SheppardMullin

4 Privacy Law Predictions For 2019

By Liisa Thomas

Law360, January 23, 2019, 5:55 PM EST
2019 promises to be an interesting year for privacy. As we start the year, looking forward at likely trends is at the forefront of everyone's minds. Part of that exercise is to see if anything that happened in 2018 will continue to occur this year. That seems almost guaranteed. In 2018 there was unending breaking news on the privacy front. It seemed like no week went by last year without some sort of privacy development — whether it was a big breach, analytics that influenced elections, or new sweeping regulatory regimes. This is sure to continue in 2019.

Will the headlines be the same, though? What types of issues will come up? What will be litigated? What new regulations will be issued? I anticipate four trends: (1) focused efforts from corporations to get into compliance with the California Consumer Privacy Act prior to the Jan. 1, 2020, effective date; (2) enforcement of U.S. global organizations under the EU's General Data Protection Regulation; (3) increased concern around tracking of individuals; and (4) continued enforcement activism in the U.S. by states.

Focused Corporate Effort Around CCPA (and Other Laws?)

The California Consumer Privacy Act, which is set to go into effect Jan. 1, 2020, has been widely read, widely reported on and widely worried about. Businesses covered by the law are those that do business in California and that get personal information and either (1) have more than $25 million in gross revenues, (2) have information about more than 50,000 consumers, or (3) make more than 50 percent of their revenue from selling personal information. The California attorney general is spending the beginning of 2019 doing a listening tour throughout the state as the office gears up to write regulations, which don't need to be issued until July 1, 2020. That six-month gap (the law effective in January, regulations not issued until July) isn't the only thing causing confusion.

The law requires companies to provide consumers with certain rights, including access (what information does the company have about them?), opt-out (from the sale of information) and data deletion (with many exceptions), and also adds many new notice obligations. Among the notice requirements is a requirement to provide a statement about how information will be used at the time of collection. So, for example, in an offline environment like retail, how will companies make this happen, from a practical perspective? How will they provide the rights contemplated by the statute?

And more fundamentally, who is a consumer? And what companies are covered? As to the first, consumers are "residents" of the state of California. Defined as someone in the state for longer than a transient period. Does that include employees? A vendor's employees? This is just one example of the many questions that have been raised. To keep the confusion going, there are rumblings that other states will pass similar laws

this year.

Clarification may not be forthcoming in the first quarter (or two) of this year, but even without it we will likely see much effort spent by lawyers trying to understand what this law means for their companies. In addition, the access requirements (what do you have about me?) will likely also mean companies are going to be spending time in 2019 looking at their data architecture and understanding how to manipulate it to be able to respond to these new rights.

And one preview for 2020: The CCPA provides for statutory damages in the event of a data breach. That goes into effect before the regulations, namely Jan. 1, 2020. And there is a private right of action for this part of the law (while not for the rest). There will thus likely be an increase in class actions following the announcement of a data breach, with the landscape looking much like what we see today under laws like the Telephone Consumer Protection Act or the Song-Beverly Consumer Warranty Act. Companies updating their breach response plans in 2019 will want to keep this in mind, thinking about how they can respond to incidents both promptly and properly in advance of this increased exposure.

Enforcement Under GDPR and Ongoing Scrutiny of the EU-U.S. Shield Program

The CCPA will sound like old hat for those who spent 2017 and 2018 addressing the EU's GDPR. Now that the law is in effect, continued enforcement (the flurry of enforcement started in the latter half of 2018) throughout Europe seems all but guaranteed. The prime focus of initial efforts will probably be — if activity in 2018 is any guide — those companies who have suffered a data breach. Did the companies provide sufficient protection for data? And if not, was that the result of the breach?

The hope, however, is that for those entities that do suffer a breach, that will not be the only reason that a regulator in Europe scrutinizes them. Indeed, there will be too many breaches for regulators to give each and every one scrutiny. Instead the question — with luck — will be whether the breach caused significant harm and that harm was caused by the action of the companies. As with U.S. regulators that have been receiving reports of breaches for years, the EU regulators will soon find that they cannot examine every single breach that is reported to them.

Also on the plate of regulators will be those companies who are engaged in extensive use of data, the technology companies that seem to be making the news on a frequent basis. For example, in 2018 the U.K. (which as of this writing is still a part of the EU!) brought action against a Canadian analytics company for its targeting activities. The company, AggregateIQ Data Services Ltd., used voter data to target users prior to elections. Also of concern will be problems under the law that would have been violations prior to GDPR. For example, insufficient consents or passive tracking without notice and choice.

Companies outside of the EU will continue, in 2019, to be concerned about the

enforcement actions brought under GDPR. Specific to U.S. companies, there will be an ongoing worry about the status of the EU-U.S. Privacy Shield program. The program was developed as a mechanism for easier data transfer between entities in the EU and the US. Built into the program is an annual review by the EU. The question: is data provided sufficient protection under the program? The program has passed the EU's scrutiny the first two years. Will it make it a third?

More Concern Around Tracking Of Individuals

The Illinois Biometric Information Privacy Act (get consent before you collect and use things like fingerprints) received a lot of press in 2018. The concern over the collection of use of irreplaceable identifiers in unlikely to cease in 2019; individuals aren't going to be able to get new fingerprints (although they do have 10) or retinas, after all.

A related concern for regulators in 2019 will likely echo what we saw in 2018, namely focus on connected devices and new and novel ways of gathering information. Companies are realizing that they can gather more unique identifiers, and engage in that gathering outside of the realm of the traditional phone or computer. Internet of things devices are proliferating. Cars, refrigerators, washers, dryers, scales — the list is endless. Everything is connected. And the collection of unique information can occur even in the most innocuous of items: Kids toys featured in 2018. It is no doubt because of this that California passed the first IoT law in 2018, which will go into effect Jan. 1, 2020. Other jurisdictions may follow this year.

Not only are the identifiers getting more and more unique, and the types of devices that collect them more widespread, but companies are combining these data points across their organizations. And often with others. This activity will also no doubt receive regulatory and legislative focus in 2019.

In the U.S., State Regulators Continuing to Become More Active

Companies will continue to be scrutinized in 2019 after something goes wrong. EU regulators are gearing up to increase examination and enforcement in Europe. In the U.S., states will likely get more active. Whether the problem that first came to attention was a data breach, many laws provide state regulators with authorization to bring action. The Children's Online Privacy Protection Act was an example where a federal law — enforceable by the Federal Trade Commission — saw state enforcement actions instead. New Jersey brought two cases for violations of COPPA. Other states may follow.

U.S. state regulators were also active in bringing cases under the Health Insurance Portability and Accountability Act in 2018, and this activity may continue in 2019. The federal law, which applies to providers of health services, has provisions regarding the level of protection that must be given to protected health information. Twelve state attorneys general last year felt that two medical information companies had not provided sufficient protection, and it was that insufficient protection that led to a breach. Similar

state settlements — including ones where multiple states reach a joint settlement with a company — may occur in 2019.

There are other federal laws that provide states with enforcement rights. This includes CAN-SPAM, the Telemarketing Consumer Fraud and Abuse Prevention Act, and the TCPA. It is possible that 2019 will see state action under these federal laws as well.

Finally, on U.S. breach notice front, states regulators won't be the only active ones. Legislators will be continuing to make edits and tweaks to the existing data breach notification statutes. Already this month, Massachusetts modified its breach notice law, with changes going into effect in April 2019. It is highly unlikely that it will be the only state with changes to its breach notice law.

Conclusion

What can you do to prepare your company for all that is to come on the privacy front in 2019? Keep your eyes open for CCPA developments, and think about how your organization will respond to access requests. Even if you aren't subject to California's laws, be proactive in the event that another state passes a similar statute. Do you do business in the EU? Think about what you would do if you became the focus of regulatory scrutiny, especially if your company suffers a breach. That said, the hope is that regulators will start to focus on the "big" problems rather than trying to find scapegoats.