CLIENT ALERTS & INSIGHTS

Privacy Floodgates Open: 13 U.S. State Data Protection Bring About Major Changes

NOVEMBER 16, 2023

Authors: Matthew Farrell

Global Privacy Controls, vendor management, sensitive personal information, and the use of Ad Tech; new U.S. state data protection laws introduce twists to traditional notions of American data protection law.

In the U.S., data protection and privacy law have expanded exponentially over the last 20+ years. Starting from humble roots, only regulating the collection and use of the personal data in specific industries such as healthcare and financial services, growing into a robust-albeit layered and contradictory at times-body of law.

A big reason for that is the advent of omnibus data protection laws regulating the collection and use of ***any*** personal information in several U.S. states. The number of states with such data protection laws in place has only grown in the last year. There are now 13.

U.S. data protection law was built on a foundation of "notice and choice". Businesses publish privacy policies and notices describing, at a high level, their data collection and use practices, and the informed consumer decides whether to continue interacting with that business. While the laws all build, and still largely rely, on the traditional privacy law foundation of "notice and choice," they've also added specific scenarios where affirmative actions must be taken to proactively protect consumers or to enhance the choices and decision-making power those consumers have.

With over a dozen states adding their own spin to this body of law, it can be hard to keep up.

To aid in the constant effort of keeping track of new U.S. state data protection laws, Benesch Friedlander Coplan and Aronoff and the Data Meets World blog now feature a "U.S. State Law" landing page that offers a high level overview of all U.S. states with data protection laws in place and key requirements and takeaways from those laws. The new webpage offers a continuously up to date snapshot of the U.S. state data protection landscape. For a review of our most recent article highlighting an overview of the U.S. states with data protection laws in place and their applicability, click here. To use the Data Meets World interactive U.S. Privacy Law webpage, click here.

While some of the high level requirements of the new U.S. state laws have taken a hold across industries and businesses-such as privacy policy and notice updates-other requirements that go beyond the traditional "notice and choice" foundation of U.S. data protection law are often overlooked.

Global Privacy Controls and Ad Tech

Two related concepts have emerged in U.S. state data protection laws in the realm of what data privacy rights they offer consumers: the rights to opt-out of the sale of their personal information and to opt-out of cross-contextual behavioral advertising.

Under most of the U.S. state data protection laws, "sale" can cover more than just the exchange of data for monetary value, covering the exchange of data access for anything of value, such as services. In 2022, the first enforcement action under California's data protection law exemplified this by labeling the unrestricted use of Google Ads and other ad tech as a "sale." Cross-contextual behavioral advertising can be understood to be the displaying of advertisements that are selected based on personal data collected from ***across*** the Internet over a period of time-what is generally understood to be targeted ads. Additionally, even if a business is only engaging a third-party ad tech provider for advertising that is based purely off of information collected from a business's own website and the consumer's direct interactions with the business, if the third-party is able to independently use the information to build out profiles or to provide advertising services to their other customers, it could still fall into the "sell" category, necessitating opt-out rights.

In furthering consumers' opt-out rights, some states-such as California, Colorado, and Connecticut-require that businesses enable their website to listen for and respond to what are called "Global Privacy Controls" that automatically broadcast out a consumer's preferences with regard to the sale of their personal information or use of their personal information for targeted advertising purposes.

The states have, thus far, failed to provide specifics on exactly what signals need to be adhered to and further regulation and clarity on this matter is forthcoming. However, GitHub has curated the following website to pull together standard Global Privacy Controls, best practices, and implementation notes: https://globalprivacycontrol.org/. Businesses subject to U.S. state data protection laws would be wise to build out their websites to adhere to Global Privacy Controls in accordance with industry standards and best practices-even absent specific regulations on the matter-with compliance deadlines fast approaching.

Cookies and Consent

Unlike European data protection law, U.S. state data protection laws still-by and large-do not require opt-in, prior consent for cookies via those pop-ups and banners we have all become accustomed to (however, there are still some scenarios under U.S. law that require opt-in consent, such as with regards to the collection of sensitive data under FTC guidance, cookies that collect PHI regulated by HIPAA, and video-viewing information subject to the VPPA).

However, cookies and cookie policies have become common for U.S. businesses in light of the "sale" and "cross-contextual behavioral advertising" requirements, and the related opt-out rights set forth in U.S. state data protection laws. Targeted advertising and the use of ad tech typically requires the use of cookies, pixels, and other online tracking technologies. It is important to note here that the information collected by cookies and such trackers are often considered personal information under U.S. state data protection laws and the definition includes information that may be reasonably linked or linkable to an individual. Because cookies are related to an individual's online behavior and activity (even in an aggregated state), cookies may be considered personal information if they are able to be reasonably linked or linkable to an individual.

Working with marketing teams and website service providers is key to understanding what will be necessary for businesses in complying with the selling and cross-contextual behavioral advertising opt-out rights (this is especially true as plaintiffs' firms, latching onto the current focus on consumer privacy, continue to bring civil suits under a multitude of laws, often using the state-provided rights as a backstop for their claims).

Crucially, an implied consent cookie banner notifying the consumer of the use of cookies, or even an opt-in consent cookie pop-up, would **not** be sufficient to comply with U.S. state data protection law opt-out rights.

Vendor Management and Data Protection Addendums

Beyond controls and measures placed on businesses, each new U.S. state data protection law also requires in-scope businesses to consider certain data privacy and information security principles in their contracts with third parties that will have access to or otherwise process personal information on the business's behalf.

The flow-through contractual requirements generally work to further four principles: (1) data minimization-using the minimum amount of information, for specified purposes and periods of time; (2) data subject privacy rights; (3) appropriate and reasonable security measures; and (4) adherence to applicable data protection laws. Some examples of more stringent requirements include requiring an opportunity to object to subcontractors who will be processing or accessing the personal information and assistance in complying with data subject rights requests (e.g., deleting personal information).

Under most U.S. state data protection laws, the contractual requirements establish the fact that the third party is a "processor" or "service provider" to ensure the access to and processing of personal information is not considered a "sale" of personal information-which would be subject to consumer opt-out rights.

California's data protection law is perhaps the most aggressive, however, in requiring contractual flowthroughs in **any** engagement with another business that allows for access to or processing of personal information, even where that third party is making independent use of the information, and the parties are not intending that third party to be a "service provider" or "processor". One of the contractual requirements that is unique to California is to ensure that the contract must include a provision that ensures the third party processing personal information keeps the in-scope personal information separate from personal information independently collected by the third party.

Sensitive Personal Information

While each U.S. state data protection law undoubtedly has substantive differences-such as the rights they grant to individuals residing in their respective states-they all have one point of overlap: the introduction of "sensitive personal information" into the U.S. data protection regime.

Each U.S. state's data protection law places greater requirements on the collection and processing of sensitive personal information, while also granting, in some form, rights to individuals to grant them more control over businesses' collection and processing of their sensitive personal information.

Generally, “sensitive personal information” includes those categories of information that, if used in an unauthorized manner, could lead to significant harm to the applicable individual. This includes financial account log-in information, health and genetic information, biometric information, personal information of children, precise geolocation information, and sensitive demographic information (such as race, ethnicity, immigration status, sexual orientation, etc.).

Of the 13 U.S. states with data protection laws on the books, 10 require that businesses obtain a consumer’s prior, express, opt-in consent before they collect any sensitive personal information. The other three-California, Iowa, and Utah-require businesses to provide individuals notice and an opportunity to opt-out of the collection of their sensitive personal information prior to the collection and use by the business.

Audits and Cybersecurity Reviews

From a practical standpoint, businesses that fall under any of the new U.S. state data protection laws will need to undergo some form of review and assessment to determine (1) what data they are collecting; (2) cybersecurity protections that are in place; (3) access controls to that data; and (4) what that data is used for and how long it is retained. An in-scope business will not be able to ascertain their legal requirements without first undergoing an internal review.

From a legal standpoint-as it relates to mandatory reviews and audits-the U.S. state data protection laws differ. California requires annual audits where a business’s data processing creates a high risk to an individual’s privacy or security. Most of the other U.S. state data protection laws (such as Colorado, Connecticut, Virginia, etc.) require in-scope businesses to conduct and document “data protection assessments” if certain activities (such as the sale of information) are occurring. Utah stands out, as it does not have an affirmative review, audit, or assessment requirement.

In addition to legal requirements placed directly on the business or controller of the personal information, the data protection laws in Colorado, Connecticut, and Virginia require the in-scope business to require its subcontractors and third parties that collect, store, use, or process the personal information on the business’s behalf to allow the in-scope business to audit that subcontractor’s or third party’s compliance with the applicable law.

Record Keeping Requirements and Disclosures

For larger business-to-consumer organizations-such as retailers-additional record keeping and transparency requirements may apply, which highlights the increased focus business-to-consumer organizations should give to U.S. state data protection law compliance.

For example, under California’s data protection law, businesses that collect the personal information of 10,000,000 or more consumers in a given year must compile the following metrics from the previous calendar year:

1. the number of requests to delete personal information the business received, complied with in whole or in part, and denied;

   the number of requests to correct personal information the business received, complied with in whole or in part, and denied;

the number of requests to know the business received, complied with in whole or in part, and denied;

the number of requests to opt-out of sale/sharing personal information the business received, complied with in whole or in part, and denied;

the number of requests to limit the use of sensitive personal information the business received, complied with in whole or in part, and denied; and

the median or average number of days within which the business substantively responded to requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.

In-scope businesses must then, by July 1 of every calendar year, publish the above information and metrics within their privacy policy that is posted on their website. This requires in-scope businesses to build out a substantive policy and program for responding to consumer data privacy rights, which will also need to include robust record keeping policies.

In furtherance of that, California's data protection law also requires businesses that know or reasonably should know that they collect or otherwise process the personal information of 10,000,000 or more consumers in a calendar year to establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer data privacy rights requests are informed of all the requirements under the applicable data protection laws.

Conclusion

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.

As the page turns to 2024, expect even more states to push for new state data protection laws.

As more states continue to implement their own variations of data protection laws and businesses juggle the various requirements, 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.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.

Matthew Farrell at mpfarrell@beneschlaw.com or 628.600.2244.