty, depending on the sensitivity of the

personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. We will act in good faith when determining the appropriate standard to apply.

If we in good faith determine that we have no reasonable method by which we can verify the identity of the consumer to the degree of certainty which we believe to be required, we will state so in our response to the consumer and explain why we have no reasonable method by which we can verify their identity.

14. Verification for Authorized Agent

When a consumer uses an authorized agent, who does not have a power of attorney pursuant to the California Probate Code sections 4000 to 4465, to submit a request to know or a request to delete, we will require the consumer to:

(a) provide the authorized agent written permission to do so; and

(b) verify their own identity directly with us.

We will also require the agent to submit proof that they are authorized by the consumer to act on behalf of the consumer.

15. Record-Keeping

All records of consumer requests made pursuant to the CCPA and how we responded to said requests will be maintained for at least twenty-four (24) months. Information maintained for record-keeping purposes shall not be used for any other purpose. Any information required for record keeping, where that information is not used for any other purpose, does not violate the CCPA.

Records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of our response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

In the event that we annually receive or share, for commercial purposes, the personal information of four million (4,000,000) or more California consumers, we will compile metrics for the previous calendar year and publish them in our privacy policy. The metrics will include the:

(a) number of requests to know that we received, complied with in whole or in part, and denied;

(b) number of requests to delete that we received, complied with in whole or in part, and denied; and

(c) median number of days within which we substantively responded to requests to know or delete a consumer's personal information.

EXHIBIT A

PENAL CODE - PEN
PART 2. OF CRIMINAL PROCEDURE [681 - 1620]
(Part 2 enacted 1872.)
TITLE 12. OF SPECIAL PROCEEDINGS OF A CRIMINAL NATURE [1473 - 1564]
(Title 12 enacted 1872.)

CHAPTER 3.6. Electronic Communications Privacy Act [1546 - 1546.4]
(Chapter 3.6 added by Stats. 2015, Ch. 651, Sec. 1.)

1546.

For purposes of this chapter, the following definitions apply:
(a) An "adverse result" means any of the following:
(1) Danger to the life or physical safety of an individual.
(2) Flight from prosecution.
(3) Destruction of or tampering with evidence.
(4) Intimidation of potential witnesses.
(5) Serious jeopardy to an investigation or undue delay of a trial.
(b) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.
(c) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.
(d) "Electronic communication information" means any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. "Electronic communication information" does not include subscriber information as defined in this chapter.
(e) "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.
(f) "Electronic device" means a device that stores, generates, or transmits information in electronic form. An electronic device does not include the magnetic strip on a driver's license or an identification card issued by this state or a driver's license or equivalent identification card issued by another state.
(g) "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.
(h) "Electronic information" means electronic communication information or electronic device information.

(i) “Government entity” means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.
(j) “Service provider” means a person or entity offering an electronic communication service.
(k) “Specific consent” means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.
(l) “Subscriber information” means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.
(Amended by Stats. 2016, Ch. 541, Sec. 2. (SB 1121) Effective January 1, 2017.)

1546.1.

(a) Except as provided in this section, a government entity shall not do any of the following:
(1) Compel the production of or access to electronic communication information from a service provider.
(2) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
(3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity.
(b) A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:
(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).
(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.
(3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.
(4) Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(5) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.
(c) A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:
(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).
(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.
(3) Pursuant to a tracking device search warrant issued pursuant to paragraph (12) of subdivision (a) of Section 1524 and subdivision (b) of Section 1534.
(4) With the specific consent of the authorized possessor of the device.
(5) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.
(6) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.
(7) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the government entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.
(8) Except where prohibited by state or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility or a secure area of a local detention facility where inmates have access, the device is not in the possession of an individual, and the device is not known or believed to be the possession of an authorized visitor. This paragraph shall not be construed to supersede or override Section 4576.
(9) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is serving a term of parole under the supervision of the Department of Corrections and Rehabilitation or a term of postrelease community supervision under the supervision of county probation.
(10) Except where prohibited by state or federal law, if the device is seized from an authorized possessor of the device who is subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release.
(11) If the government entity accesses information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.
(12) Pursuant to an order for a pen register or trap and trace device, or both, issued pursuant to Chapter 1.5 (commencing with Section 630) of Title 15 of Part 1.
(d) Any warrant for electronic information shall comply with the following:
(1) The warrant shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought, provided, however, that in the case of a warrant described in paragraph (1) of subdivision (c), the court may determine that it is not appropriate to specify time periods because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and 1054.7. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.
(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.
(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following:
(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.
(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.
(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.
(g) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:
(1) The government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.
(2) The government entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.
(3) The government entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.
(4) The service provider or subscriber is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.
(h) If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the government entity shall,

within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 call from that device.
(i) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:
(1) Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.
(2) Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.
(3) Require a service provider to provide subscriber information.
(j) This section does not limit the authority of the Public Utilities Commission or the State Energy Resources Conservation and Development Commission to obtain energy or water supply and consumption information pursuant to the powers granted to them under the Public Utilities Code or the Public Resources Code and other applicable state laws.
(k) This chapter shall not be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity’s possession.
(Amended by Stats. 2016, Ch. 541, Sec. 3.5. (SB 1121) Effective January 1, 2017.)

1546.2.

(a) (1) Except as otherwise provided in this section, any government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency access, a notice that informs the recipient that information about the recipient has been compelled or obtained, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three court days after obtaining the electronic information.

(2) Notwithstanding paragraph (1), notice is not required if the government entity accesses information concerning the location or the telephone number of an electronic device in order to respond to an emergency 911 call from that device.
(b) (1) When a warrant is sought or electronic information is obtained in an emergency under Section 1546.1, the government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.
(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).
(3) Upon expiration of the period of delay of the notification, the government entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant or emergency access, a document that includes the information described in subdivision (a), a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.
(c) If there is no identified target of a warrant or emergency access at the time of its issuance, the government entity shall submit to the Department of Justice within three days of the execution of the warrant or issuance of the request all of the information required in subdivision (a). If an order delaying notice is obtained pursuant to subdivision (b), the government entity shall submit to the department upon the expiration of the period of delay of the notification all of the information required in paragraph (3) of subdivision (b). The department shall publish all those reports on its Internet Web site within 90 days of receipt. The department may redact names or other personal identifying information from the reports.
(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.
(Amended by Stats. 2017, Ch. 269, Sec. 10. (SB 811) Effective January 1, 2018.)

1546.4.

(a) Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter. The motion shall be made, determined, and be subject to review in accordance with the procedures set forth in subdivisions (b) to (q), inclusive, of Section 1538.5.
(b) The Attorney General may commence a civil action to compel any government entity to comply with the provisions of this chapter.
(c) An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this chapter, or the California Constitution or the

United States Constitution, or a service provider or any other recipient of the warrant, order, or other legal process may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, or the California Constitution, or the United States Constitution.

(d) A California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this chapter.

(Added by Stats. 2015, Ch. 651, Sec. 1. (SB 178) Effective January 1, 2016.)