To be or not to be: a de facto consent-based framework in the U.S.?

By Idara E. Udofia, Esq., Reed Smith LLP

SEPTEMBER 17, 2025

One of the hallmarks of U.S. privacy regulations is the absence of a federal, comprehensive, data privacy law. Instead, consumer personal information is regulated by a hodgepodge of federal and state laws and regulations. Despite the complex web, the United States has historically maintained an opt-out framework, in that covered entities are not generally required to obtain consent before processing personal information.

This opt-out framework notably differs from other jurisdictions, such as the European Union or Brazil, that maintain federal data privacy laws that require controllers to have a legitimate basis to lawfully process personal data or otherwise obtain consent.

Although data privacy laws may not expressly require controllers to obtain consent in the United States, trends around increasing scrutiny and liability associated with consumer privacy have the potential to shift the industry to a de facto consent-based privacy framework.

Within the last decade, more than 20 states have passed comprehensive privacy laws. Although some state laws have notable differences, these omnibus privacy laws are relatively similar. For instance, these state privacy laws do not generally require consent. Moreover, controllers are tasked with providing privacy disclosures, honoring data subject rights, and maintaining processor agreements, among other obligations.

In terms of privacy policies, controllers are required to adequately explain their data practices, including the type of personal data they collect, the purpose for collecting the personal data, and the parties with whom they disclose personal data, among other details.

While these state laws may not generally require consent or limit processing to a predetermined list of legitimate bases, they do require controllers to clearly explain their purposes for processing consumer personal data. In turn, controllers are limited to engaging in processing activities that are reasonably necessary or compatible with the purposes disclosed to the consumers, and data subjects would have the ability to review these privacy disclosures and determine whether to opt-out from certain processing.

It is important to note that while the United States is generally considered an opt-out regime where the onus is arguably placed on the consumer to decide whether to opt-out of processing, the United States has consistently maintained certain exceptions to this framework. Specifically, consent has been required for the collection of more sensitive data such as biometrics, children's data or health data.

Although data privacy laws may not expressly require controllers to obtain consent in the United States, trends around increasing scrutiny and liability associated with consumer privacy have the potential to shift the industry to a de facto consent-based privacy framework.

In addition, certain technologies, including telematics and automatic license plate reader technology, that have the potential to reveal information about an individual's precise location or whereabouts have also required consent. Similarly, a handful of states maintain telephone call recording laws that require anywhere from one to all parties involved in the communication to consent to a recording before the call can be lawfully recorded.

In addition to making exceptions for the type of data, data subject and technology, certain states have started to require consent for certain processing activities. For example, the Connecticut Data Privacy Act prohibits controllers from selling personal data without first obtaining consent.

While the U.S. framework includes opt-in requirements for certain processing activities, companies were generally not adopting a consent-based framework wholesale. State legislatures simply had not gone that far to require it.

However, the wave of consumer privacy class actions in recent years may take a toll. By way of example, we can look to the flurry of wiretapping and eavesdropping litigation in California. According to the Report to the Committee on Public Safety for the California Senate Bill 690, over 1,500 lawsuits have been filed within the last two years under the California Invasion of Privacy Act (CIPA).

In an effort to mitigate risk, several companies turned to consent-based mechanisms. Although the United States does not require cookie banners, some companies have implemented banners asking for express consent as it relates to their use of tracking technologies.

CIPA generally prohibits wiretapping; eavesdropping on, or recording, a confidential communication; or intercepting and recording a communication without consent. CIPA provides $5,000 statutory damages for each violation of the statute.

Plaintiffs have brought lawsuits under several theories, including that the use without consent of commonplace website tracking technologies, such as cookies, pixels or tags, to collect personal information about users that visit websites constitutes "wiretapping" or an unlawful pen register under the Act.

California is not alone in that it is one of several states with anti-wiretapping and eavesdropping laws that contain a private right of action and statutory damages. While some courts have provided clarity as to whether these standard practices fall within the purview of the state anti-wiretapping eavesdropping laws, divergence exists across states, which can be challenging for companies with national platforms.

In an effort to mitigate risk, several companies turned to consent-based mechanisms. Although the United States does not require cookie banners, some companies have implemented banners asking for express consent as it relates to their use of tracking technologies. By asking for consent, companies could potentially establish an affirmative defense against wiretapping, eavesdropping, and certain other allegations where consent is a recognized exception under the law.

There has been a notable increase in the number of companies that maintain consent banners in the United States. This firm's survey of Fortune 500 company websites is illustrative of this point, as nearly half of these top performing companies have used a consent banner within the United States.

While state comprehensive privacy laws generally maintain an opt-out framework, and consent is not necessarily required, companies continue to leverage opt-in mechanisms to help mitigate risks. The response, itself, has the potential to contribute to shifting the industry further along the path to a consent-based framework, and perhaps even influencing legislative bodies to incorporate more opt-in requirements along the way.

About the author

Idara E. Udofia, a partner who leads US privacy for the emerging technologies group at **Reed Smith LLP**, focuses their practice around data privacy and security, advertising, marketing, e-commerce, technology and brand protection. Udofia advises clients across an array of industries, including, entertainment and media companies, digital platforms, consumer packaged goods companies, pharmaceuticals, retail, hospitality, travel, sports and financial services, and on various data protection laws, including, CCPA, COPPA, BIPA, and GDPR. They can be reached at iudofia@reedsmith.com.

This article was first published on Reuters Legal News and Westlaw Today on September 17, 2025.