Kilpatrick

Insights: Alert

“Secondary Uses” of Personal Data Should Still be Your Primary Concern: Consent Requirements under U.S. State Privacy Laws

August 16, 2023

Written by **Meghan K. Farmer**

In March of this year, we wrote about “secondary use” consent requirements under the CCPA and Colorado's CPA. Since that post, the number of U.S. state privacy laws has roughly doubled. Determining consent requirements under so many similar but slightly divergent laws can be an overwhelming undertaking. Distinguishing between primary and secondary uses of personal data is important because a primary use of personal data does not generally require a data subject's explicit consent (absent additional factors like the use of sensitive information). A secondary use, conversely, requires consent (unless an exception to the law applies, like processing for legal compliance). To help with compliance, we created the chart below that details secondary use consent requirements by state. We conclude with our tips on how best to ensure proper consent is obtained.

State law	Effective Date	Treatment of “Secondary Uses” of Data
California Consumer Privacy Act (CCPA) and Consumer Privacy Rights Act (CPRA)	Jan 1, 2023	Any time information is used in a manner that is inconsistent with what the “reasonable expectations” of the consumer, the business must obtain explicit consent for that use. (Sec. 7002(a)).
Colorado Privacy Act (CPA)	July 1, 2023	A “secondary use” of personal information is any use that is different than the processing purposes disclosed to consumers at or before the time of collection. (Rule 6.08). If data is being used for secondary purposes, opt-in consent is needed before the processing activity takes place.
Connecticut Personal Data Privacy and Online Monitoring Act	July 1, 2023	Unless the controller obtains the consumer's consent, the controller may not process personal data for purposes that are “neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed” as disclosed to the consumer. (Sec. 6(c)).
Indiana Consumer Data Protection Act	Jan 1, 2026	Same as Connecticut. (Chapter 4).
Iowa Consumer Data Protection Act	Jan 1, 2025	Does not include a provision on secondary use.
Montana Consumer Data Privacy Act	Oct 1, 2024	Same as Connecticut. (Sec. 7(2)(a)).

Tennessee Information Protection Act	July 1, 2025	Same as Connecticut. (47-18-3204(a)(2)).
Texas Data Privacy and Security Act	July 1, 2024	Same as Connecticut. (Sec. 541.101(b)(1)).
Utah Consumer Privacy Act	Dec 31, 2023	Same as Connecticut. (Sec. 13-61-302).
Virginia Consumer Data Protection Act	Jan 1, 2023	Same as Connecticut. (Sec. 59.1-578).
Washington My Health My Data Act	March 31, 2024	Same as Colorado (Sec. 4).

Striving for Compliance

True to form, California takes a unique approach. As you can tell from the chart above, there are essentially two approaches to consent for secondary use: The California approach and the Connecticut approach (while Colorado's statute uses different wording than Connecticut's, practically speaking, the approach to compliance remains the same).

To use data secondarily in California requires a more nuanced analysis of whether consent is required than in states that follow the Connecticut approach. The “reasonable expectations” standard is undefined. Therefore, we recommend considering how familiar consumers are with your industry and its practices generally. Under other statutes, a reasonable consumer's expectations are not determined by the ideas of a few consumers, but instead by whether “a significant portion of the general consuming public” holds such a belief.[1] The more familiar a consumer is with your industry and its data use practices, the more likely it is that using data in line with those industry practices will not require consent. We also recommend shaping consumers' expectations through conspicuous disclosures. This includes through your privacy notice, just-in-time notices, and other notification mechanisms that make data use practices more visible and therefore, more likely to be what an average consumer should expect.

The CCPA regulations lay out some of the factors that the California Attorney General (AG) will consider when determining a consumer's reasonable expectations. These include:

- The relationship between the consumer and the business.
- The type, nature, and amount of personal information that the business seeks to collect or process.
- The source of the personal information and method of collection.
- The specificity, explicitness, prominence, and clarity of disclosures to consumers.
- The degree to which the involvement of service provider, contractors, third parties, or other entities involved in the collecting or processing of the personal information is apparent to the consumer.

To use data secondarily in other states requires companies to consider whether such a use was anticipated in the notice provided to consumers. If not, a company would likely need to launch an in-product consent or similar interface to capture data subjects' permission for the secondary use. That analysis raises several tricky operational issues.

- **Separate Notices, but One Database.** Different privacy notices (i.e., different versions of the same enterprise-wide notices or separate product-specific notices) might have been disclosed to consumers. Most companies don't store data separately based on the privacy notice under which the company collected the personal data. Secondary use concerns therefore arise if any of the privacy notices under which the data was collected don't adequately describe a

desired processing activity. A company should collect opt-in consent, therefore, if any of the applicable privacy notices—not just the current notice—inadequately describe a new processing activity.

- **Processing Role and Customer Backlash.** Moreover, new uses of personal data might change a vendor's role from a processor to a controller, which might trigger notice and consent requirements—with respect to both customers and consumers. Those notice and consent requirements might introduce substantial business risk of concerned customers. Product teams should consider the business risk of making any contractual changes or seeking customer consent. Some customers may rely on a company's processor status for the company's own legal compliance. We've also seen commercial push back against changes to terms to allow for AI model training. Deciding to seek customer and consumer consent for new uses of data is therefore a business as much as a privacy-compliance choice.

Of course, the “reasonably necessary” and “compatible with the disclosed purposes” language of the state statutes do give companies a bit of leeway in how much they need to disclose up front, the safest approach is to disclose the use case from the outset.

Usecase	Secondary use in California?	Secondary use in other states?
A retailer uses personal information to fulfill an order that a consumer made. The privacy notice in effect at the time of the purchase states personal information will be used to provide products and services requested by a consumer.	No. A consumer should reasonably expect that if they place an order, their personal information will be used to fulfill that order.	No. This use of personal information was described in the privacy notice at the time of collection.
Same facts as above, but the privacy notice does not state that personal information will be used to provide products and services requested by a consumer.	Same answer as above.	Yes. Even though this use of personal information seems like it would be obvious to consumers, the usecase was not described to consumers at the time of collection and therefore, it is a secondary use requiring opt-in consent.
A video game company sells personal information to tv providers who use the information to send targeted ads to the consumer. This usecase is not described in the privacy notice at the time of collection.	Probably. An average consumer may not reasonably expect that their information would be sold to TV providers. And because the usecase is not described in the privacy notice, the company cannot argue it shaped consumer expectations through disclosures.	Yes. Because this usecase was not described to consumers at the time of collection.
Same facts as above, except that the video game company advertises their relationship with the TV provider and the video game provider offers its players a discounted rate for the TV	No. In this circumstance, the usecase's disclosure in the privacy notice along with the prominent advertising help shape consumer expectations. The video game provider has a much stronger	No. This usecase was described in the privacy notice at the time of collection and therefore, it is not a secondary use.

provider's services. This discounted rate is also advertised in the video game itself, and on the video game's website. This usecase is described in the privacy notice in effect at the time of collection.	argument that a consumer should reasonably expect their information to be used in this way.	

Footnotes

[1] Moore v. Trader Joe's Company, No. 19-16618 (9th Cir. July 15, 2021).