CEP Magazine - July 2021
A US federal privacy law will be no magic bullet

By Joey Seeber

Joey Seeber (jseeber@levellegal.com) is the CEO of Level Legal in Dallas, Texas, USA.

Who in their wildest dreams would imagine corporate general counsel (GC) clamoring for more regulation? Despite the prospect of additional statutory hoops to jump through, this is the sentiment heard at a recent in-person roundtable I attended and was the number one topic of conversation among a group of senior GCs, who expressed their desire for federal privacy legislation to replace the mash-up of different state privacy compliance laws. For years, GCs have skirted the issue with ever-increasing levels of budget and manpower, but they are eager to see this burden alleviated by an overarching federal law that delivers consistency, predictability, and clarity.

These hopes are showing some signs of becoming reality. Following the 2020 US election and a string of pandemic-induced delays, proposals for federal privacy legislation are moving ahead. In particular, a bill sponsored by US Rep. Suzan DelBene (D-WA) is supported by multiple stakeholders ranging from tech giants to corporate GCs, whose privacy holy grail would be a single, comprehensive federal law that would reduce the growing burden of privacy compliance. These views are representative of nationwide concerns about the difficulty of privacy compliance under the current fractured, state-by-state system.

Almost without exception, corporations want and need to be compliant—particularly if they are publicly listed. Yet privacy compliance is becoming more and more difficult to navigate, as the landscape has become so confusing: California, New Mexico, Maine, and Virginia, for example, already have significant consumer privacy laws; New York, Massachusetts, Maryland, and Hawaii have new laws in the works. Some 25 additional states[1] are at various stages of the legislative process, with some holding out altogether and playing the waiting game. It's no wonder this patchwork approach is a challenge for any organization with a nationwide footprint to navigate. This complexity has a significant impact on the administrative and financial overhead of compliance professionals, as well as their organizations' potential exposure.

Demand for concrete and consistent federal privacy guidelines is real and growing, and our multijurisdictional approach to privacy is certainly a key driver. However, there is another driver for change that receives less attention but is equally important: data.

The double-edged data sword

For many companies, data rank among their most valuable assets, but they are also viewed as a huge compliance risk. Now that the legislative environment is pivoting decisively toward regulating how consumer data are protected and managed, the potential consequences and liabilities of failure to comply present new and growing risks.

For example, in mergers and acquisitions (M&As), privacy is becoming a higher priority on the due diligence checklist. For their part, regulators are increasingly observant about compliance infringements, while the acquiring companies are under pressure to ensure they are not inheriting a legacy of privacy issues and liabilities. Federal Trade Commission (FTC) oversight in merger enforcement has been intense in recent months.

Describing 2020 as "a fiscal year like no other,"[2] the FTC recorded its busiest merger enforcement year since fiscal year 2001; multiple actions were amended or abandoned even before the second request stage. As pre-M&A due diligence grows more intense, privacy compliance inevitably moves closer to center stage in transactions. Failures in compliance can lead to collapsed deals or substantial reductions in purchase prices.

Also, as more states customize their privacy legislation, we can expect even more compliance challenges to emerge. Juggling state-by-state privacy compliance laws[3] is not impossible, but companies working in more than one jurisdiction will need to pay particularly close attention to their data to maintain compliance. While large companies have the ability to devote resources to the problem, the expense and personnel it takes will grow exponentially as more states introduce their own privacy legislation.

The challenges for companies and legal and compliance teams could be dramatically reduced if there were a common set of standards, but enactment of new federal legislation may initially add to the compliance burden, at least for the next few years, before things get any better.

What could a federal privacy bill achieve?

In an ideal world, preemptive federal legislation would standardize privacy compliance, and each state would know exactly what they were meant to do. Indeed, this would be the perfect outcome for the bill's bipartisan supporters. The new legislation would require companies to disclose whether they share private consumer data and would preempt most, although not all, existing state privacy laws. But this level of clarity is unlikely to exist for some time to come.

Demand for a streamlined federal law exists in certain pockets of the country—especially in tech-driven West and East Coast states. However, the nationwide pain is not yet sufficiently acute to generate a groundswell of demand for overarching preemptive legislation. Until additional motivating factors come into play, comprehensive, preemptive legislation is not likely to be passed.

In the meantime, we are most likely to see baseline legislation, which individual states can supplement with their own additional provisions. This would put at least some guardrails around the growing, amorphous mass of privacy compliance rules. A baseline bill will likely contain some standard consumer protections such as the right to know what personal data are collected and whether the data are sold or disclosed, the right to access personal data collected, and the right to request that a business delete any personal data.

No magic bullet

While adding a federal set of standards lays the groundwork for more streamlined privacy laws, in the short term, it will inevitably create duplication of work as federal initiatives are added on top of state-by-state regulations. Ultimately, though, a comprehensive federal privacy law could deliver more certainty, predictability, and consistency.

It's important to remember, however, that legislation alone does not create change. Just as regulators and legislators debated issues like internet taxation over many years until a 2018 Supreme Court judgment in the *Wayfair* case fundamentally changed the rules,[4] federal privacy legislation will take some time to mature. It will ultimately be shaped by multiple forces, including:

- A heightened focus on consumer data protection in every jurisdiction, pushing privacy compliance to a prime position on the due diligence checklist.
- Existing enforcement guidelines and fines by state and federal regulatory authorities such as the

Department of Justice.

- Increasing numbers of cases being argued through the judicial system, whose outcomes will mold future legislation.

Shaping the federal bill

One of the most interesting aspects of a new federal privacy bill would be the ability to unite seemingly disparate interests. It might be sponsored by a bipartisan coalition pushing for more consistency and certainty, and supported by larger, predominantly technology-led organizations. The most active sponsors are likely to be those legislators whose constituents are most affected by the variable compliance laws—in particular, companies headquartered in California who are feeling the effects of the California Consumer Privacy Act (CCPA) more than other states.

We might also see lobbying for interests that reflect companies' different data-led business models, coupled with lively debates between those who are focused on privacy and security rather than those for whom the monetization of data is key. Ultimately, this could promote the prospect of singular federal data privacy legislation. This, in turn, could influence state legislation in much the same way that the EU's General Data Protection Regulation influenced the shaping of the CCPA. Over time, federal legislation might create a baseline for all states, anchored by the common goal of offering greater protection to individuals and regulating how businesses may handle their personal information.

Prepping for more privacy regulation

As regulatory enforcement increases, seminal cases are litigated, and more states enact privacy regulations, a federal standard will become more likely. The implications of any federal legislation for businesses, especially those with significant personal data assets, could be enormous for the unprepared.

In anticipation of future comprehensive federal legislation and as privacy moves higher on the corporate priority list, companies should act now by assessing their data management processes, workflows, and controls to ensure their compliance protocols will remain robust. In preparation for more stringent privacy laws, companies should take steps to ensure they have rigorous data retention policies in place around how they manage employee data in case of data subject access requests, which will inevitably increase as a result of GDPR and CCPA. For companies preparing for an acquisition, now's the time to set more controls around data management strategies and remediate any that are not cohesive in terms of privacy compliance.

The professional and organizational implications of a federal privacy law could also have direct implications for companies' technology and security requirements, since it will necessitate intensive collaboration between information technology, data management, information governance, compliance, and legal teams. The intensity of the impact will depend on whether there is a size-of-business threshold regarding the imposition of these requirements—and whether the organizations affected are prepared or taken by surprise.

There is no question that the privacy compliance field will remain challenging. Now is the time to put workflows, processes, and data management in order to ensure they are built to accommodate future changes. If in doubt, bring in expert help to brace for the inevitable shifts and surprises to come in this most complex of environments.

Takeaways

- Act now to ensure your organization's privacy compliance practices are robust.

- Increase focus on data management processes, workflows, and controls.
- Put stringent employee data retention policies in place.
- Set controls around data management strategies and undertake any necessary remediation.
- Encourage closer collaboration between information technology, data management, information governance, compliance, and legal teams in anticipation of new federal legislation.

1 Sarah Rippy, "US State Comprehensive Privacy Law Comparison," IAPP Tracker, last updated April 26, 2021, https://bit.ly/39Vzcfi.
2 Ian R. Conner, "A Fiscal Year Like No Other," *Competition Matters* (blog), Federal Trade Commission, October 6, 2020, https://bit.ly/3urFWJQ.
3 Andy Green, "Complete Guide to Privacy Laws in the US," *Inside Out Security* (blog), Varonis, updated April 2, 2021, https://bit.ly/3eZ3pM3.
4 Diane L. Yetter, "South Dakota v. Wayfair is Decided: What Does It Mean For You?," Sales Tax Institute, June 26, 2018, https://bit.ly/3h8ttqK.