Challenges to Quantifying Economic Harm from Data Breaches

BY ERICA GREULICH AND STUART GURREA

September 2023

The number of incidents involving compromised personal data increased significantly over the past decade. In 2022 alone, organizations reported having data compromised in almost two thousand instances in the United States, impacting hundreds of millions of consumers. These incidents include data breaches, as well as unintentional data exposures and data leaks. Exposure of individuals' personal information may result in identity theft and monetary losses to large groups of victims. Consequently, these events often result in class action lawsuits claiming economic damages from the unauthorized access or use of personal identifiable information ("PII") and/or personal health information ("PHI"), and in some cases the mere possibility of access or use. However, plaintiffs attempting to reliably quantify economic harm on a class-wide basis may encounter several issues when assessing the economic value of lost privacy.

As a preliminary matter, exposure of data or the opportunity to access unprotected data does not necessarily imply that data was in fact accessed or sold to bad actors. Following a data breach, plaintiffs may assert harm related to the loss of value inherent in their individual personal information. Under the theory that PII and PHI have intrinsic value to each plaintiff, plaintiffs may claim to be harmed by their loss of privacy following data exposure or the opportunity to access their respective PII and PHI. However, it may be incorrect to assume that unauthorized access or use occurred and correspondingly quantify economic harm based on this assumption that personal information was stolen and used in a manner that harmed plaintiffs.

In general, assessing the economic value of lost privacy is challenging because the value of privacy is subjective and varies across individuals and circumstances. In fact, individual behavior may reveal that an individual has an inconsistent valuation of their own privacy over time or in different situations. One possible approach to assessing these individual valuations of privacy is through carefully designed surveys. However, eliciting subjective valuations in the context of litigation through a survey questionnaire for a class is susceptible to response bias given the qualitative nature of the questions and the financial incentives of claimants who are aware of the survey's purpose.

> **"In general, assessing the economic value of lost privacy is challenging because the value of privacy is subjective and varies across individuals and circumstances."**

An alternative approach to quantifying economic harm from a loss in privacy is to rely on a market-based valuation of privacy whereby actual market transactions involving PII and PHI inform the estimation of the value of the exposed PII and PHI data of interest. Conceptually, as in other contexts, the market-based approach to valuation is based on the notion that similar assets are traded at similar prices.

Prerequisites to implement the market-based approach include (a) the availability of PII or PHI transaction data, and (b) comparability between the available PII and PHI transaction data (the reference assets) and the claimants' exposed private PII or PHI information (the target assets). To satisfy these conditions, plaintiffs may propose to use data for purportedly similar transactions posted on the dark web because the dark web provides a marketplace for data obtained illicitly. The dark web is a portion of the internet that is not accessible using conventional search engines, where transactions can be conducted anonymously, and where illegal transactions involving stolen PII and PHI have been known to occur.

The use of these dark-web data, however, may not provide a reliable benchmark for purposes of valuation. First, this approach assumes that data for illegal transactions offer a reliable benchmark for the target assets. But illicit transaction data can be highly unreliable because of the lack of consistent and verifiable transaction records and because prices may not reflect the price a target asset would command if sold by a legitimate owner in a legal market. Second, available market data for the illicit transactions may be limited to listed rather than actual transaction prices. In the same way that listed prices for real estate assets may be very different than actual selling prices, listed prices for PHI or PII on the dark web may not be a reliable basis for estimating the actual value (selling prices) of these illegal transactions. Thus, relying on these listed prices is not likely to be a reliable approach for estimating the value of hypothetical legal transactions of plaintiffs' personal data.

"In addition to economic harm associated with a loss of privacy, claimants in the class may seek to recover the costs associated with mitigating any perceived incremental risks of additional exposure of their private information from the data breach."

More generally, using dark-web data to measure the value of private information following the market-based approach also is subject to common shortcomings inherent in the application of this methodology. In particular, common criteria for comparability may not be met. For example, temporal comparability, whereby benchmark transaction data are close in time to the transaction of interest, may be hard to achieve because of a scarcity of contemporaneous transactions. Additionally, actual similarity between the types of information observed on the dark web and the target assets may not be met. In some instances, the reference assets involve bundles of information that do not overlap perfectly with the target assets' bundle of information that needs to be valued. These differences undermine the comparability of the transactions. In the case of class-wide claims, there also may be significant variation in the amount and type of information disclosed for different class members.

In addition to economic harm associated with a loss of privacy, claimants in the class may seek to recover the costs associated with mitigating any perceived incremental risks of additional exposure of their private information from the data breach. For example, plaintiffs may spend time and incur costs to put in place credit monitoring services and purchase identity protection services on an ongoing basis. However, the increased use of online transactions exposes most consumers to these risks. Therefore, isolating the incremental impact of the single data breach at issue in a class-action case is difficult. Moreover, in light of these risks, many consumers already may have protection services in place, and these protection services were purchased for reasons unrelated to the data exposure at issue or because fraud prevention services were bundled with other services they purchased. As a result, the incremental cost of protection to mitigate the effects of the data breach is likely to vary across individual plaintiffs and equal zero for some or many.

An economically sound measurement of mitigation costs also must be commensurate with the risk attributable to the breach over time. This calls for accounting for the value of the exposed data over time, its potential staleness (for example, if the data exposure was in the distant past the same PII may have been exposed in another breach which may decrease its value to bad actors), and the potentially declining risk of economic harm further out in time. Any

variability in the components or scope of the individual data exposed is likely to undermine the viability of a class-wide approach to assessing mitigation costs over time. To overcome these difficulties, and because of a lack of reliable data from which to estimate the risk attributable to the breach over time, plaintiffs sometimes propose to rely on the cost of monitoring services that defendants in prior litigation have agreed to pay for in settlement agreements as a measure of individual mitigation costs. From an economic perspective, these settlement payments reflect the risks associated with litigation and are not necessarily a reasonable measurement of incremental mitigation costs borne by plaintiffs to address the risks associated with a particular data breach.

Overall, increasing consumer reliance on digital transactions makes the sharing of PII and PHI information inevitable, and data breaches have become increasingly common. To provide sound economic analysis for monetary claims brought on behalf of a class of claimants involved in a data breach, it is necessary to address the unique analytical challenges posed by data breaches. Moreover, this economic analysis also must satisfy common standards for measuring economic harm on a class-wide basis.

Drs. Erica Greulich and Stuart Gurrea are a Director and Managing Director, respectively, at Secretariat Economists and have experience assessing class action damages claims that stem from PII and PHI data breaches.

Erica Greulich, PhD
Director
egreulich@secretariat.com

Stuart Gurrea, PhD
Managing Director
sgurrea@secretariat.com