8 Privacy Law Predictions For 2024

By **Liisa Thomas, Sam Cournoyer and Kathryn Smith** (January 8, 2024)

Liisa Thomas

Sam Cournoyer

Kathryn Smith

January is New Year's resolution time. It's also the time when we exercise our predictive skills.

What trends from last year will repeat in the coming months? What steps can we take to be best prepared? How, in other words, can we heed Churchill's warning and learn from history?

As we start our year and put our best collective feet forward, here are eight data privacy developments from 2023 to keep in mind for 2024. Some — children's privacy, dark patterns and international data flows — are not new to the prediction list.

Others — focus on data brokers, health privacy, telematics and artificial intelligence — are new.

But whether new or not, keeping these 2023 developments in mind can help as companies plan their 2024 privacy programs.

Focus on Brokering Data

Over the past several years, U.S. state privacy laws brought to the forefront of general companies' minds concerns about the selling of personal information.

How? By defining a sale as not just the exchange of personal information for money, but also under some state's laws — like California — for the exchange of other valuable consideration. This definition meant that companies were examining with much greater care how they shared information with third parties.

While this may have become a common part of privacy practitioners' diligence, what hasn't necessarily been on the forefront is the concept of data brokering. In particular, with laws specific to data brokers. While definitions vary, data brokers are generally those in the business of selling data collected by others.

California and Vermont had been the only two states to regulate these companies. They were joined in 2023 by Oregon and Texas. And last year, California updated its law.

Data broker laws typically require that brokers register and implement data protection measures. California, though, modified its approach to data brokers to expand brokers' obligations. These include giving consumers the ability to have their information deleted — effective Jan. 1, 2026.

In addition to legislation for broker activity, 2023 also saw regulatory scrutiny.

The Federal Trade Commission, for example, filed suit against Kochava in July 2023. The agency was concerned about the data broker's creation and sale of profiles that contained sensitive information. These concerns were not new: The FTC issued a report 10 years ago

about its concerns with the broker industry.[1]

As we look ahead, it seems likely that other states may draft legislation governing data brokers. Or, that regulators may take action against those selling personal information.

The focus may be multifold. Including, the extent to which the sale of the information causes harm to individuals, whether the information is being sufficiently protected and the control people can exercise over the use made by brokers of their information.

FTC Will Fight to Retain Its Privacy Authority, Continue Its Actions

For more than two decades, the FTC has been the leading federal enforcer of data privacy. It has primarily relied on its authority under the FTC Act, taking action against those engaging in unfair or deceptive acts.

It does, however, have enforcement power under other privacy laws. These include the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act, where the agency engaged in rulemaking action in 2023.

On the deception and unfairness front, the FTC has a fairly long track record of settling with companies, with some exceptions. That trend may be changing.

Kochava, mentioned above, challenged the FTC's initial complaint. Others have done so as well, and the agency has been questioned about what has been viewed as its sweeping approaches to its privacy and data security enforcement.

Of concern for many is that Section V of the FTC Act does not describe what constitutes a deceptive or unfair practice. Companies must thus look to FTC guidance or prior cases to understand what the agency may view as violating the act. This can cause confusion and make predicting the agency's perspective difficult.

Notwithstanding these concerns, the FTC continued in 2023 to take action against those it viewed as violating consumers' privacy or failing to provide adequate security.

For example, a settlement with Global Tel Link following a 2020 data breach, where the company put live data in a test environment without —according to the FTC — sufficient security measures in place.

While the FTC may not be the only regulator in the privacy game these days, it will likely continue to be a considerable force in 2024 and beyond.

Expect to see not only rulemaking and enforcement activity under privacy-specific laws like HIPAA, the GLBA and COPPA, but also under Section V of the FTC Act.

Children's Privacy Will Remain at the Forefront

Early child internet users who were affected by COPPA are now in their thirties.

Some of them are partners in law firms, associate general counsels of large companies, and business owners and leaders. The law was enacted at the beginning of the internet era and is showing its age.
The original hope by the law's drafters was to get parents involved in their children's online

activities. It requires verifiable parental consent before children can submit information online to companies. In practice, however, the law has been stymied by two key practical hurdles.

First, truly verifying parental consent is almost impossible, and second, the mechanism for identifying age — asking the user — is easy to circumvent. Now-adults who were children in 1996 may tell their own children to simply input an age of 13 or older.

Given these hurdles, we have seen two trends in 2023 at a state level. First, states have entered the protection fray. Some have passed laws specifically aimed at protecting children. These include California, Ohio, Texas and Utah.

The primary focus is on social media, and increases the age of concern from under 13 to 16 in Ohio, or 18 in Texas and Utah. California's is the broadest, applying not just to social media sites, but to all who create services or features likely to be accessed by those under 18. It has been stayed — it would have gone into effect in July.

If it does go into effect, it will do things like prohibit profiling children and using information in a way that harms them. The Ohio, Texas and Utah laws, on the other hand, require parental consent before minors can create social media accounts and give parents control over minors' accounts.

These laws may be subject to the same procedural flaws as COPPA. Nevertheless, several other states — including Connecticut, Maryland, Minnesota and Oregon — have introduced similar legislation. Ohio's law goes into effect Jan.15, Utah in March and Texas in September.

Second, many states' comprehensive privacy laws have included provisions that are aimed at children. For example, children's information cannot be shared — in California, for children under the age of 13 — or processed without obtaining parental consent, like in Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Virginia and Utah.

In the U.S., beyond states, we are also seeing activity at the federal level. This includes the FTC's proposal to revamp and modernize COPPA, in rulemaking issued at the end of 2023.

The Children's Advertising Review Unit, the self-regulatory body that monitors companies who advertise to — and interact with — children, also released new guidelines to address interactions with children in the metaverse.

While we may not see increased regulation of children's privacy, we are likely to see both continued regulation as well as changing regulations. And who knows, perhaps some of the now-adults who were children in 1996 will fix the practical problems contained within COPPA and similar laws.

Dark Pattern Enforcement

So-called dark patterns have been a concern for regulators for the past two years.

Most activity has centered on rulemaking. While 2023 did not see significant new rulemaking developments, some enforcements in this area did begin. It is possible that 2024 may see a shift from rulemaking to enforcement.
Among other cases, the FTC brought action against Publishers Clearing House for allegedly

using dark patterns to get consumers to enter its sweepstakes. It brought similar allegations against Credit Karma LLC for using dark patterns to misrepresent to consumers that they were preapproved for credit cards.

Whether using deceptive trade practice allegations or laws that specifically mention dark patterns — like those under many new state laws — we are likely to see more privacy enforcement actions that specifically allege dark patterns.

Companies can keep in mind mechanisms the FTC, Europe's European Data Protection Board and other regulators have mentioned in the past to avoid engaging in a dark pattern. This includes assessing your features from consumers' perspective.

International Flows of Data

It seems that we cannot escape concerns by non-U.S. governments — and Max Schrems' nonprofit None of Your Business — over the flow of information into the U.S.

In 2023, we saw the approval by the EU of the replacement to the Privacy Shield, namely the Data Privacy Framework. The DPF approval came about in no small part because of a White House executive order that established guidelines for when U.S. surveillance agencies could use non-U.S. nationals' personal information.

In issuing the approval, the EU indicated that the safeguards applied not only to transfers based on the DPF, but also transfers based on other mechanisms — like standard contractual clauses. Schrems and others have indicated that they may contest the DPF, something we may see in 2024.

As a result, and because the EU noted that the safeguards implemented under the White House executive order apply to other means of transfer, we do not expect to see as many companies sign up for the DPF as we saw under prior mechanisms, namely Safe Harbor and Privacy Shield.

Protection of Health Privacy

There have been some significant developments in 2023 around health privacy. These developments exist both at the federal and state level.

At a federal level, the FTC proposed amendments to its Health Breach Notification Rule. The rule applies to vendors of personal health records and related entities, as opposed to HIPAA-covered entities — i.e., those who provide healthcare services — or their business associates.

The FTC's goal in amending the rule, which will likely occur during 2024, is to clarify when notices to individuals are required, expand what content to include in notices, and to clarify that the rule applies to health apps. The FTC also took enforcement actions in the health space in 2023, something it will likely do in 2024 as well.

Another federal development in 2023 was when a letter from the U.S. Department of Health and Human Services' Office for Civil Rights and the FTC was sent in July to more than a hundred hospitals and telehealth providers about their use of online tracking tools. The letter followed a December 2022 guidance from OCR about the applicability of HIPAA to these tools.

In that guidance, the OCR outlined its position that if a HIPAA-covered entity collected protected health information using the tools and shared the information with third parties, HIPAA and its requirements would apply. Several lawsuits have been filed following both the guidance and the letter, and we expect to see increased scrutiny of healthcare service providers in 2024.

At the state level, Washington passed its My Health My Data Act in April 2023.

The act will apply — with some exceptions — to companies that conduct business in the state, and that collect, process or share consumer health data. That term is broadly defined as any personal information that is linked or reasonably linkable to a consumer and identifies their physical or mental health status. It will go into effect in March, and in July for small businesses.

Under the law, companies will need to get affirmative consent to collect or share health information for reasons other than to provide the product or service requested. The law also requires more stringent authorization for sale of information. Under the law, companies will also need to give consumers rights, like access and deletion.

2024 will likely see ongoing litigation around the collection, use and sharing of personal information by companies in the healthcare space, as well as potential state legislative activity along the lines of that from Washington in 2023.

Scrutiny Of Telematics Usage

Legislators were concerned with adware and spyware in the 1990s, email messages in the early 2000s, cookies in the 2010s and biometrics in the early 2020s.

Whatever the technology, the focus of these laws has been the extent of personal information is being gathered, if individuals are aware of that gathering, and if they can control companies' collection or use of their information.

As we look forward to 2024, one technology that will likely be on the forefront is telematics: in particular the passive collection of information in — and by — vehicles. Information gathered might include information about the driver. For example, precise geolocation or driving habits.

It might also include information about individuals near the vehicle, especially as we see an increase in driverless technology. Information collected by cars is an area that may be of concern for regulators as it combines both passive information gathering and in-person gathering, something not seen in the examples listed above.

We saw some enforcement movement on this front in 2023. The California data protection authority, the California Privacy Protection Agency, announced they were opening an investigation into information collection by connected vehicles.[2] We may see more enforcement activity in 2024 and potential legislative action.

Outside of the U.S., issues around connected vehicles were included in the final draft of the EU's Data Act[3] — which will go into effect in mid-2025. Chinese regulators have also expressed concerns about these activities.

As we move into 2024, companies that market connected cars — or create tools or systems that connect to those cars — will want to keep potential regulatory concerns in mind. This

includes thinking about the extent to which personal information is either actively gathered about the driver or those around the vehicle. Or if information — including sensitive information — can be inferred.

How will that information be used? Will it be included in profiles created about the individual? What options will people be given? How will those options be operationalized?

Regulators may be thinking about this in the year ahead, and companies may want too as well.

Artificial Intelligence

No set of predictions can be complete without a discussion of AI.

But, given how much this technology — and our use of it — has changed and likely will change, what did we learn from 2023 that can inform us in 2024? We can start with a short recap of AI-related activity in 2023.

In June 2023, Connecticut enacted an AI law directed at state agencies. In July 2023, New York's AI employment law went into effect. The law requires that employers who use AI for hiring decisions regularly audit their processes for bias and discriminatory outcomes.

In August 2023, the FTC launched an investigation into ChatGPT to understand how OpenAI is using personal information and if its privacy representations are sufficient. Then in November 2023, the White House released a sweeping executive order on AI.

While the order is directed to government agencies, businesses will experience impacts as well. The executive order details requirements around data security and protecting consumers from harm.

Companies also should keep in mind that of the five state privacy laws that took effect this year — California, Connecticut, Colorado, Utah and Virginia — all but Utah contain provisions that could affect use of artificial intelligence. Namely, the obligation to conduct risk assessments if using automated decision making that could lead to legal or similarly significant outcomes.

Colorado has rules that give details about when and how to conduct these assessments. And at the end of the year, California released draft rulemaking.[4]

As we look forward to 2024, we can expect that artificial intelligence will be on the forefront. Companies using these tools may right now be focused on protecting assets created by the tools.

But regulators in the privacy space are more focused on the potential harm that might arise to a consumer. Either because their personal information has been misused, or because the tool causes them harm.

Conclusion

As these trends illustrate, there will be a vast array of privacy concerns not only on regulators' minds in 2024, but also being enforced in the courts.

This can be overwhelming as companies prepare and maintain their privacy programs. But,

it doesn't have to be. There are ways to make the approach manageable.

Obviously, keeping in mind regulatory concerns and developments are important. But also important is understanding where your organization has the most risk.

Do you have large amounts of consumer information? Do you collect sensitive information? Are you providing services to third parties that have cybersecurity implications? These are some of the many questions to ask.

Once you know both the laws and the risks, you can think through the right approach to mitigate those risks. As you do so, remember that not all risks are the same. Some are predictable, and can be mediated by policies or procedures.

Some, though, are unpredictable, and require different tools, like a focus on teamwork. Combining legal knowledge, risk assessment and appropriate mitigation tools can make companies' privacy programs more manageable.

Liisa M. Thomas is a partner and co-leader of the privacy and cybersecurity practice at Sheppard Mullin Richter & Hampton LLP.

Sam Cournoyer is a law clerk at the firm.

Kathryn Smith is a fellow at the firm.

[1] Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014) (ftc.gov).

[2] CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies (ca.gov).

[3] https://data.consilium.europa.eu/doc/document/PE-49-2023-INIT/en/pdf.

[4] https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf.