Hashed & Salted | A Privacy and Data Security Update
March 2025

Vol. 4 No. 1

2025 is here, bringing new laws, a new administration and fresh challenges for companies navigating the privacy landscape. In this issue, the first of 2025, our Privacy group leaders share their insights on key trends to watch and how to be ready for regulatory, legislative, litigation and technical developments in privacy, now and in the coming year.

The Regulatory and Legislative Landscape

Robyn Mohr, Deputy Chair, Privacy, Security & Data Innovations

Two months into 2025 and just over a month into the second Donald Trump presidency, we don't yet have a clear picture of what privacy at the federal level will look like, but some privacy issues are starting to come into focus.

On the Hill, Republicans hold the majority in the 119th Congress—controlling both the House and the Senate. The margins in both chambers are thin, so any legislation (including federal privacy legislation) will likely require some bipartisan support. Sen. Ted Cruz, R-Tex., now chairs the Senate Committee on Commerce, Science and Transportation, which is responsible for legislating data privacy and artificial intelligence (AI) issues. While privacy may not be the committee's top priority, it still seems fairly high on the list, and some think Sen. Cruz will try to refocus the comprehensive data privacy discussion around legislation that more closely resembles the new law in his home state, the Texas Data Privacy and Security Act. While the odds for comprehensive federal privacy legislation are never that high, the chances of passing privacy legislation during this congressional term seem about as good as they've been previously (but then again, we usually start the year with a lot of optimism).

At the Federal Trade Commission (FTC), Chair Andrew Ferguson has said he is focused on the negative effects of Big Tech, and he recently issued a Request for Information (RFI) on censorship by technology platforms. We also expect the FTC to continue pursuing enforcement actions around sensitive data practices. Where the previous FTC was very focused on sensitive health information, the new FTC under Chair Ferguson is likely to focus more on sensitive location information and how that information can be aggregated, sold and shared. And as Mark Meador said at his recent confirmation hearing for the open

commissioner seat, children's privacy likely will also be a major enforcement priority for the FTC.

While privacy does not seem to be a top priority for the executive branch (at the moment), we expect to see various executive orders (EOs) that will have privacy implications. Just last week, Trump signed an EO titled "Ensuring Accountability for All Agencies" that would give the president more control (and more oversight) over not just executive agencies (those administrative agencies housed in the executive branch, like the Department of Homeland Security) but also independent agencies (those housed in the legislative branch, like the FTC and Federal Communications Commission). Under the EO, the chairs of independent agencies must regularly consult and coordinate policies and priorities with the directors of the Office of Management and Budget (OMB), the White House Domestic Policy Council and the White House National Economic Council. This enhanced coordination could impact the investigation and enforcement activities of agencies like the FTC.

Tracking Tool Litigation

Caroline Hudson, Deputy Chair, Privacy, Security & Data Innovations

We're generally keeping tabs on tracking tool litigation across the country, with a focus on putative consumer class action filings involving uses of particular tracking technologies on websites and alleged violations of older statutes. For several years now, companies have faced an onslaught of actions claiming violations of statutes like the California Invasion of Privacy Act (CIPA), similar state wiretapping laws and others, such as Arizona's Telephone, Utility and Communication Service Records Act. These claims are generally tied to companies' use of various tracking technologies on websites, in apps and in emails, including tools like cookies, pixels and beacons. The plaintiffs allege that companies engage in wiretapping or otherwise invade privacy when they collect information, including about engagement or browsing history, through these tools and use that information to identify individuals.

These lawsuits go through a cycle of sorts, in which plaintiffs try out new theories and courts either give them credence or start rejecting them. Some courts continue to grant plaintiffs leeway to proceed on these claims, particularly with respect to more recent CIPA claims related to the use of pen registers and trap-and-trace devices, so this area remains unsettled. We are seeing a few more decisions in favor of businesses. A recent ruling from the Supreme Judicial Court of Massachusetts narrowed the scope of the state's wiretapping act and provided a significant win for defendant companies. Other courts have thrown out CIPA allegations—in some instances without granting plaintiffs the ability to amend their complaints. In particular, we're looking for a California appellate court to issue something definitive about the viability of these kinds of claims.

We're also keeping a close eye on litigation developments related to the Video Privacy Protection Act (VPPA). Initially, courts narrowly applied the statute's definitions of "videotape service provider" and "consumer/subscriber" to entities that seem to actually provide video-related services and those who subscribe to those video services. Then, late last year, the Second Circuit issued a decision in *Salazar v. Nat'l Basketball Ass'n* that provided a sweeping, plaintiff-friendly interpretation of the statute and then applied it narrowly to a specific set of facts. The court determined that the plaintiff actually could be a consumer for VPPA purposes just by subscribing to the NBA's email newsletter and providing his personal information. The Second Circuit also declined to limit the goods or services covered by the statute to audiovisual materials only. As expected, we've seen a number of follow-on filings of new VPPA cases by plaintiffs' lawyers—in jurisdictions within the Second Circuit, in particular, but elsewhere as well—and are closely monitoring additional developments in the case law.

Finally, there's a meaningful chance that we'll see more enforcement related to how companies implement and configure cookie banners and consent management tools. Some of this enforcement activity may be related to state comprehensive privacy laws, but regulators in states without privacy laws have enforcement options as well. Every state has its own unfair and deceptive acts and practices (UDAP) statute, and certain implementations of

tracking tools, consent mechanisms and options could be deemed deceptive or misleading under these laws. For example, in July of last year, the New York State Attorney

General issued guidance on website privacy controls, noting that "more than a dozen popular websites, together serving tens of millions of visitors each month," had privacy controls that were "effectively broken." Expect more state attorneys general—and plaintiffs' firms—to scrutinize how companies operate their sites and apps, including how they utilize tracking technologies within them.

Technical Solutions to Privacy Challenges

Jessica Lee, Chief Privacy & Security Partner; Chair, Privacy, Security & Data Innovations

Recent waves of state privacy legislation and regulatory guidance have fundamentally changed how data-driven businesses operate. As organizations race to implement AI solutions, they face a challenging paradox: an increasing need for data access amid tightening restrictions on data collection and use.

In response, companies are turning to technological solutions to balance privacy requirements with innovation. We're seeing particular momentum in three key areas: privacy-enhancing technologies (PETs), data clean rooms and advanced de-identification methods. While PETs were still in their testing phase when we first covered them, they've now become essential tools for privacy-conscious organizations.

Data clean rooms have emerged as a popular solution across industries, allowing companies to analyze data while maintaining privacy safeguards. It's crucial to understand, however, that clean rooms alone don't guarantee privacy protection. The most effective implementations combine clean rooms with advanced PETs like homomorphic encryption and secure multiparty computation, enabling collaborative data analysis without exposing sensitive information.

The FTC has taken a nuanced stance on these technologies, noting that while data clean rooms can enhance privacy protection in some cases, they can also be used to obscure privacy violations in others. With regulatory scrutiny intensifying at both the state and federal levels, we expect an increased focus on companies making misleading claims about privacy-preserving technologies. State regulators may pay particular attention to the use of technology to mask privacy violations.

Data Brokers and Sensitive Data: A Regulatory Bull's-Eye

We are also monitoring the data broker space as these companies appear poised to face increased scrutiny in 2025. From California's DELETE Act to new restrictions on sensitive data collection to the U.S. Department of Justice (DOJ) crackdown on bulk transfers of data, the data broker industry is facing regulatory pressure on multiple fronts.

At the end of 2024, the DOJ issued the final rule implementing President Biden's Executive Order 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The rule establishes the first national restrictions on personal data transfers to countries of concern—including China and Russia. It broadly defines "data brokering" to include data sales, access licensing and even indirect transfers through third parties. U.S. entities are prohibited from engaging in covered data transactions with organizations substantially controlled by or based in these countries. While the Trump administration has promised to dial back some of the previous administration's focus on privacy, we don't expect to see the same shifts in areas that impact national security.

At the state level, 2025 began with New York passing stricter health information protections, and similar legislation is pending in other states across the nation. Meanwhile, California, Texas and Oregon continue to prioritize data broker enforcement, a trend we expect will continue throughout the year.

What's Next? How To Prepare Your Privacy Program for 2025

With 19 comprehensive state privacy laws on the books and many more working their way through state legislatures, preparing a multistate privacy program is critical for 2025. Here are our recommendations.

- **Update Your Data Mapping.** All privacy compliance programs require you to have a detailed understanding of your data flows. Where and how is data being collected? Where is it going or who are you sharing it with? Data mapping is a foundational piece of a multistate privacy program and can also help identify areas for further inquiry. Data mapping often helps determine whether you are collecting sensitive personal information or information from children, or engaging in tracking or advertising activities that may require additional compliance obligations.
- **Understand Your Advertising Activities.** The California Consumer Privacy Act isn't the only legislation that imposes obligations on sales or shares of personal information. Most of the state privacy laws in effect for 2025 include a right to opt out of targeted advertising In order to honor this opt-out right, you first need to know what advertising activities you are engaged in and what technologies, tools or vendors are part of that process. As noted, wiretapping and tracking technology litigation is only going to increase. Now is the time to understand whether you have advertising cookies or tracking pixels or other technologies on your sites (and if so, which ones) that enable your company to engage in targeted or cross-context behavioral advertising.
- **Review Your Privacy Documentation.** While many states require data protection impact assessments (DPIAs) for risky types of processing activities, privacy documentation is not just data mapping and DPIAs. With the mosaic of state laws, you should be reviewing (and documenting) your privacy compliance practices, including how you honor and respond to consumer rights, your record retention policies and your information security requirements. With the increased enforcement activity we expect to see at the state level (whether it's a request for information, a civil investigative demand or a warning letter), it will be important to have the right policies in place and to have them documented in the right way.

Team Member Spotlight: Teodoro "Teddy" Shelby

How did you develop your area of focus?

I really like to learn how things work, and I was drawn to privacy exactly for that reason. I love being able to dig into the weeds about how data flows in order to provide the shows and movies we watch, the brands we buy, the news articles we read, the podcasts we listen to, the vehicles we drive, and the devices and apps we use. Layered on top of that is the need to figure out how to accomplish all of it while complying with a complex web of laws that regulate data in any number of ways. I see each project as an opportunity to work together with a client on a complex and intriguing puzzle. Plus, I enjoy seeing in real time how laws and regulations are made—locally to globally—through the lens of privacy. It is extremely eye-opening and invaluable for putting together those puzzle pieces for clients.

What's exciting you/grabbing your attention right now?

Besides having secured my ticket for Beyoncé's Cowboy Carter tour? I'm interested to see how the privacy landscape evolves this year—what growing pains we experience, so to speak, from the legislative, enforcement, litigation, marketplace and consumer perspectives. Each one of these perspectives usually seems to have its "blinders" on, which is why the privacy puzzle never feels quite complete. Any opportunity to better understand any one of these perspectives always excites me. It makes finding solutions acceptable to all involved so much easier and creates a more collaborative atmosphere.

What's something people would be surprised to know about you?

The only state I haven't been to is Alaska. I really want to make it there by boat, with my pups (Franklin and Eleanor), and then continue on to circumnavigate the rest of the world.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Robyn Mohr . . . . . rmohr@loeb.com
Caroline W. Hudson . . . . . chudson@loeb.com