5 Data Privacy Law Trends That Will Continue Into 2023

By **Liisa Thomas** (January 2, 2023)

Liisa Thomas

The start of the new year is typically when we look to the future — and to the past. The current economic uncertainty can make it even harder for companies to develop their 2023 privacy and data security compliance priorities.

There are several trends from 2022 that will help privacy teams prepare for the year to come.

The following five developments from 2022 seem likely to be with us into the new year. Looking back at these should help with planning for next year.

Regulator Action on Data Breaches and Data Security

A diverse group of regulators issued reports and decisions in 2022 affecting how companies manage data breaches and security measures. This regulator focus has been a constant for the past several years, and will no doubt continue in 2023.

Keeping track of these recommendations and decisions will be important to managing risk in 2023.

Enforcement authorities, like the rest of us, notice the types of incidents that are in the news. And in 2022, that included both ransomware and credential stuffing attacks. The latter being attacks where threat actors flood a website with previously stolen login credentials.

The U.K. Information Commissioner's Office and the U.S. Securities and Exchange Commission have both cautioned companies about making requested payments.

And, for some time, going back to July 2021, the New York Department of Financial Services has focused on measures companies should be taking to prepare in the event of a ransomware attack.

The NYDFS also issued a detailed report on handling credential stuffing. Recommendations included measures to detect potential attacks.

The goal for these recommendations is to protect consumers — and companies' systems.

Regulatory enforcement in 2022 followed the same theme. For example, the New York Attorney General settled with online retailer Zoetop Business Co. Ltd. for $1.9 million, arguing that the company's security measures were insufficient and outlining what it would have expected the company to have done.

The NYDFS reached a $4.5 million settlement with an insurer, EyeMed Vision Care LLC, who suffered a phishing attach. The Federal Trade Commission reached a settlement with Drizly LLC, the online alcohol retailer, and its CEO James Cory Rellas, over similar security concerns.

Both the FTC and the NYDFS outlined in these settlements the measures they thought the companies should have had in place. These recommendations can serve as signals to others about how to avoid potential similar investigations over their security measures.

But the focus has not rested only on steps a company should have taken before an incident. In May, the FTC looked at when and how a company should issue breach notices to impacted individuals after an incident.

In some cases, it advised, merely following breach notice law requirements may not be enough. Instead, companies should keep in mind unfairness and deception principles, enforced under Section 5 of the FTC Act and similar state laws.

In particular, notification may be needed to avoid harm to impacted individuals. Banking regulators, for their part, also looked at breach notice process. They sped up the time to notify regulators of an incident that causes a material disruption to 36 hours.

In sum, as has been the case in past years, data security measures will continue to be a significant focus in 2023, and beyond.

Continued Focus on Dark Patterns

Dark patterns were a 2022 concern in the U.S. and Europe and will continue into 2023.

In Europe, the term describes situations where consumers are misled into providing more information about themselves than they would have done otherwise. Or, in unwittingly giving consent to information uses that they would not have done otherwise.

In the U.S., while these activities are also a concern, the term also describes tricking consumers into making purchases. Guidance about how to avoid a dark pattern was issued in both the U.S. and Europe in 2022.

It is quite likely that both U.S. and EU regulators will bring actions for companies that it believes have engaged in dark patterns, so the recommendations should be used help inform privacy practices for 2023.

In the U.S., the FTC issued a staff report with strongly worded instructions about how to avoid dark patterns. The report also reminded companies that the FTC will enforce these activities under the FTC Act, and has done so in the past.

Recommendations included not setting system defaults to collect too much consumer information. The report also urged companies to make consumers choices over personal information uses easy to manage and understand.

Here, the FTC specifically recommended against ambiguous toggle buttons. The FTC also cautioned companies that they should review user interfaces from a consumer perspective: User interfaces that manipulate choice can be considered dark patterns.

Elsewhere in the U.S., dark patterns were also a focus. In California, the upcoming California Age-Appropriate Design Code Act specifically prohibits using dark patterns with children, and the California Privacy Rights Act also speaks to dark patterns.

Finally, industry-specific regulators in the U.S. are concerned about dark patterns. The Consumer Financial Protection Bureau, for example, sued online payment company

Active Network LLC for enrolling unwitting users into annual subscriptions.

In Europe, the European Data Protection Board, or EDPB, provided detailed recommendations about how companies can avoid dark patterns. Of concern were dark patterns like giving consumers too many choices, or overloading, and setting up the interface so a consumer forgets about privacy, or skipping.

Also concerning was hiding information or privacy controls, or having a user interface that was inconsistent or unclear. In 2024, the European Digital Services Act will also specifically prohibit dark patterns, something companies will want to prepare for during 2023.

And until then, as the EDPB cautions, the General Data Protection Regulation prohibits dark patterns insofar as it prohibits misleading processing of information under Article 5(1)(a), requires transparency by design under Article 25, that companies explain rights to users clearly under Article 12(1), and that consent be freely given and informed under Article 4(11).

Ongoing Worry Over U.S. State General Privacy Laws

Five states in the U.S. either updated — California — or put in place general privacy laws in 2022. All become effective at some point during 2023.

Two — the CPRA, which updates the existing California Consumer Privacy Act, and Virginia's Consumer Data Protection Act — became effective Jan. 1. Two more are effective July 1: the general privacy laws in Connecticut and Colorado.

Finally, Utah's law closes out the year, with an effective date of Dec. 31.

While companies have spent much effort during 2022 preparing for these laws, more work is expected in the early part of 2023, including finishing out any uncompleted tasks for California, as additional California regulations are expected next year.

Companies will also focus on preparing for Connecticut's and Colorado's laws, keeping in mind the draft Colorado regulations and the hearing about them scheduled for Feb. 1.

In many respects these state laws mimic the well-known European GDPR. They provide individuals with rights over their information — to access, correct, delete and the like.

They also contain provisions about managing, and contracting with, vendors. They also require companies to incorporate certain disclosures in their privacy policies — or in the case of California, to organize their privacy policies in certain ways.

Most do not affect employee information, with California as an outlier.

Perhaps one of the murkiest areas of these laws is their approach to digital targeting and mechanisms companies need to have in place on their websites to allow consumers the ability to control those activities.

There will likely be enforcement in this area, continuing scrutiny that California has given to-date under its existing general privacy law.

Scrutiny Over Interactions With Children

2022 saw several developments that influence companies' ability to interact with children. And those developments will reverberate into the new year and beyond.

First, California passed the Age-Appropriate Design Code Act that will go into effect July 1, 2024. The law mirrors a similarly named U.K. law and will require much work by U.S. companies who have not had to deal with the British counterpart yet.

The law has broad applicability — to businesses whose websites are likely to be accessed by children under 18. Unlike the federal Children's Online Privacy Protection Act, which has a 13 and under range and also carries a knowledge qualifier, although knowledge can be imputed.

The law will impose many restrictions on these sites, including having privacy settings default to the highest level of protection and conducting an impact assessment before releasing new online features. It should be noted that the law is being challenged, but the outcome of that fight is far from certain.

Regulators were not the only ones that focused on children's privacy issues in 2022. The Children's Advertising Review Unit, or CARU, the self-regulatory body that enforces advertising standards, had an active year in the privacy space.

It issued notable decisions against mixed audience sites and apps — in other words, ones that appeal to adults and children. In one case, CARU believed that the SpongeBob: Krusty Cook-Off app was appealing to both children and adults, and as such, needed to get parental consent before collecting information from children under 13.

CARU's actions also made clear that its work is not limited to websites.

For example, it investigated the maker of the kids' smartwatch TickTalk 4. As a result, the company, TickTalk Tech LLC, agreed to modify its notice and consent process around the geolocation functionality.

CARU has a long history of focusing on children's privacy, and companies will want to keep its actions in mind in 2023.

No End in Sight for Transborder Data Flow Confusion

Many regions have restrictions in place for sending personal information out of the country. These restrictions exist in the EU, which provides for some options when sending information out of the region.

Between the EU and the U.S., one option used to be the EU-U.S. Privacy Shield. Most are aware that this was declared an invalid mechanism by the EU in 2020.

A replacement has been in the works for some time. In the interim, companies have been making do with the EU's standard contractual clauses as well as heightened measures to assure sufficient security.

Those clauses were revamped in 2021, and the deadline to transition to new clauses will have passed by January. While companies should thus have made the transition prior to 2023, many may still be doing last-minute modifications at the start of the new year.

In the U.K., similar — but not identical — clauses exist and are being phased over to a new set, with a March deadline. There will thus likely be new documents to keep track of from the U.K. during 2023 as we approach that March deadline.

The U.S. has been working to develop a program to replace Privacy Shield to help companies more easily receive EU data. In October that new program was introduced, and as of this writing, was being reviewed by the EU.

Some anticipate that it will be finalized by March, although pushback is expected. To the extent the program is passed in 2023, many companies may deliberate whether to participate.

These might include current Privacy Shield participants as well as those who did not participate in that older program.

With new clauses and a potential new transfer program, the ability to send information from the EU to the U.S. will continue to be a challenge for multinational companies in 2023.

What's Next?

These five developments from 2022 can help inform companies as they develop their 2023 priorities.

From dark patterns to ransomware, interacting with children to providing rights under new general privacy laws — enforcement authorities are not likely to stop their scrutiny of companies' privacy and security practices.

This scrutiny will likely be recession agnostic, and thus as we prioritize for the coming year, these concerns should be kept in mind.

Liisa M. Thomas is a partner at Sheppard Mullin Richter & Hampton LLP.