

What privacy issues are on deck for 2023? Here are some of the most interesting ones

December 12, 2022

2022 was a remarkable year for privacy. Utah and Connecticut enacted new privacy laws. California and Colorado launched detailed (and continuing) privacy rulemakings. Congress proposed a landmark bipartisan, bicameral federal privacy bill (the American Data Privacy and Protection Act, or ADPPA). And the FTC initiated a sweeping privacy rulemaking under its Section 18 (Mag-Moss) rulemaking authority.

As if that weren't enough, the US and EU announced a new Transatlantic Data Transfer Framework. We saw aggressive enforcement of UDAP and privacy laws at the federal and state levels. California passed an Age Appropriate Design Code (similar to the UK's), while Congress proposed multiple kids' privacy bills. And, amidst all of this, "dark patterns" and "surveillance" shot to the top of the privacy lexicon.

2023 promises to be just as active, with further twists and turns on all of the above. Notably, the five new state privacy laws we've all been awaiting and planning for will take effect at various points in 2023. Further, other states may join the fray, enacting their own laws. If 2022 was the year that regulators and companies spent positioning themselves on the field, 2023 will be the year the balls start flying.

We'll be blogging on all of this in 2023 but, for now, we want to highlight some issues we're watching with particular interest.

The State Attorneys General - enforcement plans, political change

The new state privacy laws will give state AGs (and California's new privacy cop, the California Privacy Protection Agency, or CPPA) stronger tools to protect the privacy of their residents. How these enforcers set priorities and pursue enforcement will have a substantial impact on US privacy, especially with the continuing void left by Congress' inability to pass a federal privacy law.

How quickly will the AGs and the CPPA take up enforcement? What issues will they emphasize? California and Colorado have already provided clues through their rulemakings (and through California's first formal enforcement action against [Sephora](#)). But what about Utah, Virginia, and Connecticut? While we can expect prompt action from Connecticut (a longstanding leader in state and multistate privacy enforcement, with an active privacy task force), all three have stayed relatively mum as to their intentions.

In addition, political changes at the AG level could affect privacy enforcement more broadly, including as to joint privacy enforcement under the UDAP laws. As we've reported here, some AGs are questioning the value of [multistate enforcement](#), as well as the [bipartisan nature of NAAG](#), and may increasingly peel off from collaborative efforts. Also, this fall, there was significant AG turnover

at election time, with 13 new AGs elected and additional newcomers filling the void left by AGs moving to higher office. While most of the new AGs are replacing officials from the same party, one notable exception is in Iowa, where Democratic incumbent and 40-year veteran Tom Miller lost to Republican Brenna Bird. As the country's longest serving AG, Miller and his staff were often at the forefront of consumer protection and privacy initiatives, whether visibly or behind the scene. How the new AGs will embrace bipartisan action, especially without longstanding leaders like Miller, will be a key area to watch in 2023.

The outsized influence of the California Privacy Protection Agency

Who's the most powerful privacy regulator in the US? If you're thinking it's the FTC, you might get an argument from California, Congress, or even Europe. That's because California's new privacy agency, the CPPA, is wielding outsized influence for a single-state agency, both in the US and abroad.

The CPPA's mission is to implement and enforce California's new privacy law. During the past year, the agency built out its structure while also engaging in an extensive rulemaking that captured the attention of businesses and policymakers worldwide. In March, the New York Times [profiled](#) the CPPA's director, Ashkan Soltani, in reverential terms – quoting an ally as saying he is “literally inventing a state department,” describing how Soltani met with Emmanuel Macron and other world leaders, and ending with Soltani's quote that “[w]e're building the car as we drive it.”

But there's more. In October, the CPPA became a [full voting member](#) of the Global Privacy Assembly, a global forum of over 130 privacy authorities (a status it took years for the FTC to achieve). And last summer, right after the partially-preemptive ADPPA was approved by House Commerce, the CPPA launched a [campaign](#) to stop it – which included holding a public Board meeting to oppose the bill and sending a public [letter](#) to Speaker Pelosi explaining why California's law is stronger than the ADPPA. (P.S. – it isn't, according to multiple progressive privacy NGOs – see [here](#) and [here](#).) Soon after, Pelosi [announced](#) she wouldn't even bring the ADPPA to the House floor, citing the CPPA's arguments. (ADPPA was already facing headwinds, but Pelosi's decision was a brick wall.)

With the political shift in the House, the CPPA's sway over Congress may diminish in the coming year. Further, as the FTC moves forward with its commercial surveillance rulemaking (see below), some of the spotlight will shift there. Nevertheless, we expect the CPPA's influence to remain strong in 2023.

Congress - will it or won't it act on privacy?

Speaking of the ADPPA...we're watching closely to see whether it rises from the ashes and/or whether Congress can get its act together on *any* privacy bill in 2023.

Although the ADPPA ultimately foundered over (mainly) preemption, it still got further along than any comprehensive federal privacy bill in history, passing out of House Commerce by a 53-2 vote. Also, even as the ADPPA was working its way through the House, two substantive, bipartisan bills to protect kids and teens – the [Kids' Online Safety Act](#) from Blumenthal/Blackburn and the [Children and Teen's Online Privacy Protection Act](#) (“COPPA 2.0”) from Markey/Cassidy – got [markups](#) in the Senate. There was talk that even if Congress couldn't pass a comprehensive bill, kids' privacy legislation might be an attainable goal – a bipartisan “sweet spot” amidst all the privacy drama.

Assuming nothing happens on privacy in the lame duck session, might we see federal privacy legislation in 2023? Sadly, that question remains complicated as ever. For one thing, in January, Congress will start over with a new session and some new (or reshuffled) leaders – a Republican

Speaker in the House (tbd); a new Ranking Member of Senate Commerce (Sen. Cruz instead of Wicker); and a shift from Pallone to McMorris Rodgers as Chair of House Commerce (which at least brings some continuity, since both helped draft the ADPPA and continue to support it). Will this new group prioritize privacy?

For another, if Congress does take up privacy, it's not clear how it will proceed. Will it focus on a comprehensive law, a kids' bill, or something else? Will it pick up talks where it left off or start from scratch? Will Cruz be able to reach accommodation with Senate Commerce Chair Cantwell in a way Wicker couldn't? (The recent bill from Cantwell/Cruz on [recording smart devices](#) appears designed to send the message that they *do* want to work together on privacy issues.)

Even the preemption question – always an enormous challenge – could become more complicated. As more state laws take effect, preemption becomes more urgent from an industry perspective. But as the states move further down the road in implementing and enforcing their laws, they could become more invested and entrenched, making preemption even more politically and practically difficult.

The FTC's "surveillance" rulemaking – broad and slow or narrow(er) and fast(er)?

Finally, in August, the FTC issued an Advanced Notice of Proposed Rulemaking on "commercial surveillance and data security." As we [blogged](#) then, the ANPR was remarkably sweeping in scope – posing 95 questions about "surveillance," data security, dark patterns, kids' and teen privacy, targeted advertising, algorithms, discrimination, and competition issues, among other topics. The comment period closed on November 21. According to the [docket](#), the FTC received over 1,200 comments.

Now comes the hard part for the FTC – reading the comments, writing the rule, and getting through the rest of the Mag-Moss process. As discussed [here](#), Mag-Moss's many steps include proving that each practice to be regulated is both prevalent and unfair or deceptive; allowing stakeholders to request informal hearings; assessing the costs and benefits of the proposal and why it was chosen over alternatives; and, of course, judicial review. In the past, FTC rules developed under Mag Moss often have taken many years to complete.

Will this rule take just as long? Maybe, maybe not. We'll know more when the FTC issues its NPR and proposed rule. If the rule is as broad and sprawling as the ANPR portended, then we're in for a very long haul. Likewise, if it imposes strict limits on marketing and advertising, we can expect substantial pushback from industry, multiple requests for hearings, and oversight from the Republican-led House.

On the other hand, if the rule is more tailored – for example, focusing on data security, sensitive information, and principles emphasized repeatedly in the FTC's prior cases and settlements – it might have smoother sailing. Still, given the complex and controversial nature of privacy, we'd be amazed if *any* privacy rule could be completed in 2023 (unlike the FTC's impersonation rule which, as we discuss [here](#), is moving forward at a rapid clip).

In 2023 we'll be watching all of these issues with interest and will post regular updates here.