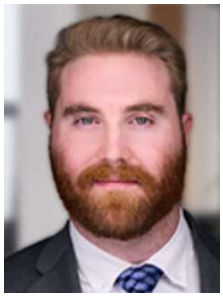
Enforcement Risk Amid Increased Consumer Data Use

By **Kyle Miller, Dalton Cline and Jessica Bartolacci** (March 8, 2024)

Kyle Miller



Dalton Cline

Jessica Bartolacci

Personal data has been analogized to oil and plutonium to demonstrate both its value and risk.

Data — including consumer personally identifiable data — is foundational to everything retailers do: monitoring market trends, predicting demand, evaluating marketing spend, tracking product purchasing patterns, increasing operational efficiency, crafting advertisements and making informed business decisions.

Retail businesses increasingly capture the value of their first-party data through their own retail media networks, or RMNs, by selling ad space on their own digital channels to third-party brands.

Simultaneously, retailers must face the growing hazards associated with third-party data, and the depreciation of formerly fundamental aspects of the digital ad economy, like third-party cookies.

Personal data has value in the abstract, however, retailers often need to put a dollars-and-cents value on data elements or the value of the aggregate personal data that it has on a specific consumer.

How to approach data valuations — and developing a methodology for a consistent answer — is important for risk management and legal compliance under the growing patchwork of comprehensive state privacy laws.

Data Valuation Under The California Consumer Privacy Act

Comprehensive consumer privacy laws often grant consumers the right to nonretaliation, protecting them from discriminatory treatment — such as differing prices, quality, or goods and services — when they exercise their data subject rights.

But, there are circumstances where a different price can be offered. For example, a California business may offer a different "price, rate, level, or quality of goods or services" if that price is "reasonably related to the value provided to the business by the consumer's data."[1]

Additionally, the business may offer a financial incentive to induce consumers to allow the collection, sale, sharing or retention of their data.[2] Under either of these provisions,[3] the business is required to provide a particular notice to the consumer.

Among the elements required in the notice of financial incentives, the California Privacy Protection Agency regulations require

an explanation of how the price or service difference is reasonably related to the value of the consumer's data, including: a good-faith estimate of the value of the consumer's data

that forms the basis for offering the price or service difference; and a description of the method(s) the business used to calculate the value of the consumer's data.[4]

The CPPA regulations also provide the factors a business must select from to calculate the value of the consumer's data:[5]

- The marginal value to the business of the sale, collection or deletion of a consumer's data;
- The average value to the business of the sale, collection or deletion of a consumer's data;
- The aggregate value to the business of the sale, collection or deletion of consumers' data, divided by the total number of consumers;
- Revenue generated by the business from the sale, collection or retention of consumers' personal information;
- Expenses related to the sale, collection or retention of consumers' personal information;
- Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference;
- Profit generated by the business from the sale, collection or retention of consumers' personal information; and
- Any other practical and reasonably reliable method of calculation used in good faith.

Other Data Valuation Considerations

The California Consumer Privacy Act factors provide a framework for evaluating consumer data, but other factors are routinely considered when evaluating data processing.

Assets are often valued at the price at which they could be sold on an open market.

However, market valuation may not be appropriate for retail data valuations for several reasons. Data is nonrival in economic terms — its use by one entity does not deplete its ability to be used by others.

Additionally, the value of data will vary significantly in the hands of different processors. An organization that collects data directly from its consumers with appropriate consent will often have more legally permissible uses of that data than a company that acquires the same data in other ways.

The comprehensive state privacy laws that restrict the use of personally identifiable data can increase the value of that same data in the hands of retailers.

Historically, retailers have been advertising purchasers, engaging in the sometimes-restricted practice of sharing data with advertisers to build targeted campaigns.

Considering increased restrictions in sharing data for advertising purposes, retailers now

leverage their RMN to offer advertisements on their platforms using the first-party data they already process. RMNs can increase the value of a retailer's data and, at the same time, provide a market-based metric for valuing the data.

Additionally, if a retailer uses data to inform its processes, the data must be correct. Comprehensive privacy laws often give consumers the right to correct data processed by retailers, further increasing the value of the retailer's data set.[6]

Other considerations in valuing data could include the business purpose for processing the data, the cost to the business of fulfilling that purpose without the data, the benefit the business receives by fulfilling the business purpose with the data as opposed to without, and the cost to the business if it did not fulfill the business purpose of processing at all.

Understanding the value and risk of the data processed will be increasingly important as regulators increasingly scrutinize data processing.

Risk Management

A retailer's approach to data valuation can be leveraged as part of a larger risk management strategy focused on collection and retention minimization.

Collection Limitation

Limitation of consumer personal data collection and retention to data that has a clear and defensible value proposition to the business reduces overhead and processing costs.

For example, cloud storage providers frequently provide different pricing levels for various cloud storage classes, charging a steeply discounted rate for data that is seldom accessed — like archival data — compared to frequently accessed data.

Retention Minimization

Deleting, aggregating or anonymizing historical data that no longer has business utility reduces the risk of a data breach, or minimizes the impact of one.

The indefinite retention of all consumer personal data means that every security event can potentially expose the company to millions of dollars of fines, penalties, judgments and other fees.

It is widely understood that breach notification statutes protect Social Security numbers and payment card details, but additional data types relevant to retailers, such as username and password combinations, are also protected in some jurisdictions.[7]

Long dormant and unused account credentials associated with loyalty programs or online accounts, especially ones created before strengthened password requirements, are a source of risk.

Collection and retention minimization are also legal requirements. All comprehensive consumer privacy laws have an equivalent of the collection limitation principle, which Virginia expresses as the duty of a controller to "limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed."[8]

Additionally, the Colorado rules have introduced a storage limitation principle, requiring that personal data that is "no longer necessary, adequate, or relevant to the express Processing purpose(s)" be deleted.[9]

Conclusion

Although consumer personal data is undeniably an asset to an organization, it also introduces risk and the potential for liability.

While no state has introduced a private right of action for noncompliance with a comprehensive consumer privacy law — except for the California Consumer Privacy Act's data breach provision — organizations face risk from enforcement actions by state attorneys general and privacy regulators.

Kyle Miller is a partner, and Dalton Cline and Jessica Bartolacci are associates, at Dentons.

Dentons shareholder Matthew H. Clark, summer associate Caroline Bailey and former associate Carina Mendola contributed to this article.

[1] Cal. Civ. Code 1798.125(b)(1), CPPA Regs. §7080(b).

[2] Id.

[3] 11 CCR § 7001(l), "Financial incentive" means a program, benefit, or other offering, including payments to consumers, for the collection, retention, sale, or sharing of personal information. Price of service differences are types of financial incentives.

[4] 11 CCR § 7016(5).

[5] 11 CCR § 7081(a)(1)-(8).

[6] See, e.g., C.R.S. 6-1-1306(1)(c).

[7] See, e.g., Md. Code Ann., Com. Law. § 14-3501(e)(1)(ii).

[8] Va. Code Ann. § 59.1-578(1).

[9] 4 CCR 904-3 Rule 6.07(B)(1).