The Chaos Of Privacy Compliance In The US

By **Alyssa Boyle**

Tuesday, September 27th, 2022 – 8:45 am

Share:

An interview with
Dominique Shelton Leipzig
Partner

MAYER | BROWN

One of the main questions people seem to have about a potential federal data privacy law in the US is similar to a question many have pondered about the end of third-party cookies in Chrome.

Is it ever going to happen?

Eventually.

But the future of the recently proposed American Data Privacy and Protection Act (ADPPA) is now decidedly up in the air, and the Federal Trade Commission (FTC) is exploring the possibility of creating new rules to try and fill the void.

Meanwhile, there's still no consensus between regulators and digital advertising companies on what types of data should constitute personal information, said Dominique Shelton Leipzig, a partner at the law firm Mayer Brown focused on cybersecurity and privacy compliance.

In the absence of a federal data privacy law, she said, states are passing their own, which makes compliance complicated.

Leipzig spoke with AdExchanger.

AdExchanger: Will the US ever pass a data privacy law?

DOMINIQUE SHELTON LEIPZIG: Yes, but not this year. It's possible for something to be passed in 2023 that goes into effect in 2024.

House Speaker Nancy Pelosi was pretty explicit that the American Data Privacy and Protection Act isn't going to be brought to the House floor until its authors address the issues that the California delegation has with it. California Privacy Protection Agency Director Ashkan Soltani also wrote that the proposed law has less privacy protections than the California state law, and a federal law should be a floor, not a ceiling.

But there's a lot happening at the federal level right now. The Securities and Exchange Commission is releasing cybersecurity proposals for public companies, and the FTC is exploring a privacy rulemaking process on "commercial surveillance."

What's the biggest obstacle standing in the way of a federal data privacy law?

It's mostly a state preemption issue.

The California delegation is concerned that a federal law would preempt state law with fewer protections and prevent stricter state laws from existing.

But in reality, some of the protections in the proposed federal law are actually greater than California's state law.

The California Privacy Rights Act (CPRA) doesn't incorporate a concept of civil rights, for example. The federal proposal, which has bipartisan support, does that and arguably makes the proposed law more expansive than California's.

How does preemption work?

Historically, when a federal law doesn't have full preemption, it preempts any law that's less restrictive but allows for more restrictive ones.

A good example is the Health Insurance Portability and Accountability Act (HIPAA). We don't usually hear about state health laws as much as we hear about HIPAA, but laws like California's Confidentiality of Medical Information Act are still allowed to exist [and they're enforced] because they're considered to be more restrictive than the federal law.

I think the concern about preemption could be mitigated. The problem is that California legislators, including the governor and the state AG, feel that even with modified preemption, the difference in standards is just too great.

And it's not just privacy advocates who are concerned. Businesses are concerned that if a federal data privacy law doesn't have full preemption, then they'll have to comply with multiple state laws in addition to a federal one.

Is California's privacy law the most stringent of the five states that have one?

Yes.

The CPRA is the strictest privacy protection we have in terms of state law and, naturally, both state and federal regulators are going to look to it as an example. California was the first state to pass a data breach notification requirement and it's also the first to expressly define dark patterns.

Colorado has some opt-out provisions in common with the CPRA, but they're less prescriptive and, generally speaking, the Virginia and Utah models are even less restrictive. But other states will continue rolling out laws that fluctuate between California and these other models.

What will happen as more states pass their own privacy laws?

It's creating a big burden for companies.

Businesses need certainty, which can't happen if there are fluctuating norms across different states. That also makes it harder to guarantee the protection for consumers that advocates are looking for.

Will a US federal privacy law have more in common with state laws or the GDPR?

It's hard to say. The ADPPA has components that aren't in the GDPR, such as civil rights concepts, but also misses provisions that are included in the GDPR, such as certain data subject rights. But the ADPPA didn't match the GDPR the way other countries' laws have tried to do, like Brazil's.

What does all this mean for the FTC's rulemaking process?

The FTC doesn't want to make their rulemaking dependent on whether or not the federal law passes. Commissioner Lina Khan has already been moving forward and making statements about commercial surveillance. She's been using that term publicly since the spring.

The FTC is already moving to fill the void, and it's interesting because the two Republican-appointed commissioners have objected to proposed rulemaking so far. **[Related: Why Commissioner Noah Phillips says rulemaking belongs in Congress.]**

It's still a delicate time in terms of the FTC's rulemaking authority.

In the meantime, should companies focus on self-regulation?

Self-regulatory models are fine for companies to be engaged in – but they're no substitute for complying with the state laws that are out there.

There's still a disconnect between regulators and digital advertising teams over whether – and which – persistent identifiers constitute personal information.

Digital advertising teams have to understand that enforcement ethos is changing.

This interview has been edited and condensed.