SheppardMullin

2020 Privacy Law Trends And How They Affect Compliance

By Liisa Thomas
Law360, December 22, 2020, 1:16 PM EST

Most of us will be happy to see the end of the year 2020. My children's favorite phrase? "2020: one star. Would not recommend." Most of us feel the same way.

While we may be looking for a few silver linings we can draw from this difficult year, some days they seem few and far between. But perhaps there are some we can glean on the privacy front. When we think about the developments in privacy laws and enforcement in 2020, there are many trends from which we can develop steps to prepare for 2021.

Several privacy trends from 2020 stand out from which we can glean learnings:

1. Transborder Data Flows

This summer the Court of Justice of the European Union found that the EU-U.S. Privacy Shield was an invalid mechanism for transferring personal data from the EU to the U.S. In its decision in Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, or Schrems II, the court concluded that standard contractual clauses could still be used, but only if the exporting entity took "additional measures" to make sure information was protected.

The Swiss and Israeli governments followed suit, and companies exporting information into the U.S., and their U.S. counterparties, now find themselves back at the negotiation table to hash out what extra security measures might be needed. This work will continue, as the current set of standard contractual clauses are being modified by the EU. While it is anticipated that they will be approved early in 2021, there will be a grace period until 2022 for companies to switch from the old to the new ones.

U.S. companies that do participate in the Privacy Shield program — which is operated by the U.S. Department of Commerce and has not yet been terminated — will hopefully get some relief in 2021. For right now, they find themselves bound to a program that no

longer delivers the benefits it was intended to produce.

2. Data Exchanges Between Companies

Companies may find themselves back at the negotiating table as a result of changes in the EU. Or, they may still be at the table hashing out "third-party/service provider" language under the California Consumer Privacy Act. Or perhaps they have been focusing on the transfer of personal information back and forth to other companies for data security reasons, wanting to take appropriate measures to address various state laws or regulator expectations.

Whatever the reason, privacy laws impact third-party relationships and will continue to do so in 2021. Companies will likely find themselves next doubling down in the new year on mapping and understanding the flow of personal information between them and other companies.

3. Ongoing Enforcement

2020 may not have been like any other year in many respects, but in one respect it was very similar to prior years. Government regulators continued to bring privacy and data security actions against corporations that they felt failed to use personal information in ways that complied with the law or that resulted in data breaches.

Similarly, there was much action on the class action front. Perhaps most active were cases brought under the Illinois Biometric Information Privacy Act. In May, the U.S. Court of Appeals for the Seventh Circuit issued a decision, Bryant v. Compass Group USA Inc., that greatly increased the number of BIPA suits filed in the latter half of the year.

The Seventh Circuit found that there was a sufficient claim of injury if the plaintiff had not given the law's requisite consent. After that decision, companies found themselves on the receiving end of many more BIPA allegations, and will likely continue to receive these in 2021.

4. Laws With Ever-Changing Effective Dates or Requirements

Many heads reeled trying to follow if the Brazil general privacy law would go into effect in 2020 — and when it would happen. First it was delayed, then it wasn't, then it was. And in the end, it wasn't delayed, and went into effect in the fall of 2020.

While companies have a year from the effective date (until August 2021) before sanctions are imposed, it is precisely this kind of stop and start with privacy laws that makes privacy officers nervous. Does one get the company started down the road to compliance if the law does not go through? Or if it is passed, will it be modified multiple times like the CCPA? The preparatory steps described in this article should help, as we do not anticipate the stops and starts for these laws changing anytime soon.

5. Impact of the Privacy Patchwork

It is bad enough to watch developments about new privacy laws, but what about those privacy laws that already exist? There are so many. Email marketing, text message laws, biometric laws (discussed above), children's privacy laws, laws around video rental history, laws that impact recording electronic communications, and much, much more. While companies may have forgotten about some of them, regulators and class action attorneys have not.

For example, the Federal Trade Commission settled with HyperBeard Inc., maker of the kids' app KleptoCats, for its alleged failure to obtain parental consent. We do not anticipate enforcement for these specialty laws decreasing in 2021, even if companies' focus is only on the big laws like the EU General Data Protection Regulation and the CCPA.

Putting Steps in Place to Prepare

It is clear that the world of privacy is going to continue to change at a rapid pace in 2021. What steps can companies take to be prepared for these developments? One of the best is to think about privacy not as a technical issue to be solved, but instead a broader issue facing the organization that requires a more adaptive and holistic approach.[i]

To ensure that an organization can address ongoing privacy changes, there needs to thus be a culture of compliance. This culture change means winning over hearts and

minds, not simply implementing a new slate of policies.

Another important, but often overlooked, step is a related one. Namely, to think about how to get those policies and procedures that are adopted actually implemented and followed by all within an organization.

What resistance might these new policies and procedures face? What stakeholders will be forced to give things up as a result of the changes? What other losses might be suffered? Can those be mitigated? Are there advantages that will inure to the company's benefit that balance this out? Taking time to think through the answers to these questions before attempting to launch new processes can make a huge difference.

Finally, being prepared for ongoing changes means having a privacy office and privacy culture that is nimble and has adopted some guiding principles. These broad principles can make it easier for a company to face a new regulation. As, ideally, the principles the company has adopted already take into account the nuances introduced, and the new law will require only minimal changes to the company's current practices.

What's Next?

Think about the developments from 2020, and previous years, as you develop your 2021 privacy toolkit. Be prepared for an active year of privacy and data security enforcement, and take advantage of holistic steps to get prepared. Avoid starting in the middle, remember partners, be holistic in your remediation, train appropriately, and don't "set and forget."

These are just a few things that can start your year well, even if 2021 brings more of what we have seen in 2020.

---

[i] See e.g., Heifetz, Ronald, et al., The Practice of Adaptive Leadership: Tools and Tactics for Changing Your Organization and the World (2009).