wiley

NEWSLETTER

The Next Major Privacy Challenge for Corporate America – California's New Privacy Law

July 2018

Privacy in Focus®

California has been at the forefront of the privacy debate for many years. Some California privacy innovations have had national implications (internet privacy notice requirements). Other provisions have led to national counterparts across the country (data breach notification). Other creations have gone nowhere else (the California Attorney General lists many dozens of "general privacy laws" applicable in California).

Now, California has passed AB 375 - through a turbulent and awkward set of legislative steps - a broadly applicable general privacy law, very loosely analogous to the recent GDPR implementation. The law covers a wide range of topics, with little of the thought or analysis that typically proceeds a law of this magnitude (compare to the enormous range of debate on GDPR topics before a final regulation was in place, and the much longer lead time for GDPR compliance). The new California statute provides that it will be "operative" January 1, 2020. While we will be dissecting these provisions for quite some time, what are the key provisions of the law and the main challenges and issues to watch going forward?

Who Does the Law Apply To?

Unlike most current US national laws, the California law is intended to have general applicability, independent of industry sector. This scope is one reason why many are comparing the California law to the General Data Protection Regulation that recently went into effect in

Practice Areas

Privacy, Cyber & Data Governance

Europe. Essentially, a business that collects personal information about California residents is covered by this law, unless there is a defined exception. The big exceptions are (1) certain companies covered by other privacy laws (such as HIPAA and Gramm-Leach-Bliley – more on that later) and (2) certain size limitations, as covered businesses have revenue thresholds (above $25 million in annual revenue) or consumer volume (personal information on 50,000 people or derives 50% or more of their revenue from sale of personal information). The status of non-profits may be unclear. There also are critical drafting issues that may depend on the placement of a comma or other paragraph spacing issues – for example, are HIPAA business associates exempted for protected health information subject to the HIPAA rules?

What Information is Covered and About Whom?

The law applies to "personal information" about California residents, which is "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." The categories from the law are defined incredibly broadly – not only to include "normal" identifiers (e.g., name, address, Social Security Number, driver's license number), but also (among others):

- Characteristics of protected classifications under California or federal law;
- Commercial information (records of personal property, products or services purchased, or other purchasing or consuming histories or tendencies);
- Biometric information;
- Internet information including browsing history and search history;
- Geolocation data; and
- Inferences drawn from any information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes;

My personal favorite involves personal information that is "Audio, electronic, visual, thermal, olfactory, or similar information." This is a tremendously broad overall definition.

Scope of Exemptions

While the law applies across industries, there are a variety of exemptions or other carve-outs. The law does "not restrict a business's ability to: collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information." It does not directly apply to activity in other states, as the law does not restrict how an entity can "[c]ollect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California."

In addition, the law does not apply "to protected or health information that is collected by a covered entity governed by the Confidentiality of Medical Information Act . . . or governed by the [HIPAA] privacy, security, and breach notification rules," meaning that large segments of the health care industry are not covered (but

how much is clearly an open issue). Similarly, this law does not apply to personal information "collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act."

Individual Rights

As with GDPR, a significant component of the law provides specific individual rights. Among the key (and challenging to implement) rights are:

- 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.
- the right to request that a business delete any personal information about the consumer which the business has collected from the consumer (a right with many exceptions).
- the right to request that a business that collects personal information about the consumer disclose to the consumer a broad range of information including (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 and (5) the specific pieces of personal information it has collected about that consumer.
- the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose (defined separately in the law), 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; and (3) the categories of personal information that the business disclosed about the consumer for a business purpose.
- 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 (what the law calls "the right to opt out"). For this right, companies must (among other things) 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 to opt out of the sale of the consumer's personal information.

Financial Arrangements

The law creates an interesting series of challenges and opportunities relating to "financial incentives" for use or disclosure of personal information. On the one hand, the law makes clear that a business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights 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; or (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.

At the same time, nothing in the law "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." In addition, the law provides that 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." However, a "business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." Companies will need to be creative and thoughtful in evaluating these provisions (and I would expect additional guidance from the state Attorney General before the law goes into effect).

Litigation Provisions and Statutory Damages

In section 1798.150, the law creates a specific and limited right to bring a civil action for statutory damages in certain carefully defined situations involving security breaches. This provision does not seem to apply to "privacy" breaches (e.g., an unpermitted sale of personal information). This provision permits any "consumer whose nonencrypted or nonredacted personal information . . . 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" to institute a civil action that can seek:

- 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;
- Injunctive or declaratory relief; and
- Any other relief the court deems proper.

Where a case can be brought for these statutory damages (where no proof of actual injury seems to be required), the court, in determining the amount of the statutory damages, shall consider:

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.

However, there are significant procedural hurdles before a case like this can be brought. Specifically, prior to bringing a case - 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." If a "cure is possible," and the business then - within 30 days - actually cures the violation and "provides the consumer an express written statement that the violations have been cured and that no further violations shall occur," then no case may proceed. (No prior notice is required if the consumer seeks actual damages, which is likely to lead to a variety of hybrid complaints in these cases). If the violation continues, then a case may be pursued (leaving open the obvious question in the security context of who gets to decide if a particular security issue has been "cured" or not – including what "issue" even led to a specific security breach).

In addition, the consumer also must notify the Attorney General of the case, and the Attorney General can, in effect, stop the civil case by instituting an enforcement action (or by notifying the consumer that the action shall not proceed – with lots of opportunities for effective advocacy here). The law is clear that the provisions of this law – beyond these carefully crafted civil cause of action provisions – cannot serve as the basis for "a private right of action under any other law." This language appears to be an effort to hold off the ability of plaintiffs' counsel in future cases to use these provisions as a "standard of care" for broader negligence claims.

Enforcement

Separately, for government enforcement (which applies to both privacy and security issues), this same idea of a "cure" period is required before enforcement can take place. A business is in violation of the law (apparently) only if it fails to cure an alleged violation in 30 days after being notified of the issue, with a civil penalty of up to seven thousand five hundred dollars for each violation. The law provides that 20% of the settlement or penalty funds shall be allocated to a Consumer Privacy Fund, created by the law, with "the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title."

Key Issues to Watch - So What's Next?

This law was drafted and passed in essentially a week, with little public debate or discussion on most of the issues, so lots of open issues remain, and there is lots of time to make changes. The impetus for the law was a desire by the regulated community to head off an even more expansive ballot initiative. So, with this law now passed, we can expect enormous lobbying pressure from all sides, including those who think that the law is insufficiently aggressive (one privacy advocate group already has submitted a letter with suggested changes). I would expect meaningful change before the law becomes effective – although this could go in several directions and could apply to many of the provisions of the law. I also expect significant guidance to address some of the most important open or unclear issues about the law, even if the law is not changed.

- *National Impact on Practices*

Companies will need to begin preparing for this law quickly. Many companies that have just finished the GDPR process (or are still in the middle of it) will at least have a familiar blueprint for the overall effort. One key question that every company will need to consider in the short term – will the California law be applied by the company only to California residents, or will the company make a broader decision to apply – at least in some parts – these provisions on a nationwide or global basis? Unlike some parts of GDPR, this law generally does not prohibit specific practices – it requires disclosure of them. So, companies may find ways to parse their practices to focus on California residents only. This is not a one size fits all decision – companies will need to consider their own business and operational models, and will need as well to think carefully about each particular provision of the law (for example, the right to deletion could be applied only for California residents, if a company chose to act that way).

- *Broader Legislative Impact. - Either Federal Law or Other State Activity*

One key policy issue will be whether this law spurs broader legislative change – either at the national level (where Congress has failed to move forward on national privacy law), or on a state by state basis. It is hard to see Congress passing a national privacy law any time soon. There is a higher likelihood of state-specific action. However, the unusual circumstances of the California legislative process clearly led to this law – without analogies, it will be an uphill battle in other states.

- *Regulations*

The law provides for the Attorney General's Office to issue regulations. Will this happen? Will these regulations have a material impact on the substance of the law? Will the Attorney General be able to issue these in a timeframe that will permit reasonable compliance activity?

- *Impact of Individual Rights*

Many existing US privacy laws create individual rights. For the most parts, these rights have not been exercised by significant percentages of the protected population. Will these provisions be different? What will the impact of these rights be on business activity, in California and nationwide? How will this impact "big data" activities around the country? In addition, most of the rights are tied to a "verifiable consumer request" – will this prove to be a challenge for regulated businesses?

- *Employers*

The law applies to personal information about residents of California. The law also says nothing specific about one enormous category of data - data relating to employees. At a minimum, it will be easier for companies to identify their employees that are California residents. However, determining how best to approach these compliance issues for employees may be challenging. At least (unlike GDPR) there is no presumption that employee consents are infeasible. For some companies (e.g., a HIPAA covered entity), this law may still require significant compliance attention related to employee data, even if much of these entities consumer data is exempted.

- *Impact on Vendor Contracts*

Many privacy laws create requirements for vendor contracts. This law does not explicitly address vendor contracts, except in fairly limited circumstances. How will companies address these requirements for their service providers? Is this yet another law where vendor contracts will need to be revised to address a new legislative requirement? And will companies - on both sides of these contracts – be reasonable about their approach to these issues?

- *Importance of Deidentification Strategies*

Like most privacy laws, the California law applies to "personal information," and does not generally purport to regulate personal information that has been aggregated or de-identified. While the law creates some interesting new twists on how de-identification is defined (including not only that data cannot "reasonably relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer" but also additional security and operational controls beyond that), it is clear that there are meaningful opportunities for businesses to utilize effective de-identification techniques as a way to minimize some of the operational impact of this legislation. However, effective de-identification is complicated, and requires a broad and thoughtful approach to data management and data analytics.

Conclusions

From humble beginnings, privacy and data security law now seems to require almost constant change for regulated entities. GDPR was a key testing ground for many companies – they were pushed to identify their practices with more carefulness than ever before, and apply a thoughtful approach to overall use and disclosure of personal information. This California law obviously will touch not only the global companies that were hit by GDPR, but also an enormous number of US companies for whom GDR was a minor or non-existent issue.

A key challenge for all companies will be how to plan for these California requirements – on a relatively fast timetable – with little confidence that the provisions will stay in this form and an expectation of meaningful change through guidance or regulations in any event. Regardless of these open questions, for companies with any meaningful California presence, it will be important to at least start the compliance process soon – to identify in general ways how the provisions apply to the company and where key hot spots would be, where business pressures will meet these compliance requirements head on. It may make sense not to build compliant processes too quickly – given the likelihood of changes – but getting a good head start likely will be a critical step over the next few months.

This article was originally published in *Bloomberg BNA's Bloomberg Law: Privacy and Data Security* and can be found here.