WILMERHALE

2024 Privacy Law Preview

JANUARY 16, 2024

As we have detailed previously, 2023 was a landmark year for privacy law, featuring numerous developments at the federal, state and international levels, ranging from newly enacted statutes to massive regulatory enforcement actions. Early signs already indicate that 2024 is likely to be just as active for privacy professionals, as legislatures and regulators continue to forge ahead in developing and implementing new legal frameworks to manage a rapidly evolving field. (For example, the opening days of 2024 have already seen comprehensive privacy bills passed or nearly passed in the New Jersey and New Hampshire legislatures, respectively). In particular, we expect to see continued developments at the state level (with the emergence of new state privacy law proposals and implementation and enforcement of recently enacted state laws), from federal regulators (where the Federal Trade Commission (FTC), in particular, is positioned to continue its recent regulatory focus on topics such as health data, adtech, sensitive customer information and artificial intelligence (AI)), and perhaps even the federal legislative level (though this seems unlikely given both the lack of forward progress on a law in 2023 and the fact that 2024 is an election year). Furthermore, ongoing legal developments related to AI are likely to have privacy law impacts—and vice versa. Understanding these trends will be critical not just for privacy professionals but also for legal departments more generally; indeed, a recent report found that regulatory compliance, data privacy and data protection are viewed by chief legal officers as their top three risks heading into 2024.

In this post, we summarize seven key US privacy law developments to watch as we move into 2024. To keep track of all these developments, please subscribe to the WilmerHale Privacy and Cybersecurity Law Blog.

1. Implementation and Enforcement of New State Comprehensive Privacy Laws

2023 was a breakthrough year for state comprehensive privacy laws. The number of states with such laws on the books more than doubled (from five to 12), with Iowa, Indiana, Montana, Tennessee, Texas, Oregon and Delaware joining California, Virginia, Colorado, Connecticut and Utah. 2023 also saw the Virginia, Colorado and Connecticut laws formally take effect, in addition to the California Privacy Rights Act (CPRA). And beyond these new statutory frameworks, we saw the Colorado Privacy Act Rules take effect in Colorado, as well as continued regulatory activity in California. All in all, then, 2023 was a year in which the state privacy law compliance landscape became much more complicated for companies.

2024 will present even more challenges for those companies as several of the aforementioned laws take effect. Utah was the first, taking effect on December 31, 2023. That will be followed by Texas and Oregon on July 1 and Montana on October 1. (Florida's narrower law, which largely applies only to certain large-scale data processors (unlike the other "comprehensive" privacy laws), will also take effect on July 1.) Though these laws' requirements are generally similar, they feature enough differences that businesses should be thoughtful about how to address their various compliance obligations. Companies seeking to comply with these new laws will need to carefully evaluate the relevant statutory requirements and assess how their privacy compliance programs can best be adjusted to satisfy those requirements.

2. New State Privacy Law Proposals

In the absence of any action on a federal privacy law (more on that below), we also anticipate additional states passing comprehensive privacy laws of their own in 2024. Indeed, within the past week, comprehensive privacy bills have been passed or nearly passed by legislatures in New Jersey and New Hampshire, respectively. Earlier this week, the New Jersey legislature passed a comprehensive privacy bill that had carried over from the previous calendar year. Meanwhile, in New Hampshire, a comprehensive privacy bill passed the House on January 4 and now awaits (expected) concurrence from the Senate. Other states, including Hawaii, Kentucky, New York and Oklahoma, are prime candidates in 2024 to pass comprehensive privacy laws because they all had comprehensive privacy bills in 2023 that cleared one legislative chamber. In terms of the substance of these new comprehensive privacy law proposals, if trends in 2023 hold, it is likely that most of these bills will adhere to the Virginia model and thus feature less prescriptive compliance requirements than those included in the California Consumer Privacy Act (CCPA) and CPRA.

Speaking of California, companies should continue to monitor privacy developments in the Golden State in 2024. In particular, California is in the early stages of developing new regulations related to cybersecurity audits, risk assessments and automated decision-making technology (ADMT) pursuant to the CPRA, as well as revisions to the already promulgated CCPA regulations. We expect to see more progress on these regulations in the new year, including the initiation of the formal rulemaking process. March 2024 will also see the beginning of enforcement of the CPRA regulations, which were delayed from their original July 2023 enforcement date in a last-minute court decision.

Finally, companies should keep an eye out for narrower privacy laws making their way through state legislatures. For example, more states may pass consumer health privacy laws (similar to the Washington law we discuss in the next section). Vermont is already considering such a law. Additionally, and as there were in 2023, more states may consider passing biometric-specific privacy laws similar to the laws in effect in Illinois, Texas and Washington. Finally, we may see continued legislative responses to the Dobbs

decision, as states (including California) look to provide additional privacy protections for reproductive rights information.

3. Enforcement of the Washington My Health My Data Act

2023 also saw the enactment of Washington's My Health My Data Act (MHMDA), a significant health privacy law that will create meaningful compliance obligations for companies that process health data outside of HIPAA. The challenges from this law are particularly important because the law includes a private right of action—where ambiguities in the legislation primarily will be exploited by the plaintiffs' bar rather than reviewed by regulators. The MHMDA takes effect on March 31, and we will be closely monitoring how plaintiffs utilize the law's private right of action. At this point, we expect the MHMDA to prompt significant amounts of litigation. For a model as to how the MHMDA is likely to be used by plaintiffs, we can look to Illinois' Biometric Information Privacy Act (BIPA). Though that law regulates biometric information rather than health data, it, like the MHMDA, features a private right of action and has resulted in a flood of litigation, with plaintiffs utilizing wide-ranging theories of liability and exposing companies to significant potential damages awards. Thus, if companies' experiences with BIPA are any indication, we can expect the MHMDA to be a source of significant potential legal exposure for companies within its ambit.

Additionally, companies should, of course, not neglect the fact that the MHMDA will be enforceable by the Washington attorney general (AG), as well. Companies looking to understand how the Washington AG may approach its enforcement of the MHMDA can consult our past writing on the AG's June 2023 enforcement guidance. Finally, companies should also be aware of Nevada and Connecticut enforcing their own consumer health privacy laws in 2024 (though neither of these laws includes a private right of action). Moreover, given how quickly three states moved to pass consumer health data laws in 2023, we anticipate additional laws joining this category throughout the year.

4. FTC Focus on Health Data and Adtech

Generally speaking, the past several years have seen an increased focus by regulators on privacy implications related to consumer health data and adtech. No regulator has better exemplified this focus than the FTC. Over the past year, the FTC has established itself as a leader in the health privacy enforcement space, making consumer health data a key focus of its privacy and cybersecurity mission. Furthermore, the FTC has demonstrated a particular interest in the intersection of consumer health data and targeted advertising, bringing, for example, major enforcement actions against GoodRx and BetterHelp that centered in large part on those companies' alleged misuse of consumer health information for advertising purposes (which the FTC deemed to be "unfair" practices, as we expand on below). We expect the FTC to continue to build on the precedent established by the GoodRx and BetterHelp enforcement actions in 2024, meaning that companies in the digital health space should be on high alert to ensure that their data privacy practices are transparent and feature appropriate consents for uses of consumers' personal information.

Additionally, the FTC is in the process of amending the Health Breach Notification Rule (HBNR), having issued proposed amendments in May 2023. As we have previously written, these proposed amendments would broaden the types of entities covered by the rule (e.g., to include health apps) and expand the scope of activities triggering the HBNR's notification requirements (e.g., to include unauthorized disclosure of certain health information to a third party without consumer consent). The public comment

period for these amendments closed in August 2023, so it is likely that we will see further developments in the new year.

5. Continued Expansion of Other FTC Enforcement Activities—Unfairness, Sensitive Consumer Data, AI and Future Rulemaking Activities

Beyond a continued focus on consumer health data and adtech, we expect to see four additional trends guide the FTC's enforcement activities in the upcoming year. First, the FTC is likely to continue its efforts to expand the boundaries of its unfairness doctrine. In recent years, we have seen the FTC push a muscular application of its authority to pursue actions against unfair acts or practices in the privacy and cybersecurity realm, expanding this concept, in particular, to reach companies that fail to adequately protect consumer data. Thus, to name a few examples, the FTC has levied unfairness charges against a data broker that collected and used vast amounts of sensitive consumer information without adequately informing or obtaining consent from consumers, a company that made retroactive material changes to its privacy policies, and an entity that failed to adequately respond to consumers' requests for the deletion of their personal data. Second, we expect the FTC to continue its focus on enforcement actions against companies that mishandle sensitive types of consumer information, in particular. This was a notable area of focus for the FTC in 2023, and so companies that handle sensitive information like consumer health data, genetic data, biometric data and the like should take extra care to ensure that that data is subject to robust privacy and cybersecurity controls. Third, we expect the FTC in 2024 to further wade into the realm of AI regulation. In 2023, the FTC issued a series of public pronouncements making clear that it views AI to be within its regulatory purview. 2024, then, is likely to be the year that the FTC takes more-concrete action in this arena, perhaps by beginning to bring more enforcement actions that feature AI-related deception and unfairness claims, specifically. The FTC also ended last year by bringing an enforcement action against a company for using AI facial recognition technology without implementing reasonable safeguards.

Finally, the FTC is also likely to continue to expand the scope of its enforcement authority through its rulemaking activities. For example, at the

end of 2023, the agency proposed new rules under the Children's Online Privacy Protection Act (COPPA) that, among other things, would require companies to limit their targeted advertising activities directed at children protected under the rule. Meanwhile, the FTC is still going through the rulemaking process related to "commercial surveillance and data security practices that harm consumers." We may see some movement on this front in the coming year.

6. Potential Movement on Federal Privacy Law

In contrast to 2022, when the American Data Privacy and Protection Act (ADPPA) managed to gain some traction in the House of Representatives, 2023 was a relatively quiet year for the ongoing effort to pass a comprehensive federal privacy law. It is possible, however, that we may see more significant movement on the ADPPA (or a similar bill) in 2024. President Joe Biden, for instance, called on Congress to pass bipartisan data privacy legislation as part of his recent executive order on AI. Thus, we may see more movement on a federal bill in the upcoming legislative session, either as a stand-alone effort or as part of a broader AI-related legislative package. We may also see narrower privacy proposals (as we have in years past), such as those aimed at expanding the Gramm-Leach-Bliley Act or the regulations that apply to non-HIPAA health data.

Of course, any legislative priority in 2024 will have to contend with the fact that it is an election year. This may make it (even more) difficult for a privacy bill to pass as a stand-alone effort. But, as noted above, there seems to be a bipartisan priority in Congress to develop rules governing AI use, and it would not be surprising to see privacy or data security rules come out of that effort.

7. Intersections with AI

As we have written elsewhere, AI is an object of growing focus for legislatures and regulators around the world. And while AI poses issues distinct from general data privacy concerns, the two areas overlap in significant ways. For instance, some state comprehensive privacy laws establish rights and obligations that affect companies' development and use of AI tools, such as by allowing consumers to opt out of certain uses of profiling and by imposing requirements on how companies may use the training data they feed into their AI models. Conversely, and as noted above, it is quite possible that broader AI legislative and regulatory initiatives, such as the effort underway pursuant to the Biden Administration's executive order on AI, will include certain elements that directly touch on data privacy issues. Either way, we expect developments in both the AI and data privacy spheres to be significantly intertwined in the years to come.

Authors

Kirk J. Nahra

PARTNER

Co-Chair, Artificial Intelligence Practice

Co-Chair, Cybersecurity and Privacy Practice

kirk.nahra@wilmerhale.com

+1 202 663 6128

Ali A. Jessani

SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105

Samuel Kane

ASSOCIATE

samuel.kane@wilmerhale.com

+1 202 663 6114