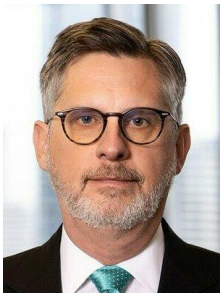
A Federal Data Privacy Law Is The Disaster We Urgently Need

By **Roy Wyman and Colton Driver** (August 24, 2022)



Roy Wyman

Colton Driver

Privacy is so hot right now. When China, India and Utah — for heaven's sake — are passing laws, you know it's moved past a fad and become an inevitable wave of change.

While the rest of the world, and some individual U.S. states, have moved ahead with comprehensive data privacy statutes, the U.S. federal government thus far has failed to pass a law covering all industries throughout the country, and some significant roadblocks remain to passage of the American Data Privacy and Protection Act, or ADPPA, introduced in June, or any similar bill.

The problem, of course, is that businesses can't keep up. For multistate — not to mention multinational — organizations, the legal landscape has become a zombie apocalypse.

Large entities can address a zombie or two, but the problem with zombies is that eventually they surround you, and running from one may send you directly into the hoard.

Costs of compliance with these statutes can easily rise into the millions, and that investment still doesn't guarantee security from regulatory enforcement or even — depending on a plaintiffs lawyer's creativity — class actions.

Understandably, large businesses are pushing hard for a federal privacy law and, no matter how inept a legislature may be, big businesses usually get their way on Capitol Hill.

So we know one thing with as much certainty as is possible in this area of the law: A broad federal privacy law will eventually happen.

It will be an absolute train wreck. And we still need it.

Why is it necessary?

The zombie apocalypse of 51 separate laws with inconsistent requirements will, at maximum, create enormous costs, confusion and headwinds to businesses and the economy generally.

At minimum, it will cause many companies to simply ignore nuances, comply with what's easy and build in set-asides to pay the inevitable regulatory fines.

Current laws work for almost no one and have had little impact on the actual privacy of personal information, which was the purported purpose for these laws.

Yes, every website now has a privacy policy. Nearly every browser window includes a pop-up banner. Privacy laws have created yottabytes of legal language that almost no one reads — other than regulators and plaintiffs attorneys.

And yet, your personal data is already everywhere. The current laws do very little to keep data in the U.S. from being sold by data brokers, and more laws requiring notice or consent are unlikely to change that reality in the near term.

Why will it be a disaster?

Privacy laws are doomed from the start for two implacable reasons.

First, legislating an abstract concept like privacy is impossible to do perfectly. The ideas involved are simply too slippery and subject to changing public concerns.

Second, technology is developing faster than any law can keep up. For example, there are sharp arguments about the current state of autonomous vehicles, but one must broadly assume that the technology will develop to a point where it will save thousands of lives.

The problem? That technology depends on knowing exactly where the vehicle is — your geolocation, which is often considered sensitive personal information.

Do we let people die in order to protect against knowing their locations? Do we give up on the concept of individual privacy for the broader social good?

Can we at least make it less of a disaster?

Let's manage expectations: Our hope is that federal legislation will create consistent rules across all states and industries.

With regard to states, the legislation will need to fully preempt all state and local laws. Prior privacy laws, such as the Health Insurance Portability and Accountability Act, only preempted state laws that were less rigorous.

That approach — setting a floor — will not work here, as it leaves open the potential for contradictory laws and an unnecessary drag on the economy with no clear benefit.

Field preemption — where Congress does not allow for any state legislation about the same issue — would drastically simplify compliance, but admittedly could prevent states from legislating where necessary to account for the inevitable shortcomings of a federal law.

Such full preemption, however, seems the only viable alternative though a bit of a Catch-22. Let's face it though, what are the chances that state legislatures actually improve the legal landscape rather than make compliance with 50 different laws impossibly confusing?

The proposed federal law, the ADPPA, actually did include field preemption with minor exceptions, and now it's encountering headwinds from state regulators like the California Privacy Protection Agency as well as congressional representatives with both too much pride of ownership in a law that was slapped together in order to avoid a legislative nightmare and misplaced faith in regional solutions to a global problem.

With regard to application across industries, there are two concerns.

First is that we have a current patchwork of laws that are industry-specific — e.g., the Gramm-Leach-Bliley Act for financial institutions and HIPAA for health care.

Permitting a situation where HIPAA and the GLBA continue to exist after a general privacy

law is enacted creates a scenario where, for example, the front of your local pharmacy is subject to one complex set of privacy laws and the back of your pharmacy — where the drugs are — is covered by separate, inconsistent and perhaps more lax laws.

The second concern is that many proposed bills would only cover entities that are subject to Federal Trade Commission jurisdiction. This would not cover certain niche industries or nonprofits.

While the ADPPA does currently include nonprofits, recent FTC rulemaking does not, and is far from a cure-all. The result is that your local burger franchise could be subject to higher standards of privacy than your employer, your church or the local pregnancy counseling center — which, in the post-Roe v. Wade legal world, has become an additional hurdle for the ADPPA because it has brought some shortcomings in that law to light.

Privacy's role has always been characterized by tension with public good, and the job of Congress is to weigh relevant trade-offs to come up with thoughtful compromises.

From the start, the concept of privacy was in tension with First Amendment rights to a free press and free speech. Today, additional trade-offs are required between privacy and the ability of companies to function and deliver goods.

Technological innovations commonly require the provision of personal data in order to actually be innovations. Is there a line between necessary uses on one hand and abuse on the other? Certainly.

Finding that line, though, will be a near-impossible task for current representatives, some of whom may learn most of what they know about technology from watching their grandkids.

What pitfalls should federal legislation avoid?

While we remain pessimistic even in the wake of attempts from Congress, our hope is that eventual federal legislation might avoid some of the clear ditches into which other laws have gleefully leaped.

First, as noted above, many current laws rely primarily on concepts of notice and/or consent. This arises from the belief that the problem isn't what a business does with personal information, the problem is that individuals don't know, and agree to, that use.

There is far too much data flying around, however, for most individuals to have the time or inclination to review every relevant privacy notice and consent to each use. And what some businesses do with personal information is itself highly objectionable.

Next, there is a distinction made between controllers — broadly, businesses that decide what to do with your data — and processors, who are usually vendors. Two broad problems arise with this distinction.

First, it's often difficult to distinguish between them — who is the relevant holder of your information, the Marriott that rents you a room or Sabre, the reservation system that collects your payment and other information and uses it for many different hotels?

Second, why do we care about the distinction? If a vendor loses your data, is that any less problematic than if the controller is the one who loses it?

Third, all sorts of silliness has crept into definitions. The term "personal information" has grown so broad as to potentially include random information, while information that sophisticated entities can use to discover personal information about you is unprotected.

In the end, the boundaries are so vague that one ends up seeing private information as akin to U.S. Supreme Court Justice Potter Stewart's threshold for obscenity in his 1964 Jacobellis v. Ohio opinion: "I know it when I see it."

Finally, one must be concerned with how a federal privacy law would be enforced. Privacy advocates will push hard for a private right of action as exists in the European Union: Any individual harmed by an improper disclosure can bring suit.

Those advocates will, justifiably, point to other privacy laws — e.g., the Children's Online Privacy Protection Act — where years of lax enforcement have only recently been the subject of interest by regulators, and a number of companies have largely skirted with impunity the burdens associated with COPPA.

While this concern is warranted, allowing individuals to take legal action directly could also lead to frivolous suits and increased exposure to litigation for companies.

That, in turn, could breed counterproductive behaviors across industries, much like a doctor performing unnecessary procedures — or not performing necessary procedures — out of fear of suit.

Perfect balance may not be possible, so any legislation is likely to err in one direction or the other, but hopefully any private right of action included in a law will be well-reasoned.

Currently, the ADPPA includes a broader private right of action than existing state laws, but whether that will remain part of whatever federal law passes remains to be seen.

Don't let rationality get in the way of optimism.

Now, to leave things on a slightly brighter note: As we said at the start, in spite of the hurdles standing in the way of a comprehensive law and the reasonable degree of certainty that it will be a disaster when it passes, the U.S. desperately needs federal privacy legislation.

To start, while states should be given credit for taking the first steps to protect their citizens, the long-term effects of Congress not acting and all 50 states passing their own variations of a privacy protection law will be an even more monumental disaster. U.S. businesses are currently drowning in a river of state privacy laws that is becoming deeper and wider each time another law passes.

There are significant differences from jurisdiction to jurisdiction, making it difficult for organizations to comply in a timely and coherent manner. Quite simply, it's a moving target, and each time a company's compliance strategy gets finalized, there is a new law to analyze.

The legal landscape of a 50-state patchwork would make compliance cost prohibitive for legal teams and completely unfair to businesses that are trying to do the right thing without providing any more incentive for businesses that are not doing the right thing to change their ways.

Moreover, such a patchwork is the worst of all worlds because protections stop at state borders when organizations need a way to standardize data practices across the entire country — and internationally, but let's not get ahead of ourselves.

The prospect of a federal data privacy law also improves our chances to help craft international policy on these issues and strengthening our relationships with long-standing allies. In a world where data has become king, privacy is a new diplomatic frontier.

A law that establishes sufficient protections to earn the U.S. adequacy status for international transfers from the EU would also remove massive roadblocks to conducting business that currently exist when companies reach across the Atlantic Ocean.

Now what?

There is a lot of work to do before any federal law passes, regardless of when that happens.

We are hopeful that when a bill finally gains enough traction, it will preempt the murkiest parts of state and industry-specific laws, allow for appropriate and timely enforcement without crippling companies with meaningless litigation (looking at you, Illinois Biometric Information Privacy Act), do away with vague and meaningless rights and burdens, and be substantial enough to alleviate the burden on international organizations by finally showing that the U.S. cares about its citizens' data.

But we aren't betting on it.

Roy Wyman is a member and Colton Driver is an associate at Bass Berry & Sims PLC.