Wiley Rein LLP

# PRIVACY IN FOCUS®

**Developments in Privacy and Information Security Law** | July 2018

Our articles this month focus on two enormous developments in the privacy and security universe. First, I review the recent California Consumer Privacy Act, and begin the discussion of its implications across the U.S. privacy landscape. We also include a transcript of my recent podcast interview with Marianne McGee about the California law. We will be following the developments on this law closely, as companies move towards the January 1, 2020 compliance date. Second, we look at the Supreme Court's recent *Carpenter* decision and its impact on government access to personal data for investigative purposes.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

**— Kirk Nahra, Privacy & Cybersecurity Practice Chair**

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

**By Kirk J. Nahra**

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).

ALSO IN THIS ISSUE



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

*continued on page 4*

# *Carpenter v. United States*: The Supreme Court's Recent Decision Will Have Widespread Implications for the Collection of Digital Information by Law Enforcement

**By Megan L. Brown, Matthew J. Gardner, Kathleen E. Scott and Vesna K. Harasic-Yaksic**

On June 22, 2018, in a major decision on data privacy, the U.S. Supreme Court **held** that the government must obtain a warrant when seeking historical cell tower records providing a detailed and comprehensive history of a user's movements. The Supreme Court's holding has widespread implications for all companies that collect user data and may require companies to re-evaluate how they comply with legal process in certain instances.

## Overview of *Carpenter v. United States*

**Factual Overview:** In 2011, the Federal Bureau of Investigation (FBI) suspected Mr. Carpenter of robbing a string of Radio Shacks and T-Mobile stores in Detroit, Michigan. The FBI issued an order under 18 U.S.C. § 2703(d) to both MetroPCS and Sprint – Mr. Carpenter's wireless carriers – seeking cell site information for Mr. Carpenter's cell phone for the four-month period in which the robberies occurred. An order pursuant to 18 U.S.C. § 2703(d), often referred to as a 2703(d) Order, allows the government to compel disclosure of certain "non-content" information when the government "offers specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material to an ongoing criminal investigation."

The FBI ultimately used the cell-site information at trial to prove that Mr. Carpenter was near each store at the time of the alleged robberies. Before his conviction, Mr. Carpenter moved to suppress the cell-site data, arguing that the government's seizure of these records violated the Fourth Amendment because it was not obtained pursuant to a warrant supported by probable cause. The Sixth Circuit affirmed the conviction and the Supreme Court granted certiorari.

**Legal Analysis:** The Supreme Court reversed the Sixth Circuit's decision, concluding that obtaining cell-site location information (CSLI) requires a warrant supported by probable cause. In its opinion, the Court analyzed cases establishing the third-party doctrine, which had previously held that a person has no legitimate expectation of privacy in information that he or she voluntarily discloses to third parties.

Noting that CSLI "does not fit neatly under [these] existing precedents[,]" the Court ultimately declined to extend the third-party doctrine to CSLI. According to Chief Justice Roberts, CSLI is akin to GPS information in that it provides an extraordinary amount of personal information: it "provides an intimate window into a person's life revealing not only his particular movements, but through them his 'familial, political, professional, religious and sexual associations.'" Moreover, because cellphones are such a necessary part of daily life, it cannot be said that CSLI is "truly shared as one normally understands the term." Therefore, "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party[.]"

*continued on page 3*

## Implications of *Carpenter v. United States*

The Supreme Court's decision in *Carpenter* limits application of the third-party doctrine in light of the ability of modern technology to collect data. The opinion not only acknowledges that transmission of data in the digital age reveals a wealth of information about an individual's personal life, but also that participation in technologies is a necessity of modern life. In recognizing these principles, the opinion makes clear that the government can no longer argue that individuals using digital technology somehow assume the risk of warrantless government action.

*Carpenter* should not be interpreted in isolation. Rather, *Carpenter* is the third recent case where the Court has expressed its willingness to expand Fourth Amendment principles and adopt a flexible approach to protecting the privacy of digital information. In *United States v. Jones*, the Supreme Court limited the government's ability to use a GPS device to track an individual's movements. Additionally, in *Riley v. California*, the Supreme Court declined to extend the search-incident-to-arrest doctrine to cell phone searches, stating that "the storage capacity of [a] cell phone" allows it to "collect[] in one place many distinct types of information… that reveal more in combination than any isolated record." Collectively, these cases signify that the Court believes that the Fourth Amendment provides a strong check on law enforcement when it comes to the collection of digital information.

As courts and law enforcement work to understand the limits of *Carpenter*, companies that collect user data should consider the following:

- Companies will still enjoy broad protections when they respond to law enforcement requests in good faith.
- Companies may need to review how they respond to subpoenas and 2703(d) Orders in certain cases—particularly requests for location information.
- *Carpenter* expressly held that the emergency exception to the Fourth Amendment's warrant requirement still applies to location information. Companies may continue to process these requests under their existing policies.
- The scope of the Court's holding beyond the facts of the case (a 2703(d) Order seeking location information during a four-month period) is unclear. However, the Court's limitation of the third-party doctrine and expanded interpretation of a user's privacy interests suggests a broad ruling. Companies will have to consider whether the Court's ruling has extended Fourth Amendment protections (and a warrant requirement) to other classes of collected data. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

Vesna K. Harasic-Yaksic
202.719.4506
vharasic-yaksic@wileyrein.com

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 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."

*continued on page 5*

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

*continued on page 6*

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

*continued on page 7*

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.

*continued on page 8*

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

*continued on page 9*

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**.



For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

# Nahra Interviewed on Why California's New Privacy Law Is a Whole New Ballgame

*Kirk Nahra recently was interviewed by Marianne Kolbasuk McGee, executive director at the Information Security Media Group, concerning the California Consumer Privacy Act of 2018.*

**Marianne Kolbasuk McGee:** California recently signed into law a new privacy bill that is considered by some as the strictest of any state. Parts of the bill also mirror the European Union's General Data Protection Regulation. So, Kirk, what's your assessment of this new law? Is it indeed the strictest state privacy law in the U.S., and wasn't California already considered as having stricter privacy laws than most states? What's changed?

**Kirk Nahra:** It's certainly true that California has more and varied privacy laws than anywhere else in the country. They've got dozens of privacy laws covering all kinds of issues. So certainly, it's the toughest state for privacy provisions from the perspective of industry, in general. However, this law is a whole new ballgame, and it's particularly important because it essentially applies to all personal data in all situations. There are some exceptions to that, but the idea is that it applies to everything, and that's very different from not only all the prior California laws, but also the entire approach to privacy and security regulation that we've seen in the United States to date, where the laws have been industry specific, like HIPAA or the Gramm Leach Bliley Act for Financial Services Industry. They've been practice specific, dealing with the particular law for a particular activity. We don't have one size fits all laws, which is why the comparison to the EU's GDPR has been coming up so often. The GDPR in Europe, and the privacy directive before that, were provisions that tried to apply to all personal data in all contexts. This is the first time we've really seen this in the United States.

**Marianne Kolbasuk McGee:** So speaking of GDPR, what makes this California law similar to GDPR; are there certain provisions, or other sorts of similarities?

**Kirk Nahra:** Yes, there are both similarities and differences. GDPR is the most obvious comparison; that doesn't mean it's a perfect comparison. Why we're seeing the comparison is that GDPR is so new and on everybody's mind. Lots of companies have just gone through that compliance exercise. That set of rules just went into effect at the end of May. It's a good comparison in terms of overall scope. The California law covers any business and any personal information, which GDPR does too. It is also a good comparison because a lot of the California law is driven by individual rights, the ability of residents of California to decide what to do with their information, what happens to their information and to make various requests of companies that have their information. That again is very similar to GDPR and some of the principles of GDPR. There also are some differences from GDPR.

There are important differences on enforcement. We have less of an issue in California about things like data transfers. California isn't worried about data moving from California to Pennsylvania, or from California to some other country. GDPR is very concerned about data leaving the EU. So there are similarities and differences, but in terms of people needing a starting point to think about in the United States, GDPR

*continued on page 11*

might be the best place to start. But at the same time, you really need to focus on the specifics of the California law.

**Marianne Kolbasuk McGee:** So, who needs to comply with this law; is it just California based businesses or any business that does business with consumers based in California?

**Kirk Nahra:** There are going to be two important issues for companies to think about. One is, are they covered at all and, two, if they are covered at all, how far does that coverage go? And this is the same kind of issue that we had with GDPR. Not every company is covered by GDPR, but lots of companies are, including lots of companies that aren't physically present in the EU. The companies that went through that analysis in the EU had to decide whether they were going to apply GDPR only to EU contacts or were they going to try to extend it more broadly. We're going to have the same issue in California. The law essentially provides protections for California residents. So that would be not only a business in California, but it would also include a business in Chicago that is dealing with personal information of California residents. It certainly goes beyond California state borders in that sense. Companies are going to have to think about whether they have dealings with California residents, and the law is pretty broad as to what that means. So companies are going to have to be thoughtful about figuring that out. If the business is a restaurant in Washington, DC and somebody from San Francisco walks into the restaurant, I doubt that all of a sudden that restaurant is going to be covered by the California law. Again, businesses are going to have to be thoughtful about it.

Then if companies decide that they have obligations under the California law, perhaps the more challenging issue is going to be whether to apply the standards of the California law broader than to California residents. And that's one of the tricky challenges. If you give a California consumer certain rights in their data, is your company going to deny those same rights to somebody who's from Michigan? You have that option, assuming you can separate out their activities, but companies are going to have to think more broadly about whether that's a smart strategy, whether it's an effective strategy, and whether they can actually efficiently run their business that way.

One of the earlier California innovations was laws dealing with data breach notification. Other states didn't immediately jump on board, but as soon as we had a big security breach where a company was reported as taking the position that they were going to notify California people and not notify people in other states, all of a sudden those other states started saying, wait a minute, we have to protect our citizens as well. One big issue politically is whether other states are going to start acting in the same way that California has done here. I think there are some significant reasons why that may not happen, but that's going to be a real issue.

**Marianne Kolbasuk McGee:** When it comes to healthcare entities and their business associates, what steps should these entities be taking in order to comply with this new California law, and how does this law differ from what they need to be doing anyway under HIPAA?

*continued on page 12*

**Kirk Nahra:** A lot of things that we're talking about today are still very much open issues. The California law was passed in a kind of a crazy set of circumstances. There was a ballot initiative that was about to be put on the November ballot that was going to involve significantly stricter privacy controls applied broadly across the board in California. Lots of relevant industry and lots of other folks were nervous about the California ballot initiative, and so there was last minute pressure to pass a law as an alternative to the ballot initiative. That's what happened. So, this law, despite how broadly it applies, was written very quickly and passed very quickly with very little discussion and very little analysis. So we have lots of open issues that we'll be dealing with over the next few months, before this law goes into effect in January 2020.

With that said, a couple of things are important for the healthcare industry. First, the law seems to exempt covered entities for protected health information, meaning the information that is already protected by HIPAA when it's held by covered entities. So, there is the intention to have that broad carve-out. Now that obviously will remove many healthcare entities and some of the information they have. It doesn't exempt them from employee information; it doesn't exempt them from information that is not subject to HIPAA, that's not about their patients or whatever. But that's going to be a big piece of this. It is completely unclear whether this law exempts HIPAA business associates. You could read the words in a couple of different ways. One would exempt business associates, one would not, and we don't have an answer to that. So that's going to be a big issue. I would expect either some guidance or a legislative amendment to deal with that, but we don't have that yet. Then you also have the enormous range of healthcare information that is not subject to the HIPAA rules because of the quirks in how HIPAA applies. That information generally will be protected under the California law. So for companies that produce wearables or mobile apps or have healthcare websites that aren't connected to a hospital, things like that where HIPAA may not apply, the California law will apply to protect the covered information.

**Marianne Kolbasuk McGee:** You mention that there are certain kinds of data that might not fall under HIPAA and that this law covers any personal information. Are there certain categories of information that fall under this bill that we haven't seen as part of a privacy law before? For instance, I know that there's a big section there about biometric information. Are there any elements in this law that before fell through the holes?

**Kirk Nahra:** It basically captures essentially anything they could think of that might be used to identify a person. So, I'm not sure you can look at any particular element and say we've never seen that before. But we haven't seen much of it. For example, cookies and internet browsing, which haven't always been thought of as personal information, certainly are treated as personal information. It's very broad. It does include some information, that I did scratch my head about a little bit. For example, the law explicitly applies to olfactory information, which I guess means information about personal smells. I'm not sure what we're going to do with that language. But it's a very very broad definition of personal information, with the idea of trying to regulate

*continued on page 13*

anything that a company could collect about an individual that either does or might reasonably identify that individual.

**Marianne Kolbasuk McGee:** Now this California law doesn't take effect until January 2020. Does this give businesses enough time to comply and also, can the law be potentially amended until then, and, if so, what sorts of amendments might we expect?

**Kirk Nahra:** A couple of different things are going to make this period between now and January 2020 really important. I would expect there to be significant pressure from all sides to change parts of this bill. One of the reasons that this law was put into place instead of the ballot initiative is that it is easier to amend this type of law than it is to amend the provisions of a ballot initiative. Again, quirks of California legislative process. So, there will be pressure to change this law, there will be lots of pressure to change this law. Some of that pressure is going to come from privacy advocates; other pressures are going to come from the industry side. I'm not sure where that's going to go. I could see almost anything on the table.

We are also going to see two other elements. There's a provision in the law that allows the State Attorney General to issue guidance about the law, and there is the possibility of regulations promulgated under the law. Now both of those have timing issues, because there's not a ton of time between now and 2020. The California government is going to have to go through this law pretty carefully and figure out where a bunch of these ambiguous points are. For example, are HIPAA business associates covered or not covered? It would be useful to everyone if they could explain that. Some of the ambiguities they will be able to explain; some they may say need to have a legislative fix. So, I think companies should begin evaluating how this law would apply to their business. Begin thinking about the data that they have. Begin organizing the data that they have. If they've done a GDPR compliance exercise recently, they may have already gone through some of that activity. If they haven't done GDPR, this may be new. I think that sort of front-end information gathering effort will be worthwhile. I would wait a little bit to finish all your preparations, because it's clear that there will be some changes to the law in some way. And so, I don't think you want to get too far down the compliance road, but I also don't think you want to wait until the end of the clarification process. That process of reevaluating the law, giving guidance and considering regulations, could continue until the last minute. So, you want to get prepared now. That's going to be important but you're also going to want to wait a little bit before you make all of your final decisions on how you're going to implement this law.

**Marianne Kolbasuk McGee:** Finally Kirk, the law goes into effect in January 2020, but when does enforcement begin and what sorts of noncompliance penalties do organizations need to worry about?

**Kirk Nahra:** Unlike some of the other laws we've seen, I don't see a distinction between when it goes into effect and when enforcement can, at least in theory, begin. It's not, for example, like the HIPAA rules where the law went into effect for a certain period and there wasn't going to be enforcement for two years after that. With that said, the enforcement provisions are

*continued on page 14*

one of the areas that have already generated a lot of controversy. It basically says that that if there were going to be enforcement, the government has to tell the company that there's going to be enforcement and give the company a period of time to fix the problem. If they fix the problem, there isn't enforcement at that point. So, that's an interesting provision that certainly lessens some of the concerns about people just getting something wrong or making a mistake. Privacy advocates are clearly going to say that doesn't give businesses enough incentive to comply if they always have the opportunity to fix things after notice.

But I don't think that we're going to see massive enforcement on January 2, 2020. I do think that we're going to see lots of people paying lots of attention to this law very quickly after that day. I also expect that there will be focused lobbying on trying to change those provisions, both to weaken them and to make them stronger. We just don't have a really good sense of where that's going to come out. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

*This interview was originally published on Information Security Media Group's HealthcareInfo.Security.com news website on July 9, 2018 and is available* **here**.

## Events & Speeches

### *Genetics: New Healthcare Opportunities New Legal Challenges*

**Kirk J. Nahra, Speaker**

***The Virginia Bar Association's 128th Summer Meeting***

**July 21, 2018 | Hot Springs, VA**

### *Data Privacy and GDPR Within the Life Science Industry*

**Kirk J. Nahra, Speaker**

***Q1 Productions Life Science Data Privacy Governance & GDPR Alignment Conference***

**July 26, 2018 | Philadelphia, PA**

### *Legal, Privacy and Regulatory Considerations: A Fireside Chat with Anne Kimbol*

**Kirk J. Nahra, Speaker**

***HITRUST2018***

**September 11, 2018 | Grapevine, TX**

### *Privacy Bootcamp*

**Kirk J. Nahra, Speaker**

***IAPP Privacy. Security. Risk. 2018***

**October 17, 2018 | Austin, TX**

### *I'm a Lawyer: How Can I Advise on Data Security Issues?*

**Kirk J. Nahra, Moderator**

***IAPP Privacy. Security. Risk. 2018***

**October 18-19, 2018 | Austin, TX**

### *Mastering the Evolving Law of Data Analytics*

**Kirk J. Nahra, Speaker**

***AHIMA Data Institute: Making Information Meaningful***

**December 6, 2018 | Las Vegas, NV**

## Contributing Authors


| | | |
|---|---|---|
| Megan L. Brown | 202.719.7579 | mbrown@wileyrein.com |
| Vesna Harasic-Yaksic | 202.719.4506 | vharasic-yaksic@wileyrein.com |
| Matthew J. Gardner | 202.719.4108 | mgardner@wileyrein.com |
| Bruce L. McDonald | 202.719.7014 | bmcdonald@wileyrein.com |
| Kirk J. Nahra | 202.719.7335 | knahra@wileyrein.com |
| Kathleen E. Scott | 202.719.7577 | kscott@wileyrein.com |


To update your contact information or to cancel your subscription to this newsletter, visit:

**www.wileyrein.com/newsroom-signup.html**.