iapp WHITE PAPER

The Alignment Problem with "Sale of Data"

By IAPP Westin Fellow Anokhy Desai, CIPP/US, CIPT

Contents

CONTENT OVERVIEW

- Discover how privacy professionals across ten industries responded to the Sephora enforcement action.
- Learn how privacy professionals are updating their practices to account for the expansion of "sale."
- Explore the technical, legal and business lenses different organizations use to review existing processes and create new ones.

Executive Summary

In August 2022, the California Office of the Attorney General announced a $1.2 million settlement with international cosmetic retailer Sephora for violations of the California Consumer Privacy Act. A wave of questions about the regulator's emphasis on the broad interpretation of the CCPA's "sale of data" and adoption of the Global Privacy Control followed the announcement. The interpretation of a "sale" of personal data has been a lingering issue since the passage of the CCPA. Variations between existing U.S. state consumer privacy laws and the proposed American Data Privacy and Protection Act, industry groups' definitions and self-regulatory guidance and the California attorney general's focus on technical compliance highlight a lack of consensus on how to implement compliant "sale" and sharing of personal data across organizations and industries.

The Sephora enforcement action sparked new questions about the definition of "sale of data," the feasibility of reclassifying vendors as service providers and the necessity of conducting organizational compliance overhauls. The reclassification of vendors as service providers is especially crucial because of the way a sale of personal information is defined as such when the recipient is a third party, whereas the definition does not extend to a service provider.

The IAPP Westin Research Center interviewed privacy professionals across ten industries to understand how organizations responded to the enforcement action. Privacy professionals from organizations of varying sizes and industries are attempting to address questions created by Sephora through technical, legal and business lenses, each with their own priorities and risks. With several statutory loopholes unaddressed by the CPRA and current draft regulations, some industries are left to balance compliance and business needs. Respondents were split between wanting more clarity in the definition of "sale of data" and being ambivalent about an update in the language, noting what is really needed is clear implementation guidance. In an effort to find a consistent approach to comply with a post-Sephora CCPA with limited resources, privacy professionals are looking within their industries for answers.

The technical issue

Privacy professionals found the Sephora enforcement action directly addressed technical issues. Sephora has since committed to operational improvements, which include recognizing browser-based opt-out mechanisms like the GPC. A privacy professional in the retail industry shared their organization's priority, before diving into the GPC, is agreeing on a way to implement a sustainable method across all states, especially those with distinct privacy laws.

> ***Certain organizations find it more onerous to process opt-out requests and tend to treat opt outs as deletion requests instead.***

Another privacy professional in the marketing technology industry said their company understands GPC compliance as a market differentiator, showing consumers they prioritize privacy. This company treats the GPC as a "do not sell" button. Along with another privacy professional in the fraud-prevention industry, they agreed certain organizations find it more onerous to process opt-out requests and tend to treat opt outs as deletion requests instead, due to company size, budget, the way data is used or the way databases are managed.

One advertising technology attorney noted organizations' main confusion is not what the GPC or "do not sell or share" buttons are meant to do, but how to operationalize privacy requirements. Further, they noted most current vendor solutions effectuate the opt-out by dropping a "do not sell" cookie on the user's browser, which is removed when cookies are cleared. This type of solution may not meet California compliance obligations because it puts the onus on consumers to continuously monitor their opt-outs, rather than on organizations to recognize the first opt-out request. Two privacy professionals agreed, saying organizations that have reviewed their back-end processes to ensure the functionality of user opt-out mechanisms have yet to find a one-size-fits-all solution to optimize the process of notifying downstream participants of user opt-outs.

The legal issue

In addition to the importance of the GPC and the "do not sell" button, privacy professionals agreed the enforcement action emphasized legal solutions. The settlement required Sephora to update its consumer privacy disclosures to indicate it sells consumers' personal information, allow consumers to opt-out of the sale, review its agreements with third parties and service providers to restrict the use of consumer personal information and regularly submit compliance reports to the attorney general's office for two years. This has prompted organizations to take similar actions: providing notice and opt-out rights to consumers and reviewing vendor and third-party contracts.

Notice

Providing consumers with notice about whether their personal information is sold is not a new concept. All respondents indicated their organizations have complied with this requirement since the passage of the CCPA. The broad interpretation in the Sephora enforcement action to include data shared for valuable consideration, coupled with the CPRA's pending expansion of opt-out requirements for even broader sharing arrangements, have caused some organizations to reconsider their notices. Three attorneys in this space noted, while statutory interpretation is a standard part of a lawyer's job, the difficulty lies in explaining the expansion of "sale" to include selling to key decision-makers within their organizations and organizational clients. They shared initial pushback at the broadened definition is often accompanied by panic about whether their internal practices will need another full compliance overhaul — something they said most organizations today do not need — and concern about how to operationalize "do not sell" to avoid becoming the next enforcement example.

Contract review

Two privacy professionals in the retail and adtech industries shared similar concerns about the pressure law firms and consent-management providers place on organizational decision-makers to purchase legal or technical services for such compliance overhauls. While their organizations end up paying outside counsel to redraft contracts with vendors and service providers and perform various risk analyses, they believe internal reviews of existing contracts, reviews of user data flows and usages and potential reclassification of vendors as service providers are of greater importance. Budgetary concerns amid economic headwinds play a factor here. Respondents unanimously noted such a reclassification would take minimal, if any, time because most third parties they work with made this change proactively, or agreed to it before the Sephora enforcement action.

All respondents agreed one of the main solutions they utilize is reviewing and updating contracts with service providers and external organizations. Service providers are a crucial part of the alignment problem with "sale" because a sale of personal information is only a "sale" if it is transferred to a third party, but is not classified as a "sale" if it is transferred to a service provider. A Fortune 500 privacy professional's main response to Sephora has been reviewing how their organization contracts with service

providers and other vendors. They noted the organization has not drastically changed its practices, but Sephora gives it "more teeth" and the ability to be stricter with outbound data. The marketing technology privacy professional shared nothing changed for their organization because the B2B company already underwent both the service-provider transition and contract reviews to make sure agreements were ironclad. A senior privacy manager at another B2B company stated their organization does not sell personal information or collect data from its organizational clients. However, they are still taking a cue from Sephora by retaining outside counsel to review data flows for any gaps not covered under their existing contracts and internally discussing various data-use cases and privacy solutions to each of those instances.

Internal review

Similarly, a privacy attorney at a social media company is conducting a data inventory of personal and non-personal information flows to outbound partners to determine whether to update the organization's current policies and contracts. Their service provider review process includes exhaustive evaluations of security and CCPA requirements, to ensure any data used by service providers is for the controller's benefit, data is only shared for the purposes listed in written agreements and data is siloed based on sensitivity and privacy requirements. Three attorneys alluded to minor difficulties with vendors that held greater bargaining power and did not initially agree to undergo the reclassification process to become a service provider.

A partner at a privacy and data security firm pointed out vendors who resist becoming service providers may do so because they gain more value from their current usage of an organization's data than they might from a business relationship requiring purpose and use limitation. Businesses only wanting to share data with a service provider must make the difficult decision to ensure their disclosures are compliant by reviewing third-party contracts and opting to end long-standing relationships to search for vendors who will agree to service-provider requirements.

Interpretation

In order to provide the best counsel to clients, attorneys often try to decipher the intent behind an enforcement action or regulation when the guidance seems unclear. In the view of the retail privacy professional, the Sephora enforcement action was more about addressing noncompliance than highlighting the violation of an explicit privacy right, and the intent behind the settlement was unclear. "We'll read FTC decisions and immediately be able to understand what privacy right they are addressing, whether it's unfairness, deception or a privacy or security control the FTC regularly monitors. Between Kochava and Sephora, though, it's clear that one was about violating privacy rights and one was just about a compliance error," they said during the study. They also noted organizations trying to comply with the law, without considering the intent of the enforcement and their organization's overall "privacy story," are going to provide bad user experiences. At the same time, they understand a number of organizations are waiting to see how others in their industry assess what is "good enough" before allocating more resources towards their legal or privacy team.

The business issue

Finally, privacy professionals alluded to the enforcement action highlighting unaddressed business issues. The uncertainty of how and when to meet compliance obligations under the Sephora enforcement action is a business problem because organizations' finite resources cannot be fully allocated to frequent regulatory updates within one department and their strategic goals are halted when staff turn their attention to urgent compliance needs.

Vendor management

The privacy professional from a Fortune 500 company shared they are reviewing and, in some cases, reassessing vendors to ensure they are both willing to comply with service provider requirements and are agile enough to update their data use and processes based on current varying privacy laws and those on the horizon. "In this tough regulatory environment, you have to act in good faith to comply with U.S. and EU regulations and updates," which, they lamented, can take more than one fiscal year's allocated budget for a privacy department and lead to delayed compliance. They encourage privacy professionals who are renewing vendor contracts to consider the context of upcoming privacy regulations, economic headwinds and the value of continued business relationships.

Two birds, one stone

Another resource-related consideration an in-house attorney worked on is globalizing their organization's data processing agreements and applying existing EU General Data Protection Regulation sub-processer requirements to California processers and service providers. By utilizing existing privacy processes, the organization saved time and money without sacrificing user privacy. Other organizations are using the opposite approach by creating new processes to protect user data. Two privacy professionals who worked with mobile apps found, while certain privacy protective measures "hit a lot of pockets," they also acted as an encouraging push for organizations to develop a way to collect and employ user data for protected business purposes while still promoting transparency.

Strategic considerations

Some companies strategically capitalized on the "do not sell" language to ensure their users' data is protected and only used by specific parties in agreed upon ways, and to mark their places as industry leaders in privacy. Strict adherence to the regulation also shows vendors following service provider requirements is the only way to continue their business relationship, which bolsters the organization's reputation. In contrast, one attorney noted it is disappointing to make the right call regarding privacy only to lose a previously held business advantage and witness others in the same industry avoid penalization while being noncompliant. Until there is alignment across industries, attorneys and business leaders will make these difficult decisions every day.

The "what about us" problem

The risk and fraud-prevention industry has not yet been heavily impacted by new "sale" interpretations or by the Sephora enforcement action. A privacy attorney in the industry stated their organization is strictly a processor and does not use data in a customer capacity. Instead, they look at fraud clusters to leverage suspicious transactions and make relevant correlations to prevent misuse of personal and sensitive information, like an individual's credit card number and driver's license. The organization's use of personal data is a legitimate interest; if they were unable to collect a consumer's transaction pinpointed to a specific date, time and geolocation, they would not be able to alert consumers about their personally identifiable information being used in potentially fraudulent transactions. For the same reasons, they cannot utilize privacy-conscious solutions like data aggregation and deidentification, because the specificity of individual data allows the organization to do its job. While this industry uses mechanisms like hashes to compare sensitive information or consumer records after documents are deleted, it is difficult to work with fully encrypted databases, for example, when fraudulent activity is so time sensitive. Additionally, if a user submits a deletion request, fraud-prevention organizations need to balance privacy rights with the necessity of retaining information, like a scan of a counterfeit ID, to notify the affected individual in a more accurate and timely manner in the future.

In addition to the countervailing interests of providing more accurate services while giving users the privacy rights they are afforded elsewhere, there lies a definitional issue regarding the allowed uses of data. The above-mentioned partner at a privacy and data security firm, pointed out a gap in the CPRA's definition of "service provider." The definition requires a contract prohibiting the service provider from combining personal information received from the businesses it works with, other people or from its own interactions with consumers, "provided that the service provider may combine personal information to perform any business purpose" as defined by section 1798.185 (a)(10) of the CCPA. The paragraph notes

> ***The combination of personal data from multiple sources allows many companies in the security, risk and fraud-prevention industries to provide their services.***

the California attorney general will adopt regulations to further the purposes of the act, including issuing regulations to further define the business purposes under which service providers and other parties "use consumers' personal information consistent with consumers' expectations, and ... combine consumers' personal information obtained from different sources." The combination of personal data from multiple sources allows many companies in the security, risk and fraud-prevention industries to provide their services. Further, they note the current draft regulations outline purposes under which a service provider can retain, use and disclose personal information, but they do not clearly propose any business purposes for which service providers or contracts can combine personal information. Accordingly, both this attorney and the privacy attorney in the fraud-prevention industry agree the gap in this definition requires more clarity.

What needs to change?

Various factors, including size, budget, risk tolerance and industry profile, impact the approach privacy professionals took to respond to Sephora and prepare for future scrutiny in California. When asked whether they would change the term or definition of "sale of data," respondents provided one of two responses. The first group did not feel strongly about changes to the term or definition but understood the expansion of "selling" to include "sharing" is guided by the intent to protect consumers broadly based on privacy principles and focused on intent rather than the text. The other group would prefer to see explicit separation between the two terms in both the definition and statute. They believe the definitions of "selling" and "sharing" data should remain distinct and statutory language should explicitly state whether certain activities can involve selling, sharing, both or neither. Attorneys who were part of the second group prefer this kind of change for ease of explanation to decision-makers with little to no privacy knowledge. Whether it is more clarity in statutory definitions or guidance on how to operationalize the results of future CCPA enforcement actions, one thing is clear: the more transparent organizations are with each other about their roadblocks and interpretations, the more consistent the privacy community can be when building best practices across industries.

> ***The more transparent organizations are with each other about their roadblocks and interpretations, the more consistent the privacy community can be when building best practices across industries.***

Contact

Anokhy Desai, CIPP/US, CIPT
Westin Fellow, IAPP
adesai@iapp.org

IAPP Research and Insights
research@iapp.org

Follow IAPP on Social Media

Published December 2022.