BCLP. Client Intelligent

Insights

"SENSITIVE PERSONAL INFORMATION" – UNDERSTANDING AND COMPLYING WITH THE NEW RULES IN THE UNITED STATES

Feb 16, 2023

The concept of Sensitive Personal Information (SPI) has made its way into new and emerging U.S. privacy laws. The usual challenges associated with a novel privacy obligation certainly apply to Sensitive Personal Information, but differing approaches across state laws and, in particular, California's right to limit processing of SPI, have further complicated the issue. Although there are no simple answers for organizations trying to address these new obligations and the landscape may continue to shift as states finalize their regulations, certain themes have emerged. Below, we break down the different requirements and potential strategies organizations can consider when tackling compliance.

WHAT QUALIFIES AS SENSITIVE PERSONAL INFORMATION?

Each new and pending U.S. state privacy law includes a definition for SPI.[1] Although there are slight variations across these laws, the term generally includes information about a consumer's (which in California includes employee, job applicants and contractors as well as B2B contacts):

a. Social security, driver's license, state identification card, or passport number;

b. Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

c. *Precise* geolocation;[2]

d. Racial or ethnic origin, religious or philosophical beliefs, or union membership;

e. Contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;

f. Genetic data processed for the purpose of uniquely identifying a consumer;

g. Biometric information processed for the purpose of uniquely identifying a consumer;

h. Information concerning a consumer's mental or physical health;

i. Information concerning a consumer's sex life or sexual orientation;

j. Some states also include a child's (under 13 years of age) personal data (e.g., Colorado, Connecticut, Virginia).[3]

WHAT REQUIREMENTS APPLY TO SENSITIVE PERSONAL INFORMATION?

With the exception of California and Utah[4], the new U.S. state laws require organizations to obtain affirmative opt-in consent to collect and use SPI. While onerous from a process standpoint, such opt-in requirements are relatively straightforward.[5] At a high level, the key for organizations will be to adopt a mechanism that allows individuals to affirmatively express their consent (i.e., no pre-checked boxes or misleading language) in an explicit, voluntary manner and to also establish a process for proving that consumer consent has been obtained. In practice, the evidentiary step is often addressed by setting up a process by which all consumers must consent prior to providing the relevant information and/or maintaining a digital record/logs of consents.

California

As opposed to the opt-in requirements discussed above (to which there are no exceptions), the amendments enacted by the California Privacy Rights Act to the California Consumer Privacy Act (collectively, the CPRA) require organizations to provide consumers with the right to **limit** the use and disclosure of their SPI "to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services."[6] Where required, organizations must provide a "Limit the Use of My Sensitive Personal Information" link on their homepage that consumers can use to exercise this right.[7]

What has been often overlooked about this obligation, however, is that it applies only in certain circumstances as defined by the draft CPRA regulations, which are currently anticipated to be finalized in the second quarter of 2023. More specifically, if an organization uses SPI for one of the purposes set out in Section 7027 of the draft regulations and/or "without the purpose of inferring characteristics about a consumer", the organization is **not** obligated to offer this right to limit (although, the organization is still required to obtain opt-in consent for other states, where applicable).

Section 7027 lists the following uses and disclosures as those that do **not** trigger the right of opt-out, "provided that the use or disclosure is reasonably necessary and proportionate for this purpose:"

1. **To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.** For example, a consumer's precise geolocation may be used by

a mobile application that is providing the consumer with directions on how to get to [a] specific location. A consumer's precise geolocation may not, however, be used by a gaming application without offering the right to limit where the average consumer would not expect the application to need this piece of SPI for the use of the game itself.

2. **To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information, provided that the use of the consumer's personal information.** For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.

3. **To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.** For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

4. **To ensure the physical safety of natural persons.** A business may disclose a consumer's precise geolocation information to law enforcement to investigate an alleged kidnapping.

5. **For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.** For example, a business that sells religious books can use information about its customers' interest in its religious content to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use SPI to create a profile about an individual consumer or disclose SPI that reveals consumers' religious beliefs to third parties.

6. **To perform services on behalf of the business.** For example, a business may use SPI for maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

7. **To verify or maintain the quality or safety of a product, 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 by, manufactured for, or controlled by the business.** For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.

8. **To collect or process SPI where such collection or processing is not used for the purpose of inferring characteristics about a consumer.** For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.

The inference exception (No. 8 above) bears particular attention. The language of the CCPA itself would seem to suggest that the right to limit does not apply in any instance in which SPI is not used to make inferences ("*Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section….*").[8] However, it is unclear whether this carve out was really intended to be the exception that swallows the rule, particularly because it is included in the list of exceptions to the right to limit in the CPRA regulations, rather than being called out as an overarching exception.

In addition, neither the CPRA itself nor the regulations themselves provide clear guidance regarding what activities would specifically qualify as making an inference. "Inference" or "Infer" is defined as "the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data."[9] Although this term itself does not define what activities would constitute making an inference, in March of 2022, the California Office of the Attorney General (OAG) did provide some additional guidance on this issue. According to the OAG, the information must be used to create a profile about a consumer, which "rules out situations where a business is using inferences for reasons other than predicting, targeting, or affecting human behavior." Based on the definition itself and this guidance, it seems reasonable to assume that organizations using SPI for purposes of building or improving profiles about consumers or targeting specific goods or services to them based on their SPI would be required to offer the right to limit, but it is not completely clear what else might get swept into this concept.

As a result of the ambiguity surrounding the inference exception, organizations should apply it with a certain caution and assume that it cannot be applied too broadly until further clarification and/or guidance is provided by the California regulatory authorities.

WHAT SHOULD COMPANIES DO?

Like so many requirements, addressing the new requirements for SPI will require time and resources, but breaking it down into specific steps will help make the process more manageable.

These important steps include:

Know Your SPI

As with all new requirements, organizations first need to understand whether and when they collect Sensitive Personal Information (noting that in California, these obligations now apply to HR Data (see our related insight). Although many companies would not routinely collect information

regarding race or ethnic origin on their website, many would collect account log-in information. Therefore, it is important to thoroughly understand what information is collected from consumers rather than assuming that SPI is not collected.

Understand What's Happening

In addition to understanding what SPI is collected from consumers, organizations must also understand how it is used to parse out, in particular, whether the California right to limit may be triggered. For example, if health and medical data are used and/or disclosed only to provide the service expected by the consumer, then the organization may still need to obtain consent for the collection of that SPI to meet other state law requirements but not offer the right to limit. In addition, the structure of these consents or authorizations may be different. An authorization under HIPAA has specific elements beyond the statutory definition of consent found in the state laws at issue. Likewise, wiretap statutes in the United States likely will require a different type of consent than, for example, analytics cookies subject to the EU ePrivacy Directive. This practically means that companies should always understand what legal regime applies as this will affect the structure of the consent.

Develop a Compliance Strategy

Once the relevant fact-finding has been concluded, the most critical step in the process is to develop a consolidated compliance strategy for meeting applicable requirements. This could include the need for a strategy for obtaining consent as required by other state laws, if applicable, as well as providing the right to limit or designing the use of SPI to avoid providing a right to limit. In many circumstances, companies will also need to design a process for revoking a previous consent. Where the right to limit does apply, organizations will need to develop a mechanism to segregate or tag SPI for consumers who have exercised this right, so the SPI is only used for the purpose(s) that do not trigger the limitation right. Moreover, if a company is contractually obligated to disclose this SPI to another organization, the agreement should carve out the disclosure of information about consumers who have exercised this right.

While companies could consider implementing different approaches for consumers located in different states, we expect that in the long-run this will be a difficult approach to manage. Moreover, due to the practical difficulties associated with offering the right to limit, we anticipate that many organizations will work to keep their activities with regard to SPI within the bounds of uses that do not trigger this right, but it will be important to monitor uses and disclosures of SPI to make sure that this decision continues to be defensible and also aligns with internal business priorities. Regardless of the approach ultimately adopted, it must be something that companies can actually implement and maintain evidence of across consumer data collections, uses and disclosures.

Be Ready to Adjust

As discussed above, none of the states that has enacted new privacy laws has finalized its regulations and/or provided meaningful guidance on how companies should address the numerous new requirements emerging from these laws. Therefore, organizations need to be ready to adjust their strategies as the legal landscape and their own practices evolve. In the meantime, it is critical to get started working through these thorny issues.

---

[1] *See, e.g.,* Cal. Civil Code § 1798.140(ee) (California Privacy Rights Act); Col. Rev. Stat. § 6-1-1303(24) (Colorado Privacy Act); Connecticut Public Act No. 22-15 § 1(27) (Connecticut Data Privacy Act); Utah Code § 13-61-101(32) (Utah Consumer Privacy Act); Virginia Code § 59.1-571 (Virginia Consumer Data Protection Act).

[2] Precise geolocation has varying definitions under state law but the definitions are very specific with respect what qualifies as "precise". For example, the Connecticut Data Privacy Act defines precise geolocation to mean "the specific location of an individual with precision and accuracy within a radius of [1,750] feet." Connecticut Public Act No. 22-15 § 1(19). California's precision requirement is 1,850 feet, while Utah and Virginia both use 1,750 feet. Cal. Civil Code § 1798.140(w); Utah Code § 13-61-101(33); Virginia Code § 59.1-571. Colorado's law does not include a precise geolocation concept.

[3] Publicly available information is generally excluded from the definition of SPI, but it is important to confirm how that term is applied in a particular state and situation.

[4] Utah does not require affirmative opt-in consent to the processing of SPI, but does require notice and the ability for a consumer to opt-out of this processing. Utah Code § 13-61-302(1), (3).

[5] Col. Rev. Stat § 6-1-1308(7) (cannot process SPI without first obtaining consent, and in the case of a child's personal data, obtaining consent from the child's parent or lawful guardian); Connecticut Public Act No. 22-15 § 6(a)(4) (cannot process SPI without first obtaining consent, and in the case of a child's personal data, complying with the Children's Online Privacy Protection Act (COPPA) for verifiable parental consent); Virginia Code § 59.1-574(A)(5) (cannot process SPI without first obtaining consent, and in the case of a child's personal data, complying with COPPA). Generally, consent is considered to be an affirmative act by a consumer that unambiguously indicates the consumer's voluntary, informed agreement to the processing. *See, e.g.,* Connecticut Public Act No. 22-15 § 1(6); Virginia Code § 59.1-571.

[6] CPRA 1798.121(a).

[7] CPRA 1798.135(a)(2).

[8] CPRA 1798.121(d).

[9] CPRA 1798.140(r).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Martha Kohlstrand

Boulder

martha.kohlstrand@bclplaw.com
+1 303 417 8516