PROGRAM MATERIALS
Program #2944
January 9, 2019

California's New Privacy Law and Internet of Things Cybersecurity Laws

Copyright ©2019 by Michael Bahar, Esq., Frank Nolan, Esq., Ali Jessani - Eversheds Sutherland LLP. All Rights Reserved.
Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

EVERSHEDS SUTHERLAND

Does the sun now rise in the West?

California's Consumer Protection Act and Internet of Things Cybersecurity Law, and What They Mean for the Rest of the Country

January 9, 2019

Michael Bahar, *Partner, Co-Lead of Global Cybersecurity and Data Privacy*

Francis X. Nolan, *Counsel*

Ali Jessani, *Associate**

*Not admitted to practice. Application submitted to the New York Bar.

© 2019 Eversheds Sutherland (US) LLP

All Rights Reserved. This communication is for general informational purposes only and is not intended to constitute legal advice or a recommended course of action in any given situation. This communication is not intended to be, and should not be, relied upon by the recipient in making decisions of a legal nature with respect to the issues discussed herein. The recipient is encouraged to consult independent counsel before making any decisions or taking any action concerning the matters in this communication. This communication does not create an attorney-client relationship between Eversheds Sutherland (US) LLP and the recipient. Eversheds Sutherland (US) LLP is part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.

Agenda

- Introduction to evolving threat and regulatory landscape
- General Data Protection Regulation (GDPR)
- California Consumer Protection Act (CCPA)
- Introduction to Internet of Things (IoT)
- Potential IoT Threats
- California's IoT Law
- Federal Guidance on IoT
- Future Developments

Rapidly evolving threat and regulatory landscape

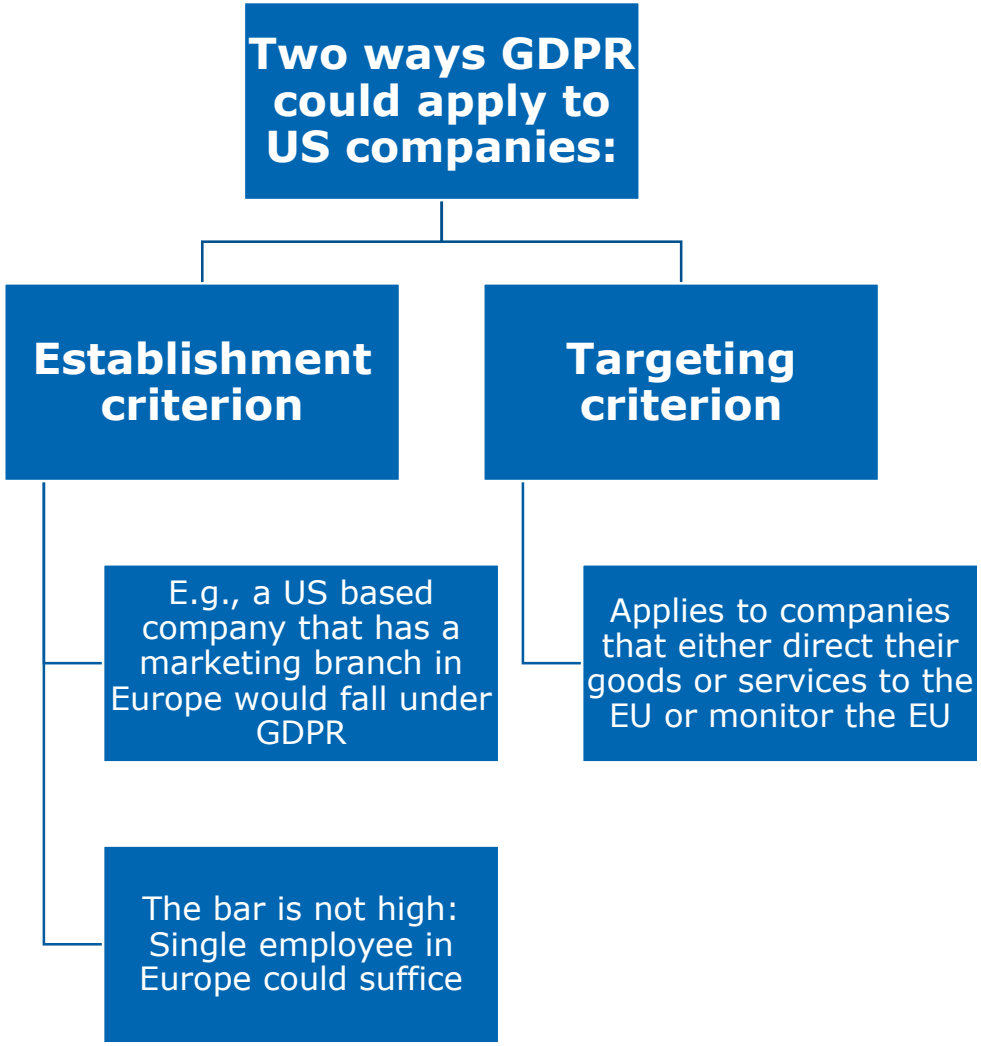
- General Data Protection Regulation (GDPR) – 2018
- California Consumer Protection Act (CCPA) – 2018
- New York Department of Financial Services – 2017
- IoT legislation and other guidance – 2018
- Securities Exchange Commission – Emphasis on cyber 2018
- State-specific rules for broker-dealers and investment advisors (Colorado and Vermont) – 2018
- 50 state data breach notification laws

General Data Protection Regulation (GDPR)

- Effective May 25, 2018
- Protects personal information (PI) and pseudonymized data
- Does not protect anonymized data
- Creates individual data privacy rights for users including:
  - Right to be forgotten
  - Right to access
  - Right to rectify
- Imposes obligations on data controllers and data processors
- Fines for non-compliance can be as high as $23 million or 4% of global annual revenue from the previous year, whichever is greater

GDPR (cont.)

— *Like CCPA, GDPR applies extraterritorially*



California Consumer Protection Act (CCPA)

- Similar, but not identical, to the GDPR
- Scheduled to go into effect January 1, 2020 and enforced in July 2020
- Like GDPR, Protects PI and pseudonymized data but not anonymized data
- Creates certain individual data privacy rights, including right to opt-out from selling data to third parties (GDPR does not have this)
- Can apply beyond California's borders, but is triggered not by what the company does, but by who the individual is
- Fines up to $7,500 per violation
- Enforceable both by the AG and by private actor

CCPA (cont.)

Four core obligations businesses face under the law

Other requirements of the CCPA

No discrimination

- A business may not discriminate against Residents who exercise their rights under CCPA – may not degrade services or charge different prices
  - A business may offer financial incentives for collection, sale or use of PI, upon notice and opt-in

Online privacy policy required

- A business must disclose the Resident's rights under CCPA, and the method of submitting the request, etc., in its online privacy policy (and in any California-specific description of privacy rights). Businesses must update that policy every 12 months

Comparing the GDPR and CCPA

The two laws overlap but are not identical

GDPR	CCPA
Applies to US companies that are either established in the EU or target EU citizens	Applies to California residents wherever they are located
Defines PI broadly	Defines PI broadly
Creates individual data privacy rights	Creates many of the same individual rights as GDPR
Requires consent or other lawful basis	Does not require consent or an otherwise lawful basis
Requires more disclosure than CCPA	Only requires businesses to disclose the categories of personal information collected and the purposes for which it will be used
Notice must be provided if data is sold to third parties but does not include a right to opt out	Requires notice and a right to opt out if data is being sold to third parties
Requires, in most situations, a company to appoint a data protection officer	Does not require a data protection officer

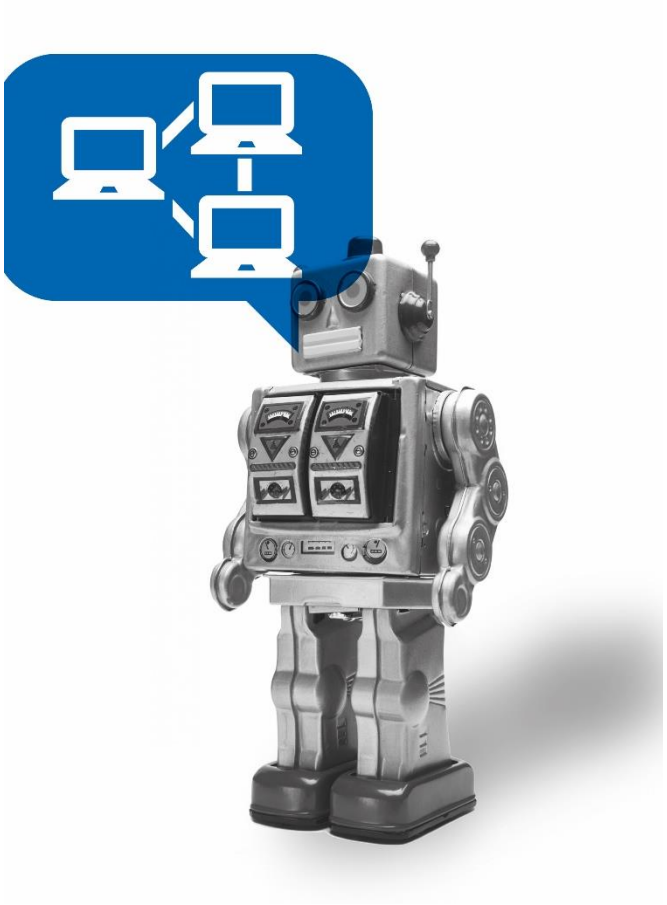
What data is protected?

Type of Data	Level of Protection	Examples
Personal Data	Maximum protection under both laws	Name; email address; phone number; tax ID number; biometric data; IP addresses
Anonymous or Aggregated Data	Not protected under either law	Aggregation of data from many users such as how many people are watching this presentation
Pseudonymized Data	Continues to be protected under GDPR; CCPA is silent	A list of individuals who are watching this presentation, with their names replaced with an identifying number and the identifying document is stored separately

Case Study: Mirai Botnet

Series of cyber attacks in 2016 highlight the risks of IoT

- Malware developed by hackers and used for large-scale network attacks
- French cloud service OVH and domain service Dyn were among the targeted
- Number of everyday IoT devices were infected, including CCTVs, home routers, printers and baby monitors



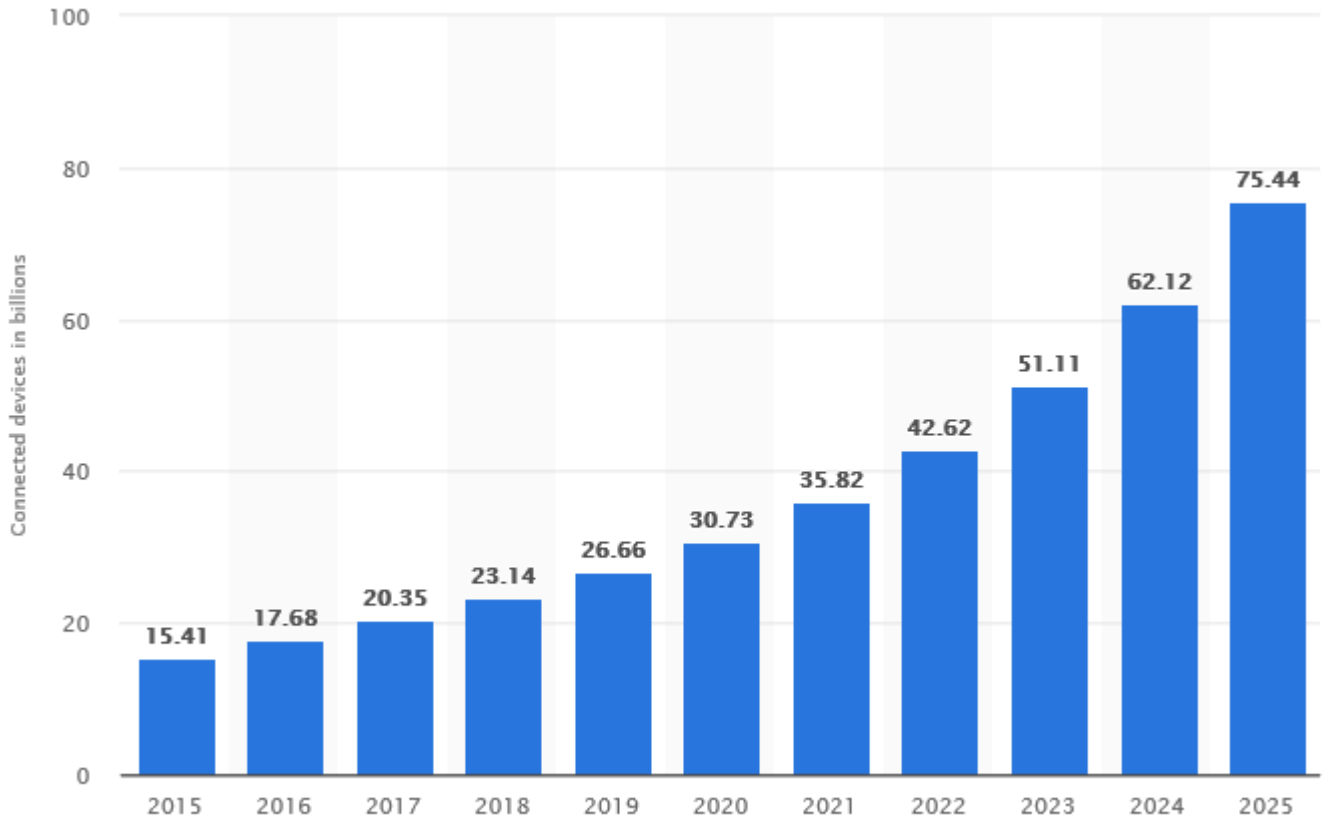
What is IoT?

Refers to embedding everyday objects with the capacity to connect to the Internet

E.g., coffee makers, laundry machines, televisions, even lamps and light switches

Booming industry

Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)



https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

With great power comes great responsibility…

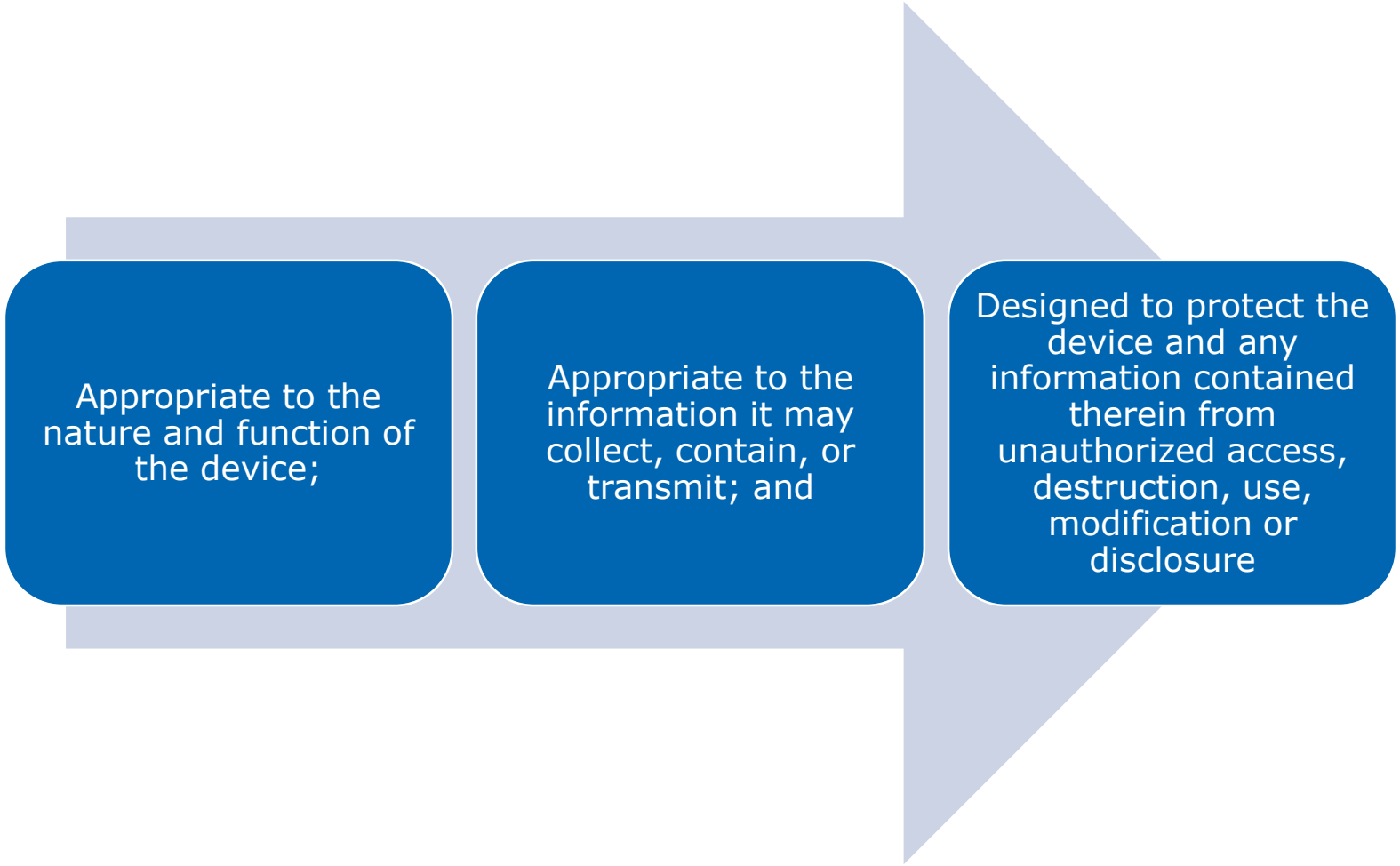
- Cybersecurity risks
  - More connected devices mean a greater risk of being hacked
  - Many IoT devices do not have software update capabilities
  - Cloud computing creates a new source of attack for hackers
- Data privacy concerns
  - IoT devices collect user PI, which can be sold to third parties

This sets the stage for… California's IoT law

- Signed into law on September 28, 2018, and will go into effect on January 1, 2020
- Focuses on IoT cybersecurity risks
- Does not specify penalties
- Enforceable by California AG and other government agents
- Litigation risk nonetheless
- No grandfathering of legacy devices

What does the law require?

- IoT Manufacturers required to equip devices with "reasonable security features"



What is a "reasonable security feature"?

- Little guidance on standard of "reasonable"
- One example of default compliance mechanism
- Connected devices that are equipped for a means of authentication outside of a local area network (LAN) can comply with the law by either:
  - Unique, preprogrammed password; or
  - User-generated unique password

CCPA's impact on IoT

- IoT law focuses on cybersecurity, while CCPA focuses on data privacy
- CCPA also creates privacy obligations for IoT manufacturers
- CCPA's "right to be forgotten" standard directly implicates a significant amount of IoT devices
- IoT manufacturers can also be subject to CCPA's private right of action

Federal guidance on IoT

- Federal Trade Commission (FTC)
  - No binding regulations
  - Examples of FTC enforcement actions relating to IoT
- Non-binding guidance from other agencies:
  - Department of Defense
  - Department of Homeland Security
  - National Institute of Standards and Technology
  - Government Accounting Office
- Congress has proposed three IoT bills in the last two years but none have gained traction

Future developments

- California IoT Law:
  - Delayed implementation?
  - Further clarification from AG?
  - Challenged in court?
- Throughout the United States:
  - Other states may follow California's lead
  - Congress could decide to preempt
- Internationally

Data privacy protections are here to stay, both domestically and internationally

EVERSHEDS SUTHERLAND

Michael Bahar
Partner, Co-Lead of Global Cybersecurity and Data Privacy
+1 202 383 0882
michaelbahar@eversheds-sutherland.com

Francis X. Nolan, IV
Counsel
+1 212 389 5083
franknolan@eversheds-sutherland.com

Ali Jessani
Associate*
+1 202 383 0950
alijessani@eversheds-sutherland.com

*Not admitted to practice. Application submitted to the New York Bar.

eversheds-sutherland.com

© 2019 Eversheds Sutherland (US) LLP
All rights reserved.

This communication cannot be used for the purpose of avoiding any penalties that may be imposed under United States federal or local tax law.

PRIVILEGED AND CONFIDENTIAL

Citations

1. Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
2. The California Consumer Privacy Act (CCPA), Cal. Assem. Bill No. 375, Ch. 55 *Privacy: Personal Information: Business* (2017-2018); codified as Cal. Civ. Code §§ 1798.100, et seq.
3. California IoT Law, Cal. Sen. Bill 327, Ch. 886, *Information privacy: Connected devices* (2017-2018); codified as Cal. Civ. Code §§ 1798.91.04-.06.
4. OECD, *OECD Technology Foresight Forum 2014—The Internet of Things* (Dec. 11, 2014), *available at* http://www.oecd.org/sti/ieconomy/technology-foresight-forum-2014.htm.
5. Growth Enabler, *Market Pulse Report, Internet of Things* (April 2017), *available at* https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf.
6. IHS Markit, *IoT Platforms: Enabling the Internet of Things* (March 2016), *available at* https://cdn.ihs.com/www/pdf/enabling-IOT.pdf.

California's new data privacy law:

What you need to know

By Michael Bahar and Mary Jane Wilson-Bilik

Companies doing business with Californians, even those located outside of California, may need to start planning to comply with California's sweeping new privacy law, even if they are already compliant with other US and European privacy laws. An analysis by the International Association of Privacy Professionals estimated that more than half a million US companies will be impacted by the law.[1] Any business with more than $25 million in annual revenue that employs or does business with residents of the world's fifth-largest economy may want to evaluate the potential impact of the California Consumer Privacy Act of 2018 (CCPA) before it goes into effect in 2020.

In addition, any company that is compliant with the EU's General Data Protection Regulation (GDPR), or working to be, may find it worthwhile to identify the overlap and the distinctions between these two privacy regimes.

Comparing the jurisdictional reach of CCPA and GDPR

The CCPA provides California residents with a potent set of new privacy rights and protections. Like the EU's GDPR, the California act has expansive jurisdictional reach. Under the act, a California resident is (i) any individual who is in California for other than a temporary or transitory purpose, and (2) any individual who is domiciled in California, but is outside the state temporarily. All other individuals are non-residents.

As a threshold matter, the CCPA generally will apply to a business that collects personal information, does business in California, and (i) has annual gross revenues exceeding $25 million; (ii) uses the personal information of 50,000+ consumers (i.e., California residents); or (iii) derives 50% or more of its annual revenues from selling consumers' personal information. The act encompasses entities that control or are controlled by such businesses, if they share common branding.

One example of a critical difference between the California and EU privacy laws is their approach to *how* the law applies.

1 Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More Than Half a Million US Companies*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Jul. 2, 2018).

Whether a US company without an EU presence must comply with GDPR depends on whether that company takes certain specific actions with respect to individuals geographically in the EU – namely, whether it offers goods or services to, or monitors the behavior of, people in the EU. The CCPA, on the other hand, applies to "consumers," defined broadly to include all California residents, and many consumer rights under the CCPA apply regardless of where the individuals are located, so long as they remain California residents.

For example, a hotel located in California will not have to afford CCPA protections to its guests who are New York or Texas residents; however that same hotel may have to afford CCPA protections to the California resident in the next room. Conversely, a hotel in New York or Texas may have to afford certain—but potentially not all—CCPA protections to its California guests, but would have no obligations under the act to guests who are not California residents. In contrast, none of those hotels must comply with the GDPR with respect to EU citizens visiting their US locations simply because those consumers are EU citizens.

Because the CCPA's requirements are based on California residency, tracking compliance obligations is potentially more onerous for companies compared to the GDPR's geographic test. The CCPA has the potential to require businesses to turn rights on and off depending on the state of residence of a highly mobile population.

What rights does the CCPA give to California residents?

The CCPA affords new rights to all California residents, including: (i) the right to request that a business disclose to the consumer the personal information it collects about the consumer, upon receipt of a "verifiable consumer request"; (ii) the right to request that a business delete any such personal information, with some exceptions; and (iii) the right to direct a business that sells personal information about the consumer to third parties to stop selling such information. These rights, which are similar to GDPR rights, are granted not only to business customers, but also to employees, patients, children, and any other California residents. This blanket approach is similar to the GDPR's, but it is a marked departure from the sectoral approach of most US privacy laws such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA).

The rights of California residents under the CCPA are designed to protect their "personal information," which is defined extremely broadly—even broader in some cases than in the GDPR. It includes:

- Any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including biometric information and geolocation data;
- "Commercial information," including "purchasing or consuming histories or tendencies";
- Internet activity, such as browsing or search history or a consumer's "interaction" with a website, application, or advertisement; and
- "Inferences drawn to create a profile of the consumer" from any of the enumerated categories.

Personal information does not even have to identify a particular person; identifying a "household" counts (e.g., residential electricity use data or an IP address). Under the CCPA, personal information does not include de-identified or aggregate consumer information. However, particularly as technology advances, truly de-identifying or anonymizing data becomes increasingly challenging.

Because the CCPA's requirements are based on California residency, tracking compliance obligations is potentially more onerous for companies compared to the GDPR's geographic test. The CCPA has the potential to require businesses to turn rights on and off depending on the state of residence of a highly mobile population.

When a business is responding to a consumer's "verifiable request," it must deliver to the consumer within 45 days a list of all categories of personal information collected, the sources of the information by category, the business purposes for collecting such information, the categories of third parties with whom the business shares (or sells) the information, and the "specific pieces" of personal information collected. A business may request an extension of the 45-day period when reasonably necessary. All of these aspects of the CCPA are subject to rulemaking by the California Attorney General.

Further, a business may not discriminate against a consumer because the consumer exercised any of his or her rights under the CCPA. But a business may offer financial incentives for the collection, sale, or deletion of personal information, upon notice to and opt-in by the consumer.

The CCPA requires a business to disclose in its online or web-based privacy policy the consumer's rights under the CCPA, the methods for submitting requests, the categories of personal information collected and sold in the past 12 months, and the business purpose for each category. The business must update that policy at least every 12 months.

Unlike the GDPR, which would require affirmative consent for the sale of personal information in most circumstances, the CCPA takes an opt-out approach to the sale of personal information. Under the CCPA, any business that sells personal information to third parties must provide a clear and conspicuous link on its homepage titled "Do Not Sell My Personal Information" to enable customers to opt out of the sale of their information.

An entity is not a third party for purposes of the CCPA if it uses consumer personal information received from a business for "a business purpose pursuant to a written contract" that prohibits the selling, retention, or disclosure of customer personal information, except under limited circumstances. This opt-out/opt-in distinction will likely require different business rules for handling personal information within those companies subject both to the GDPR and the CCPA. For example, businesses could require their customers to state up front whether they are EU data subjects or California residents, or use billing zip codes or other proxies to help make that determination.

Exceptions: When compliance with the CCPA is not required

The CCPA includes a number of exceptions, but their exact parameters and uses remain uncertain and subject to Attorney General rulemaking. Even so, many companies will likely find little safe harbor in them.

First, the CCPA provides limited exceptions for the processing of personal information that is already covered by certain federal privacy laws. The CCPA generally does not apply to:

- HIPAA-covered information;
- the sale of personal information to, or purchase of personal information in a consumer report from, a consumer reporting agency under the Fair Credit Reporting Act (FCRA) if the use of that information is limited by the FCRA; and
- information processed "pursuant" to the GLBA, insofar as the CCPA "conflicts" with it.

The exceptions in relation to HIPAA and the FCRA are relatively straightforward, but the application of the GLBA exception, which does not provide clarity on what would conflict with GLBA, may be soon amended as discussed on the next page. Along those lines, the CCPA allows for the application of any greater privacy protections existing in California, but leaves undefined what that means. Industry will likely pressure California to resolve these uncertainties between now and January 2020, when the CCPA takes effect (although, as discussed on the next page, amendments may cause enforcement to be delayed until six months after the publication of final regulations under CCPA or July 1, 2020, whichever is sooner).

Second, the CCPA provides an exception for conduct taking place wholly outside of California. Under that exception, the CCPA will not "restrict a business's ability to . . . collect or sell a consumer's personal information" if the relevant conduct takes place wholly outside of California. Under the CCPA, conduct occurs wholly outside of California only if all of the following conditions are met:

- *the business collected a consumer's personal information while the consumer was outside of California;*
- *no part of the sale of the consumer's personal information occurred in California; and*
- *no personal information collected while the consumer was in California is sold.*

Several examples shed additional light on the potential complexities of using this exception:

- Suppose a national car insurance business has insured a Texas resident who travels to California on holiday, gets into a car accident, and files an online claim in California. The company has collected this individual's personal information in California and stores the data in the cloud. However, the insured does not enjoy any CCPA rights because that person is not a California resident protected under the CCPA. However, if the insured later becomes a California resident, then the insurance company will need to either treat all of the insured's legacy data as subject to the CCPA or somehow segregate the CCPA-covered data from the data that is not covered (e.g., if certain legacy data qualifies for the wholly outside exception).
- Suppose a national retailer has a California resident as a regular online customer and customer within its California stores. If that customer travels to New York and visits a store there, the retailer may be able to take advantage of the wholly outside exception, but only with respect to the information actually collected in New York, and only if no part of the sale of that information takes place in California.
- Suppose a customer uses a virtual private network (VPN) for online shopping, which obscures the person's location. In this situation, the website operator does not know the shopper's true location. But if the website operator wants to take advantage of the wholly outside exception, the burden is on the operator to demonstrate why the collection and sale of the shopper's information took place outside of California.
- Suppose a company collects a California resident's personal information outside of California, sells that data to a data analytics company based in Seattle, but the negotiations for the sale occurred via an email service based in California. Absent further guidance, it is possible that at least a part of that data collection and sale took place in California.

There is also a degree of ambiguity about what it means not to restrict a business's ability to collect or sell personal information if the relevant behavior takes place wholly outside of California. Will businesses still be required to disclose the collection and sale of information because mere disclosure does not restrict the collection and sale of personal information? What about the right of access? While some other exceptions apply to the CCPA *as a whole*, the wholly outside exception appears only to apply to provisions that *restrict* the collection or sale of personal information.

In sum, while the wholly outside exception is available, the facts matter, and there are practical realities in trying to handle similar data differently and in keeping track of residency and data location, all of which add a degree of legal risk to this exception.

Enforcement

The California Attorney General can enforce the CCPA, subject to a 30-day cure period. The civil penalty for intentional violations of the Act is up to $7,500 per violation.

In addition, the CCPA provides a private right of action, both individually and as a class, if there is a data breach (i.e., an unauthorized access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted personal information) due to a failure to implement reasonable security procedures and practices. Filing suit requires the plaintiffs to undertake certain procedural steps, and the claim can be subject to intervention by the California Attorney General. Suits which do go forward, however, can eventually subject companies to significant liability.

Opportunities to reshape remain

Relief for ambiguity may come in the form of amendments or rulemaking—but the prospect of further legislative action could also add to the uncertainty.

California quickly passed the CCPA to avert a proposed November 2018 ballot initiative that would have required a two-thirds vote in each chamber to amend, implicitly acknowledging that more work needed to be done. In fact, amendments to the CCPA in SB 1121 were enrolled on September 7, 2018. SB 1121 is awaiting Governor Brown's signature as of September 11, 2018. If it is signed by Governor Brown, SB 1121 will make a number of changes to the CCPA. Notably, it would provide for an extension of time for enforcement (until six months after the publication of the final regulations under CCPA or July 1, 2020, whichever is sooner), make it easier to bring private claims for data breaches, and clarify the application of certain exceptions, including the exception for information governed by the Gramm-Leach-Bliley Act and its implementing regulations. Further amendments are also expected to be forthcoming, and the CCPA calls on the California Attorney General to "solicit broad public participation" when adopting the regulations that will spell out key provisions of the law, including certain definitions, notice provisions, and exceptions.

We can also expect court challenges under the theory that the CCPA unduly burdens interstate commerce, but, most likely, the CCPA is largely here to stay.

Conclusion

Given how burdensome and uncertain it is, early planning for CCPA compliance may prove beneficial. Virtually overnight, California has created a sweeping new privacy law with little safe harbor, even for businesses operating outside of California. As companies have learned with the GDPR, taking early steps to prepare for the CCPA enables smoother, more efficient implementation later. Consider sketching out a roadmap to compliance that begins with inventorying existing data collection, purposes and flows, and works through various scenarios for how to meet the CCPA challenges between now and the effective date for the CCPA.

The authors would like to thank Eversheds Sutherland alum Tony Ficarrotta for his invaluable contributions to this article.

About the authors

Michael Bahar, partner in the Washington DC office, is the co-lead of Eversheds Sutherland's global cybersecurity and privacy practice and a member of the US Litigation Practice Group. As former Deputy Legal Advisor to the National Security Council at the White House, former Minority Staff Director and General Counsel for the US House Intelligence Committee, and a former Active Duty Navy JAG, Michael provides advice on cybersecurity and privacy, international law, and national security law. While with the House Intelligence Committee, he was lead draftor and negotiator for the Cybersecurity Act of 2015, the USA Freedom Act (which reformed certain key surveillance authority), and four annual Intelligence Authorization Acts. More recently, he was leader of the Committee's investigation into the Russian hacking of the 2016 election. Michael offers clients a wealth of knowledge about cybersecurity, information sharing, privacy, crisis management, and establishing cybersecurity programs that are not only in accordance with evolving laws and regulations but that also find business opportunities. Michael can be reached at michaelbahar@eversheds-sutherland.com.

Mary Jane Wilson-Bilik is a partner in the Washington DC office, who for more than 20 years has helped her financial services clients comply with the fast-changing requirements of state, federal, and international regulations and successfully respond to evolving consumer demands in the digital economy. She has been particularly focused on the implications of the GDPR, federal, and state cybersecurity and privacy regulation for her financial services clients and their business partners. Her extensive knowledge of securities, insurance, and privacy regulations helps companies evaluate risk and reach successful outcomes. And her interest in big data, blockchain, and artificial intelligence initiatives has positioned her to be a thought leader in this space, working with many financial services companies and their business partners on emerging issues. Mary Jane can be reached at mjwilson-bilik@eversheds-sutherland.com.

LJN LAW JOURNAL NEWSLETTERS

NOT FOR REPRINT

Click to Print Click to Print or Select '**Print**' in your browser menu to print this document.

Page printed from: *http://www.lawjournalnewsletters.com/2018/12/01/sticking-a-hand-in-the-internet-cookie-jar/*

CYBERSECURITY LAW & STRATEGY

DECEMBER 2018

Sticking a Hand in the Internet Cookie Jar

By Jeffrey Higel, Michael Bahar and Mike Nelson

As convenient, useful and cool mobile technology and interconnected devices are, they come with risks that remain largely unseen or, worse, ignored. Some pose security risks, like those present in voice-activated devices that can access bank information, unlock doors, and control water temperature, and others pose privacy risks — especially for children. For manufacturers, they also pose regulatory litigation, and insurance risks, especially when children end up using their "smart" products. For example, California's recently passed Internet of Things cybersecurity law will be requiring "reasonable security features."

In addition to data breaches involving this sensitive data — compromises that could follow a child through his or her entire life—one of the key laws that makers of IoT devices have to worry about is COPPA, the Children Online Privacy Protection Act.

Collecting Data Under COPPA

Under COPPA, any company that collects information, directly or indirectly, must provide parents with detailed terms and conditions, allow parents to stop the company from gathering data at any time, take reasonable steps to safeguard the data, and delete the data once the purpose of the collection has been fulfilled.

Furthermore, the company is not allowed to distribute any child's information to any third party, with a few, limited exceptions.

But, why would, say, a refrigerator maker have to worry about COPPA? If the smart refrigerator incorporates voice-activated apps designed to promote healthy eating among children, for example, a 12 year old could have her voice "listened to," potentially recorded and acted upon. Suddenly, this refrigerator manufacturer can be subject to regulatory fines for not following COPPA to the letter.

Traditionally, only companies "marketing to children" had to concern themselves with COPPA, but with the IoT and even expansion of targeted, online advertising, more companies potentially fall into COPPA's net. To determine whether a company is marketing to children, the FTC will look at: "the subject matter of the site or service, visual and audio content, the use of animated characters …, the age of models, the presence of child celebrities or celebrities who appeal to kids" and other factors. However, COPPA also contains a catchall provision for "any operator that has actual knowledge that it is collecting personal information from a child."

If a company's website or services ask for age, grade, or any other details that allow a company to identify the age of users, then they could have "actual knowledge" of children. For example, as a result of collecting age data, the FTC fined Yelp $450,000 because, by requesting age when registering an account, they were aware of the collection of information on children under 13, and they failed to follow the COPPA notice and parental consent requirements.

While Yelp was not designed to help children find a review on the latest craft breweries or get revenge for a cold burrito, the FTC invoked the "actual knowledge" clause to fine them.

But let's say you aren't actually a website provider, but instead are in the industry of pop-up ads and spam content. Even these industries may be exposed to liability under COPPA. Third party services providers, including "ad network and plug-in [operators]" can be liable under COPPA if they are informed about the child-marketing nature of the sites for which they provide ads or plug-ins. This means even though a ten-year-old may want to learn how "a startup company has revolutionized car insurance in their zip code" or how "scientists are baffled by this one neat trick to lose weight fast," those ads may be subject to COPPA penalties, even if it is not being marketed to children intentionally.

Conversely, if you are the operator of a children's website or app and you allow third parties to collect advertising information, you can be the one held liable. For example, the app developer Retro Dreamer was fined $300,000 for allowing third-party advertisers to gather information that originated in their apps like Ice Cream Jump, Happy Pudding Jump, Ice Cream Drop, Sneezies, Wash the Dishes, Cat Basket and Tappy Pop.

COPPA Penalties

The penalties for violating COPPA vary, but they can be up to $41,484 per violation. These numbers can add up quickly, and a seven-figure settlement is not unheard of. In a recent case, the children's tech company VTech was fined $650,000 for violating COPPA following a data breach that led to the disclosure of 6.3 million children's profiles that VTech collected.

Whether through integrating "smart components" or through integrating ad companies on your website, new COPPA pitfalls abound. And there are many challenges to COPPA compliance, especially if you do not fully realize you are subject to COPPA.

Of particular interest is the requirement to delete data collected from minors, even without any request to do so. As the FTC reminded companies in a May 2018 press release, COPPA requires the data be deleted once it has "fulfill[ed] the purpose for which the information was collected." This means the burden is on companies to determine when the data has served its purpose, and they must act unilaterally to delete unused data. For those already undertaking GDPR compliance, the concept of data minimization is already familiar, even if it remains painful. But, even for those companies that have escaped the GDPR, if they collect children's data, they must know to delete it.

Another requirement concerns location information. The FTC has recently warned two foreign companies, Gator Group Co. Ltd. and Tinitell, Inc., over the distribution of mobile phones and smartwatches that were marketed to children. These devices gathered location information through the use of a GPS receiver without prior parental consent (yes, location of a child is protected by COPPA as well). These warnings also indicate FTC's determination to exercise jurisdiction even over non-US companies.

Furthermore, in a 2014 incident, Mattel was fined $250,000 for embedding YouTube videos in their websites that enabled Google to track the demographics of the user. While Mattel was careful with most of their sites, this oversight allowing for third-party tracking was still sufficient for the FTC to levy a fine. Situations such as Mattel are easily repeatable across any IoT device or website that could have third party data tracking, if the manufacturer of the device either markets to children, or knows children are using their devices.

The IoT complicates companies' duties and requirements under COPPA by putting devices in the hands of children everywhere. For example, in the VTech case, VTech's software was designed to work across various devices, some of which were portable. This highlights the threat of IoT children's devices and toys when data breaches occur. However, given the soon to be ubiquity of sophisticated IoT devices, there is a real danger that children could be entering personal information in devices that were not designed as children's toys and lack the appropriate COPPA disclosures.

For a more interesting hypothetical, let's say that an ambitious engineer decides it would be a fun feature to have a smart toaster sing "Happy Birthday" to you every year and congratulate you on your age (I'm sure we'd all love to hear our toaster remind us of our age every year). Without realizing it, that company may have just produced a non-COPPA compliant smart toaster if the device recorded a name and birth date. While it seems like a ridiculous example, it highlights the possible risks that the IoT pose to unsuspecting and well-intentioned companies.

Audio and Visual Recordings

While our Smart-Toaster (patent pending) is certainly a threat under COPPA and totally fabricated, the most realistic, novel risk under COPPA comes from the changes in the data that is protected by the Act. COPPA protects the usual "personal information" such as Social Security numbers and names, but it was extended in 2013 to have a significant IoT impact. In 2013, the FTC added any "photograph, video, or audio file that contains a child's voice or image" to its list of protected information. The FTC clarified their position in October 2017, in the eloquently named "Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings."

In the FTC's Policy Statement, the Commission delivers good news and bad news. On a positive note, the FTC clarified that this rule is not intended to require each and every voice recording to need parental consent to be recorded. For voice-activated devices (a key feature of IoT devices), voices can be collected so long as they are "a replacement for written words" that is used to "perform a search or fulfill a verbal instruction." However, these recording may be kept for only a limited time, and must be deleted almost immediately after use. Furthermore, the companies who record these voices are still required to give "notice provided by the COPPA Rule, including clear notice of its collection … and deletion policy." Finally, these guidelines do not modify COPPA in any way, so if a child is asked to give his or her name verbally or the device saves a recording online, and the company knows the speaker is under 13, there is an immediate trigger of the full COPPA rule.

A very concerning aspect of IoT devices and COPPA stems from the risk of the audio and video recordings if there is a data breach. As we saw in VTech, a company may fall victim to COPPA violations if they fail to reasonably safeguard their data. If, for instance, a company is maintaining video or audio recordings of children, even with parental consent, and there is a breach of that data, the company will likely face COPPA and private actions. It is one thing to lose names of children, but when associated pictures and voice recordings get stolen, record breaking COPPA fines and class actions may ensue.

Insurance Concerns

Whether it is VTech purposely gathering information about children or a "Happy Birthday"-singing smart toaster gone rogue, the companies that produce IoT devices may be hit by numerous claims stemming from the same cyber incident. On one hand, the FTC and state governments may bring a COPPA action on behalf of the affected individuals; on the other hand, the consumers themselves (or their parents) may have a private right of action for the theft of their data and invasions of their privacy. Additionally, the recent trend is for consumers to also push for a "quasi-COPPA" claim on the basis of state laws before they experience any harm following a breach.

Currently, companies are fending off the recent quasi-COPPA classes. VTech managed to defeat two class action certification attempts using conventional cyber defenses, first on a lack of standing without actual harm, and second, by defeating an "implied promise of security" argument. The plaintiffs of these quasi-COPPAs have taken various approaches ranging from the breach of contract/implied promises in VTech to the more recent purported class against YouTube utilizing the California constitutional right to privacy as the cause of action. Regardless of the certification of any of these classes (which to date, we do not believe any court has certified a quasi-COPPA based action), the costs associated with defending a large class action can quickly escalate.

As troubling as it is to incur the costs of litigation, IoT manufacturers may also start to feel equal heartburn over how to pay for these fines and lawsuits. Traditionally, a refrigerator or a toaster was only a risk for product defects, which are covered through a casualty policy. However, as companies continue to integrate technology into their devices, there is an opening for cyber liabilities that traditional insurance policies may not cover.

For instance, suppose a smart device with a camera is hacked, revealing access into a consumers' home and capturing family videos. In this Big Brother-esque scenario, the average casualty policy would not likely be available to cover the loss that arises due to a software vulnerability. Furthermore, as insurers continue to tighten the wording of so-called "silent cover" (coverage for cyber events in property or casualty policies) the window is closing on companies' abilities to get coverage for cyber events through non-cyber policies.

Analysis

Given all of this, what should be taken away from this discussion of COPPA and IoT?

First is that COPPA is growing as a security and privacy risk for a variety of advertising companies, e-commerce platforms, and for manufacturing companies across the board looking to develop integrated or "smart" products. Violating COPPA does not come cheap, and it can be another kick when a company is still down from a data breach. While no court has found that a data breach creates a per se violation of COPPA's "reasonable security" standard, it seems like the two actions may occur hand-in-hand when children's information is lost or stolen.

Second, whether class actions succeed in certifying or not, private class actions will occur under quasi-COPPA theories, and that can create high defense costs regardless of the outcome.

Third, even if a company doesn't market to children, a COPPA claim can be a threat within the IoT if a child inputs their personal information and a company doesn't have parental permission to collect that information.

Fourth, insurance coverage should be re-evaluated with an eye to cyber risks.

Finally, if your child's toys start asking too many personal questions, disconnect them from Wi-Fi.

*****

Jeff Higel is a Vice President – Claims Expert at Swiss Re Corporate Solutions, handling Cyber, Aviation, and Technology claims. Jeff is a New York licensed attorney. **Michael Bahar**, a partner at Eversheds Sutherland (US) LLP, is the co-lead of the Global Cybersecurity and Data Privacy team. He was previously Staff Director and General Counsel for the Minority Staff of the U.S. House Intelligence Committee, and prior Deputy Legal Advisor to the National Security Council. **Mike Nelson** co-chairs the Eversheds Sutherland (US) Class Action Team where he represents publicly traded companies and privately held corporations in complex business litigation. *This article is intended to be used for general informational purposes only and is not to be relied upon or used for any particular purpose. Swiss Re shall not be held responsible in any way for, and specifically disclaims any liability arising out of or in any way connected to, reliance on or use of any of the information contained or referenced in this article. The information contained or referenced in this article is not intended to constitute and should not be considered legal, accounting or professional advice, nor shall it serve as a substitute for the recipient obtaining such advice.*

Copyright 2018. ALM Media Properties, LLC. All rights reserved.

NOVEMBER 14, 2018

Legaltech® news

ONLINE

An ALM Publication

Right Out of the Box: California Enacts First-of-its-Kind Statute Regulating Internet-of-Things

Companies impacted by California's SB-327—especially manufacturers and distributors of IoT devices—should work to ensure compliance with the act as soon as possible if regulatory fallout is to be avoided come January 2020.

BY MICHAEL BAHAR, FRANK NOLAN AND TREVOR SATNICK, EVERSHEDS SUTHERLAND (US) LLP

The California legislature had a big year in 2018. While a great deal of attention has focused on the California Consumer Privacy Act of 2018 (CCPA), a sweeping new privacy law often compared to Europe's General Data Protection Regulation (GDPR), California also passed a less-publicized, but highly critical, statute that will regulate certain aspects of Internet of Things (IoT or connected) device security.

The IoT law, known as SB-327, should have a significant impact that extends well beyond California's borders when it goes into effect in January 2020. Companies impacted by SB-327—especially manufacturers and distributors of IoT devices—should work to ensure compliance with the act as soon as possible if regulatory fallout is to be avoided come January 2020.

What does the IoT statute cover?

As "smart" devices, like internet-connected refrigerators, coffee makers and even industrial control systems for the nation's critical infrastructure, become more prevalent, the opportunity for device hacking and improper use becomes more widespread and potentially more devastating. For example, the Mirai botnet, which took down a large swath of the internet in 2016, gained control of poorly protected IoT devices and used them to carry out one of the largest Distributed Denial of Service (DDoS) attacks on record.

On a more personal level, the proliferation of integrated cameras and sensors, often with easily hackable manufacturer default passwords, provides hackers with a ready means to peer into, if not break into, homes. With SB-327, California seeks to address these and related security concerns head-on.

What requirements does the IoT statute impose?

The primary way in which SB-327 will attempt to address IoT security risks is by directly imposing security requirements on the device manufacturers themselves. In contrast, regulations like the GDPR, New York's Department of Financial Services Cybersecurity Regulation (and even, implicitly, the CCPA), only call for third-party security reviews. Specifically, SB-327 will require companies offering IoT devices for sale in California to equip their products with "reasonable security features." The obvious question then becomes, what does "reasonable" actually mean?

Unfortunately, "reasonable" features are not specifically defined in this context. Instead, SB-327 uses a principles-based approach, encompassing security features that are:

1. Appropriate to the nature and function of the device;
2. Appropriate to the information it may collect, contain or transmit; and
3. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification or disclosure.

This approach will require manufacturers of connected devices to continuously assess the risks attendant with these products, and incorporate security features commensurate with those risks, preferably (and most cost effectively) at the design phase. Manufacturers must also be prepared to document their risk-based decisions in the event that their reasonableness decisions are challenged.

In addition to the principles set forth above, SB-327 also provides certain reasonableness floors. For example, any IoT device that can be authenticated outside a local area network (LAN) must either come with authentication unique to that device, or require the user to "generate a new means of authentication before access is granted to the device for the first time." A connection outside a LAN usually refers to the ability to access the functions of a device from anywhere with an internet connection, as opposed to a limited connection available only when connected to same network as the device in question. This is similar to the difference between an intercom system, accessible only from within the building it is located in, and a landline telephone network, where any line is accessible so long as one is connected and dials the appropriate number.

Looking elsewhere, including how other regulators approach risks associated with IoT devices, can also help inform what is considered "reasonable." In fact, reasonableness standards around IoT device security under California law will likely come to mirror those developed around other products, services and systems that are vulnerable to a cyberattack. For example, regulators across industries are increasingly urging multifactor authentication security systems in other products and services, instead of just usernames and passwords. In addition, the National Institute of Standards and Technology is currently examining ways it can standardize encryption methodologies for these devices, and regulators will likely consider those standards when they are released. Another example is the Food and Drug Administration (FDA), which recently released its "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook" as an increasing number of medical devices become part of the IoT. The report provides a number of preventative actions, many of which could also come to represent reasonableness across industries. For example, for each medical device, the FDA advises a "Hazard Vulnerability Analysis" to better understand and potentially address the effects an attack on that device could have. The guide goes further and provides particular examples of mitigation strategies, like isolating legacy devices that cannot be easily secured and connecting those devices to their own protected network.

Other sources of insight into the likely meaning of reasonableness include the Department of Homeland Security's "Strategic Principles for Securing the Internet of Things" and the Federal Communications

Commission's discussion of IoT devices in its "Cybersecurity Risk Reduction" white paper.

How will the IoT law be enforced?

Fortunately, SB-327 does not provide a private right of action, and the law will be left to the California Attorney General and other state attorneys to enforce. On the other hand, to the extent these connected devices violate—or contribute to violations of—the privacy of its users, or are subject to third-party breaches, the CCPA can provide consumers with the ability to bring a civil complaint.

The CCPA may apply in other ways, too. For example, California residents have the right under the CCPA to request deletion of personal information collected. Section 1798.140(o)(H) of the CCPA includes "[a]udio, electronic, visual, thermal, olfactory, or similar information" under the definition of personal information, which directly implicates a number of IoT devices.

As is typical of the new wave of cyber and privacy regulations, there is no explicit grandfathering of legacy devices under SB-327, meaning that California could take the position that retrofitting is required to achieve compliance with the statute. Although it is unlikely that California will take that position, it does raise the question of whether IoT devices should, going forward, allow for remote security updates to maintain the requisite level of "reasonable security features" under the law. In addition, companies may want to consider how early in their production cycles they need to implement changes to make sure compliant devices are entering the supply chain no later than the effective date.

Conclusion

Ultimately, as IoT devices proliferate throughout supply chains and our homes, the benefits in efficiency and convenience they offer will come with increased cyber and privacy risks. California, in passing SB-327, is the first state to anticipate and attempt to prevent against those kinds of vulnerabilities, but it will likely not be the last state to do so. Companies that manufacture and distribute IoT devices will be required to comply with this and other laws, and sufficient security features will need to be put in place. More importantly, however, these same security features can prevent against breaches and hacks, and the resulting regulatory enforcement actions and litigation.

Although SB-327 is not scheduled to go into effect until January 2020, now is the time to plan and come into compliance with the law. This is particularly true for manufacturers, which will need plenty of lead time to design and implement the necessary security features.

Michael Bahar *is a partner in the Washington DC office of Eversheds Sutherland (US) LLP where he co-leads the firm's global cybersecurity and privacy practice and is a member of the firm's litigation practice.* ***Frank Nolan*** *serves as counsel in the New York office of Eversheds Sutherland (US) LLP. He defends class action lawsuits and complex business litigation matters in federal and state courts throughout the country.* ***Trevor Satnick*** *is a staff attorney in the New York office of Eversheds Sutherland (US) LLP where he focuses on the full range of data issues, including data privacy and security, cyber risk and cyber breach responses, e-discovery and information governance.*

Originally published on Corporate Counsel. Reprinted with permission from the November 14, 2018 edition of Legaltech News. © 2018 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 010-11-18-04