Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# 3 Privacy Law Predictions For The New Year

By **Liisa Thomas** (January 1, 2020, 11:56 AM EST)

Liisa Thomas

As 2019 draws to a close, and companies recover from the stress of preparing for California's Consumer Privacy Act, one question keeps coming up: How can we have greater predictability in our management of privacy compliance?

There have historically been two primary hurdles to overcome. First, as demonstrated by the CCPA, there is no end to new regulations. Second, enforcement priorities seem to constantly shift. The exercise of looking back over the past year and trying to predict the regulatory and enforcement landscape of the coming year can go only so far, especially when we know that new laws will inevitably crop up, and in forms that we were not anticipating. The preparatory efforts can become that much harder when enforcement actions take a new and unexpected direction.

In looking at legal, regulatory and enforcement privacy trends for 2020, companies may want to take a new approach. Rather than try to guess what direction the law will go, ask: What steps can we as a company take to be prepared for those directions? There are some essential steps privacy officers can take now to prepare for 2020 — and beyond.

1. First, think about how you can integrate your privacy program into your corporation. Given the ongoing privacy developments anticipated in 2020, corporate privacy offices will become more and more important. Taking steps now to align your team with the goals of your organization will make accomplishing your compliance tasks that much easier.

2. Have a clear understanding of your data collection and use practices. Many of the laws we have seen in the past years have required companies to make disclosures about their practices. Each law seems to add to the overall disclosure obligation. Rather than having to conduct new diligence each time a law is passed, have a clear understanding of your practices that you can pull from to craft new notices.

3. Be dynamic. Be prepared to update notices and provide rights to new consumers. Whether it is "privacy by design" as you develop new products, or thinking about privacy as you onboard a new data storage system, being prepared to address potential future disclosure requirements will make your privacy program more flexible.

With these three suggestions in mind, thinking about the upcoming trends for 2020 should hopefully

feel less stressful, and addressing them more achievable. Keeping with the theme of three, here are three trends to be on the lookout for in 2020.

**New York and other states will join the CCPA bandwagon.**

New York leads the pack on states that are contemplating — or have contemplated over the course of 2019 — broad privacy laws. Other states included Texas, Massachusetts and New Jersey. The New York law started to receive traction again in late November 2019 and mirrors the CCPA in many respects. Unlike the CCPA, as currently contemplated, the New York law would include a private right of action and the concept of a "fiduciary duty" between a company and the individual whose data the company holds.

The law was initially proposed by Democratic New York Sen. Kevin Thomas earlier in 2019 and was referred to committee in May 2019. It sat for some time, with legislators in New York hoping for a federal privacy law. Finding no movement in that realm, the bill has again received attention. Many anticipate that this law may be the second broad state privacy law. If this happens, companies will need to address the requirements of not just CCPA during 2020, but also requirements from New York, as well as other states who may seek to join in the regulatory fray.

Even absent a law from New York — or elsewhere — companies will be impacted during 2020 by other lesser state privacy laws. Many of these have existed for some time and are based on how a company uses information (telemarketing and telephone solicitations), the type of information a company collects (biometric information), or the industry a company is in (telecommunications, healthcare financial services, etc.).

**Companies will continue to focus on the CCPA.**

Two significant CCPA developments will result in preparedness efforts stretching into 2020. First, in late 2019, the CCPA was amended to address how companies should provide notice and certain rights to employees. This included both the company's own employees and employees of third-party companies.

For the company's own employees, the law requires giving notice to employees about information collection and use practices. That requirement begins (or began, depending on when you read this!) in January. For employees of third-party companies, the more significant rights (notice, access and deletion) do not need to be provided until in January 2021. The company's own employees are slated to get access and deletion rights in January 2021 as well. This delay until 2021 means that many companies will find their CCPA preparations continuing in 2020.

The second CCPA development that will have an impact on companies in 2020 is the law's regulations. Released in draft in October, the regulations received significant commentary (and criticism). The regulations aim to give detail to companies on — among other things — how to provide notice to covered individuals, how to verify identity of rights seekers and how to respond to rights requests.

As it is unlikely that the regulations will be finalized before companies close for the holidays (or if they do not close, before personnel take a few days off to spend with their families), it is reasonable to anticipate that most companies will be addressing compliance with the final regulations in the early part of 2020.

**Privacy regulations and enforcement will pick up around the globe.**

In 2020, Brazil's privacy law (General Data Privacy Law) will go into effect. That law, passed in 2018, is similar to the European Union's General Data Protection Regulation. It is not, however, identical. For example, those seeking to exercise access rights are entitled to responses in a much shorter time frame, and the definition of personal information is broader.

Brazil will likely not be the only country with a GDPR-like privacy law, and companies will be tasked in the coming year (and beyond) to develop and design scalable approaches to privacy. This will include having the flexibility to provide rights to many individuals (not just Europeans and Californians) and the ability to dynamically update privacy notices.

In addition to new laws, enforcement actions will likely continue. Many enforcement actions were brought in 2019 for violations of GDPR. In the U.S., we saw many cases brought against companies who had allegedly failed to protect personal information. For example, in a case settled at the end of the year, the Federal Trade Commission alleged that Infotrax Systems failed to use reasonable security, resulting in a hacker accessing its servers unnoticed at least 17 times. As a result, the bad actors accessed sensitive information, including Social Security numbers and payment card information. These enforcement actions are likely to increase in 2020.

**Conclusion**

2020 may be the start of the "roaring 20s" in the privacy realm. Privacy regulation and enforcement are likely to pick up pace, and companies will need to be prepared. Having a dynamic and flexible approach to privacy will allow companies to address these trends on a proactive rather than reactive basis.

Understanding your data uses, aligning your privacy team with your organization's mission and being prepared to make changes to your practices will serve privacy teams well as we enter into the next decade. Part of being dynamic will likely result in many companies rethinking how they approach to their privacy programs. This will include how companies conduct and maintain the diligence needed to keep their notices current and their responses to access requests accurate.

---

*Liisa M. Thomas is a partner and leader of the privacy and cybersecurity practice group at Sheppard Mullin Richter & Hampton LLP.*