Professional Perspective

Value of Personal Information Theories in Data Privacy Class Actions

Michael Kheyfets, Edgeworth Economics

Bloomberg Law

Read Professional Perspectives | Become a Contributor

Reproduced with permission. Published September 2022. Copyright © 2022 The Bureau of National Affairs, Inc. 800.372.1033. For further use, please contact permissions@bloombergindustry.com

Value of Personal Information Theories in Data Privacy Class Actions

Contributed by Michael Kheyfets, Edgeworth Economics

A theory of harm frequently alleged in consumer and employee data breach class actions is that plaintiffs "lost the value of personal information." That is, plaintiffs allege that their sensitive information held by the defendant had value, and the cyberattack on the defendant exfiltrating the data diminished that value.

Assessing economic injury and damages under this type of theory presents economists with questions that may seem semantic but are in fact foundational. What does it mean for "data" to have "value"? And what does it mean for the "value" of "data" to "be lost" as a result of unauthorized disclosure in a cyberattack?

This article will provide an introduction for practitioners to the economic concepts behind these questions.

Market Value Methodologies & Exfiltrated Data

As a starting point for assessing "value of information" theories, it is important to remember that the relevant economic framework is the comparison of what actually happened—the "actual world"—and what would have happened if the cyberattack at issue in the particular litigation did not occur—the "but-for world."

That is, for a given individual in a proposed class to have suffered economic injury under this theory, it must be the case that the value of the exfiltrated data to that individual diminished relative to a but-for world because of the cyberattack. Put differently, it must be the case that the exfiltrated data would be worth more to the individual class member in the but-for world.

Importantly, the relevant economic question is not whether—in general—certain data may have certain types of value to certain types of entities. This distinction is important because the economic arguments with respect to "value of information" claims often purport to rely on "market value" methodologies.

Data is a Unique Asset

A "market" approach refers to a type of methodology for valuing an asset that considers the market prices of recent sales of comparable assets. For example, a person looking to sell their car may be able to use a tool like Kelly Blue Book, which collects data on automobile sales, to estimate a "market value" of their vehicle by looking at data on what prices similar cars were sold for in their area.

However, "markets" for information are less straightforward than those for assets like cars. Arguments about economic injury and damages from the diminution in the value of information in a cyberattack often reference the existence of two types of potential markets: legal and illegal ones. Illegal marketplaces for information are sometimes called the "dark web," a term that refers to websites that do not appear in web searches and require specialized browsers to access.

Plaintiffs in a data breach litigation may reference the existence of the dark web as being a relevant market by noting that it may be able to provide "prices" for certain types of information. For example, if a batch of Social Security Numbers (SSNs) may be illegally purchased on the dark web for an average of $10 per SSN, plaintiffs may reference this amount as a "market value" for this type of information—and the amount by which a given class member would be allegedly damaged if their SSN was exfiltrated in a cyberattack.

"Valuations of data," in a certain sense, may also exist in legitimate contexts. For example, companies called "data brokers" collect information from disparate sources, combine these sources into consumer profiles, bundle those profiles, and sell them to other companies. Firms other than data brokers may also derive value from data—illustrated by the fact that they may be willing to incur the cost of collecting, storing, and analyzing it—if they believe they will be able to extract insights from the data that will result in increased profitability, e.g., through offering a better product or more effectively reaching potential customers.

 ©2022 The Bureau of National Affairs, Inc.

Plaintiffs in a data breach litigation may reference these marketplaces in the same way as the dark web, by noting that they may be able to provide proxies for value lost due to the cyberattack. However, there is a fundamental disconnect between the general notion that "data has value" in certain circumstances and the relevance of that notion to the assessment of economic injury from a particular data breach to individuals like the customers or employees of a specific firm.

Individuals' Access to Data Markets Is Limited

Consider the example of a car theft. There are legitimate marketplaces where an individual car owner can sell their vehicle, and an automobile has monetary value to the owner because it can be sold to another entity—e.g., a used car dealership. For example, if a car can be sold for $20,000, having it stolen would deprive the owner of $20,000 in value they could have received in that hypothetical sale. Additionally, replacing the stolen car with a similar one would cost the owner $20,000.

The question of whether any individual proposed class members would—or even could—have engaged in a "sale" of any information exfiltrated in a cyberattack is more complex. In fact, the economic literature on data privacy and value of information discusses the general inability of individuals to monetize various elements of their personal data. That is, while firms may engage in the sale of certain types of personal data, individual consumers—i.e., the subjects of that data—do not actually have access to the same markets.

To the extent individual class members would not—or could not—sell their personal information on the black market, there would be no but-for world in which those class members were going to monetize their exfiltrated personal identifiable information (PII) but were prevented from doing so by the cyberattack. The same would be the case when using information from "legitimate markets" for PII as a proxy for individual class members' injury and damages. That is, if the individual class members cannot participate in the kind of transactions that data brokers engage in—i.e., bundle their own individual PII with that of others and sell it—then those "market values" are not relevant for assessing the questions of injury and damages to the proposed class member.

At least two additional factors are relevant to the assessment of potential "markets" for data. First, average "values" typically available in the public domain would obscure the individualized value each class member may—or may not—place on any particular piece of information and thus would overstate —or understate—that particular individual's valuation.

Additionally, value of large data sets or data systems to a firm may not reflect the value of an individual's data to that individual. This is because—as the economic literature notes—data about any one person may have limited value to firms, and only gains value once it is combined with data about other people such that it can reveal trends or patterns. For example, an individual's health-related data often gains much of its value from comparison with aggregate patterns across broad populations, but has little—if any—value on its own.

Courts are Split on the Issue

The US District Court for the Southern District of New York recently contemplated this issue in its ruling on the motion to dismiss in the *De Medicis v. Ally Bank* case. Plaintiffs alleged that defendant "negligently disclosed their customers' account usernames, passwords, and other private information to unnamed third parties" and that they have suffered "actual injury in the form of damages to and diminution in the value of [their] Private Information—a form of intangible property."

In granting the defendant's motion to dismiss, the court opined that "Plaintiff fail[ed] to establish that he suffered an alleged 'diminution in the value' of his private information because he fails to allege that there is a market for such information." Moreover, the court noted, "even when assuming that such usernames and passwords have any independent economic value, Plaintiff still fails to allege any facts indicating how the Coding Error diminished such economic value." See *De Medicis v. Ally Bank*, No. 21 Civ. 6799 (NSR), 2022 BL 268366 (S.D.N.Y. Aug. 02, 2022).

The standard by which to assess "lost the value of personal information" theories is not settled, however. For example, in denying—in part—defendant's motion to dismiss, the court in *In re Blackbaud, Inc., Customer Data Breach Litigation* found that "Plaintiffs have sufficiently alleged a causal link between the Ransomware Attack and their damages to survive a motion to dismiss." See *In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 3:20-mn-02972-JMC, 2021 BL 305039 (D.S.C. Aug. 12, 2021).

©2022 The Bureau of National Affairs, Inc.

Economic Characteristics of Information Goods

Data, including PII like names, email addresses, phone numbers, and SSNs that are typically at issue in consumer and employee data breach litigation, is what economists call "information goods." A key characteristic of this type of product—or "good"—is that it is what economists call "non-rival." This means that data can be simultaneously held and/or used by multiple parties without being depleted or diminished.

Consider again the example of a car theft. In contrast with data, a car is a "rival" good. This means that if one entity—e.g., an individual—owns a car, another entity cannot simultaneously own it. Having their car stolen deprives that individual of ownership and the ability to derive value from the car, whether by using it or monetizing its value by selling it. In contrast, no such economic "deprivation of ownership" occurs when data is exfiltrated in a cyberattack. The subject of the data is not deprived of the ability to use their name, address, or SSN.

For example, one way in which individuals derive "value" from their personal information is by providing it to merchants in exchange for discounts and other benefits of retail loyalty programs. If certain information is exfiltrated in a cyberattack, this would not preclude the subject of that information from continuing to use it to sign up for loyalty programs and receiving the associated benefits. That is, there would be no difference between the post-cyberattack actual and but-for worlds in terms of the individual's ability to use and derive value from their PII.

The non-rivalrous nature of information compounds the difficulty of applying "market valuation" methods to "value diminution" theories of economic harm. Individuals—such as proposed class members in a consumer or employee class action—generally do not have access to the kinds of markets where they could sell their personal data, nor is it generally the case that there could exist a circumstance where individuals would sell certain information about themselves—like SSNs and bank account numbers—at all. Moreover, unlike in the case of a car, the "theft" of information does not deprive an individual of economic "ownership" or the ability to use that information.

Conclusion

Given this set of economic characteristics, it is unlikely that generic statistics from public sources purporting to represent "market value" can serve as reliable proxies of the "lost value of information" for any individual class member in a data breach litigation. However, economic arguments and techniques are likely to continue evolving as the analysis in data privacy litigation continues to mature.

©2022 The Bureau of National Affairs, Inc.