CLIENT ALERTS & INSIGHTS

Privacy Points 2024: Recap and What to Watch For in 2024

JANUARY 17, 2024

Authors: Ryan T. Sulkin

Last year proved to be a big year in data protection with U.S. state data protection laws popping up across the country, the FTC updating its guidance and regulations on everything from data breaches and biometric information. 2024 could prove to be even more consequential.

As we close the book on 2023 and look to 2024, data protection law remains as active as ever. 2023 saw eight new states pass omnibus data protection laws; five states had updates to existing data protection laws or new data protection laws come into effect; the Federal Trade Commission updated regulations for financial institutions regarding data breach notifications and provide guidance on the collection and use of biometric information; exponential growth of BIPA litigation in Illinois, states increase the legal protections for children using online platforms and social media; and so much more.

And the above list only scratches the surface. This new year could see even more activity in data protection law.

Below are some highlights of key issues and topics to watch as we progress into 2024.

New US State Data Protection Laws

As the clock hit midnight a few weeks ago (and as of the date of this article being published, five states have broad, omnibus data protection laws in effect regulating the collection and use of personal data: (1) California, (2) Colorado; (3) Connecticut; (4) Virgnia; and (5) Utah. In total, there are thirteen states with omnibus data protection laws on the books, with the other eight going into effect this year and in the years to come.

Specifically in 2024, we have five new states to welcome to the party:

2024:

- Florida**:** July 1, 2024
- Montana**:** October 1, 2024
- Oregon**:** July 1, 2024
- Tennessee**:** July 1, 2024
- Texas**:** July 1, 2024

Delaware and Iowa have data protection laws coming into effect in 2025, and Indiana rounds out the bakers dozen with its data protection law coming into effect in 2026.

And 2024-not even a full three weeks into the new year-has already seen a new state join the ever growing list. New Jersey's legislature passed an omnibus data protection law on the last day of its state legislative session. If signed, New Jersey will become the 14th state with a broad, omnibus data protection law on the books. Last year saw a number of large, typically conservative leaning states enter the fray. Could 2025 be the year that large, liberal leaning states such as Illinois or New York join the list?

As state legislative years begin, it will be something to keep an eye out.

By the end of the year, it will be hard to come across a business operating in the U.S. that is not impacted or that does not need to comply with one or multiple U.S. data protection laws.

The privacy policy and notice requirements are often what businesses first think of, and first build out compliance for, with regard to U.S. state data protection laws. However, the privacy policies and notices are but the first step towards compliance.

In order to be fully compliant with U.S. state data protection laws, businesses will need to dive deeper into the layered, complicated, and sometimes contradictory depths of this burgeoning body of law. Compliance programs will need to span, yes, those privacy policies and notices, but also to procurement and sales teams to handle vendor management, internal customer relation teams to handle data privacy right requests, web developer teams in order to build out Global Privacy Control compliance, and all departments and teams of a business to understand how data is being collected and used.

See our past coverage of some of the less talked about requirements here. Additionally, see Benesch's and Data Meets World's new, interactive U.S. State Privacy Laws website page for a high level overview of (1) what U.S. states have data protection laws on the books; and (2) of what such data protection laws cover and will require.

Ad Tech & Universal Online Opt-Out Mechanisms

One of the new fronts of data privacy that the U.S. state data protection laws are mostly all addressing are the use of cookies, online trackers, and online advertising. The vast majority of the U.S. state data protection laws give users a right to opt out of cross contextual behavioral advertising. But many of the laws go further.

States such as California, Colorado, Connecticut, Delaware, Montana, Oregon and Texas require that-for businesses that engage in any sale of personal information or that use the personal data for targeted advertising-businesses to ensure their websites are configured to adhere to what are called "universal opt-out signals". The vast majority of those states kick any specifics on universal opt-outs to forthcoming regulations.

But at the dawn of 2024, Colorado was first to the line to provide that regulation. Under Colorado's data protection law, any in-scope business will need to ensure their website is configured to listen to and adhere to what is called the Global Privacy Control. The Global Privacy Control allows a user to download a browser plug-in that broadcasts to websites that the user does not wish to have its

personal information sold or used for targeted advertising. The signals allow the user greater control over their privacy rights and options, and a more seamless route for exercising those rights.

As the year progresses, expect further clarity and potentially a growing list of universal opt-out signals that businesses will need to keep track of.

An additional story to watch on this front is out of California, where the newly minted California Privacy Protection Agency advanced regulation that would require browser vendors themselves to include universal opt-out signal options for users to utilize. It would be the first such requirement at the browser level instead of the website-by-website level.

Both of the opt-out signals at the browser-level and the website-level will greatly impact the use of common analytics and advertising tools that commonly make use of cookies tracking personal information and online activities of users.

Children Online Privacy Protections

The last year saw a number of U.S. states advance and pass new laws intended to better protect children online activity.

Utah was the first state to pass a bill requiring social media platforms to obtain parental consent before allowing users under the age of 18 to create an account. Not only does the Utah's law require express consent from parents for users under the age of 18, but it also requires social media companies to (1) verify the age of existing and new Utah account holders; and (2) verify that existing Utah account holders have provided the requisite consent if they are under the age of 18. This is just a sample of the far reaching aspects of such laws that have spread beyond Utah-court cases putting such laws on hold notwithstanding.

Other states such as Arkansas and Louisiana have followed Utah's lead on this issue, which-if laws are not held up in court-would drastically increase the obligations social media platforms take on when engaging one of their largest constituencies.

California has also started a trend with its Age-Appropriate Design Code Act aimed at requiring companies with websites aimed at children to design the website with privacy and data protection in mind. The bill-while only focused on those users under the age of 18-tracks closely with the E.U.'s principle of privacy by design and default. Courts have also held this law up in court and whether or not this version of the law goes into effect this year remains to be seen.

Perhaps most importantly-in its broad, far reaching effects-the Federal Trade Commission has proposed changes to its Children's Online Privacy Protection Act regulations.

In its notice of proposed rulemaking, the FTC proposed (among other things):

1. specifications on existing COPPA regulations (such as adding examples and factors to help determine which websites are "directed to children");
2. adding biometric data to the definition of personal information;
3. **separate**

verifiable parental consent requirements before a business is allowed to disclose personal information to third parties (mainly directed at limiting the use of children's personal information for targeted advertising purposes);

4. further notice requirements by requiring disclosures of what personal information is shared with third parties, what categories of third parties receive such personal information, and data retention policies for children's personal information; and
5. the introduction of standard data security requirements (e.g., a written, comprehensive security program, annual risk assessments and regular monitoring practices, etc.).

As the FTC progresses down the rulemaking process, businesses that are in any way directed towards children or otherwise collect children's personal information will need to keep note with additional obligations that are finalized in 2024.

Biometric Information

Since the advent of Illinois' Biometric Information Privacy Act ("BIPA"), litigation regarding the collection and use of biometric information has been exponentially growing.

The Illinois Supreme Court handed down decisions that are sure to have lasting impacts well beyond 2023, including a ruling that found claims accrue ***each time*** a business improperly collected an individual's biometric information. The ruling was seen as a boon for plaintiffs' attorneys, broadening the potential damages plaintiffs could claim.

Then, in November of last year, the Illinois Supreme Court again broadened an aspect of BIPA, but this time, in defendants favor. Under BIPA, there is an exemption to the definition of "biometric identifiers" that states: "*Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996*." The court ruled that this exemption goes beyond only applying to a patient's information, but also applies to a healthcare provider's employees' information as well.

The ruling on the healthcare exemption under BIPA was fact specific, so expect litigation under BIPA to continue to increase as plaintiffs' attorneys continue to find the boundaries of the law, its exemptions and the amount of damages available to claim.

However, businesses will also need to keep their eye on the federal government with regard to biometric information. in Mid-2023, the FTC released a new policy statement that cleared up the FTC's definition of what constitutes biometric information and what the FTC expects from businesses collecting and using biometric information so as to not fall into the "unfair" or "deceptive" business practices buckets. The FTC policy statement now puts forth examples of how businesses should be analyzing such practices. For example, businesses should incorporate discussions and reviews of any foreseeable harms that could come from the misuse of the in-scope biometric information and conduct on going due diligence of any current or new biometric information service providers.

Businesses that collect and use biometric information also need to ensure they have clear public-facing (e.g., to employees or consumers depending on those identified by the technologies)

notices that are accurate to the biometric information practices and that clearly set forth how that information is used.

Data Breach Notifications

Data breach notification requirements (whether at the general U.S. state level, specific to financial institutions, or otherwise) make up the oldest, non-Constitutional foundation of data protection law in the U.S. However, 2023 saw new structural requirements built into that foundation.

Over the summer, the Securities and Exchange Commission formally adopted a rule that required any public company to make a formal-publicly available-disclosure to the SEC notifying the agency as well as the public of any cybersecurity incident. The rule also adds an annual reporting requirement on public companies to disclose material information regarding their cybersecurity risk management, strategy, and governance.

Under the new rule, public companies will generally have only four hours to make the formal disclosure to the SEC once the business determines that the cybersecurity incident is material.

As the rule has come into effect, many have worried that the disclosures could actually be leveraged by bad actors and hackers. As 2024 marches on, it will be important to look to the SEC to see if clarifications and guidance help ease the growing pains.

Also at the federal level, the FTC recently adopted new Safeguards Rule updates under the Gramm-Lech-Bliley Act. The 2023 amendment to the Safeguards Rule consists of the new requirement that financial institutions report notification events to the FTC through an online reporting form to be made available on FTC.gov. The form is not yet available. The amendment to the Safeguards Rule will take effect 180 days after publication of the amended Safeguards Rule in the Federal Register.

The new year will see these new data breach reporting mechanisms come into effect and will undoubtedly see an increase in data breach notification and reporting requirements increase as cybersecurity remains a regulatory and legislative focus.

AI Regulation

Artificial intelligence and regulation thereof was among not just the hottest topics in the data protection legal world, but across the legal world generally.

The E.U. lead the way passing its landmark Artificial Intelligence Act that was the first comprehensive regulatory scheme in any major jurisdiction specifically addressing-albeit at a high level-the development and use of artificial intelligence. The E.U. Artificial Intelligence Act is focused on a risk-based approach, placing more far reaching and prescriptive requirements on what it deems to be more sensitive or high risk uses of artificial intelligence.

China quickly followed suit in the summer of 2023 passing its first round of artificial intelligence regulations that will require artificial intelligence providers to register with and obtain a license from government agencies. It will also require regular security assessments for all in-scope artificial intelligence providers and additional registration requirements for the algorithms driving certain subsets of artificial intelligence tools (such as those that can influence public opinion).

In the U.S., there has also been a focus on artificial intelligence; however, there has been no substantive regulation or legislation on the matter. In late 2023, President Biden issued an executive order directing federal agencies to focus on artificial intelligence regulation.

However, 2024 will undoubtedly see more specific artificial intelligence regulation and legislation, and perhaps the US will affirmatively jump in to the fray.

Changes Across the Pond…and Beyond

There are also a number of changes across the globe that will shape data protection law in 2024 and beyond. The below list highlights some of those additional topics to keep an eye on:

1. India passed its first comprehensive data protection law, largely following in the footsteps of the E.U.'s GDPR and common data protection principles (e.g., comprehensive transparency requirements, data privacy rights, internal audit and security requirements, and data minimization). No official effective date has been announced, so global businesses will need to keep note.
2. The United Kingdom is in the final stages of finalizing amendments to its data protection law (modeled after the E.U.'s GDPR pre-Brexit). The amendments are aimed at making the UK a more "business-friendly" data protection jurisdiction, moving away from the E.U.'s GDPR, which is often seen as the strictest jurisdiction.
3. The U.S. - E.U. Data Privacy Framework-aimed at making cross-border data transfers easier to lawfully accomplish-will continue having come into effect in mid-2023. The framework is already facing similar legal questions that doomed its predecessor (Privacy Sheild).

Conclusion

The breakneck speed at which data protection laws are being passed, coming into effect, and changing can be difficult for businesses to keep track of as one business can often find itself navigating compliance with multiple, and substantively different, data protection legal regimes.

2024 will likely prove to continue the trend of an exponentially growing body of data protection law as use of and reliance on technology, data, and artificial intelligence grows. Make sure to check back throughout the year for specific updates on all data protection topics.

As data protection law updates continue to roll in throughout the new year and new data protection legal requirements take shape, the Benesch Data Protection team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.