Damages Based On The Intrinsic Value Of Privacy?

*Law360, New York (July 8, 2015, 10:15 AM ET)* –

While privacy and data breach cases receive a great deal of media attention, these cases have not produced the large settlements that some observers have predicted. In many cases, plaintiffs have found it difficult to quantify harm beyond the direct financial losses suffered by consumers, such as unauthorized credit card charges and the time spent dealing with these problems.

Damages based on these direct financial losses are typically minimal in comparison to the number of consumers affected. For example, Target Corp. recently settled a class action stemming from the theft of the personal and financial information of over 100 million customers for $10 million.[1] Further, several recent cases, such as those against Gamestop Inc.[2] and Zappos.com Inc.[3], have been dismissed for not meeting the standards for class certification because the plaintiffs could not demonstrate direct financial harm.

Perhaps in response to these recent trends, the number of privacy suits filed in some venues is falling.[4] Given this, plaintiffs are likely to consider new theories of harm and new means by which to estimate damages in privacy and data breach suits.

One relatively untested approach is to seek damages for the intrinsic value of privacy itself. Some plaintiffs now appear to be exploring this route. For instance, in Juliano v. Anthem the plaintiffs argued that unauthorized access to their personal information due to a data breach resulted in a loss of value, even in the absence of direct financial harm.[5]

Even rulings that limit the scope of damages to direct financial losses do not completely close the door on the idea of privacy having an intrinsic value. For instance, in Carlsen v. GameStop the plaintiff alleged harm because his personal information was shared with Facebook Inc. after he had paid for online access to premium content. In dismissing the case U.S. District Judge Donovan W. Frank stated:[6]
Because nonpaying and paying users received the same privacy policy in this case, plaintiff cannot establish that the privacy policy has intrinsic monetary value attributed to it that was paid for and not received.

This suggests that if the plaintiff could have established that an expectation of privacy was included in the price of the good, then he would be entitled to seek damages for the lost intrinsic value of privacy.

Will courts ever accept damages based on the intrinsic value of privacy? If so, how can we measure this intrinsic value?

To the first question, there are precedents for awarding damages for lost intrinsic value, most notably from cases related to environmental disasters. In those cases plaintiffs (usually state and federal agencies) have sought and won damages based on “existence value” or “passive use value.” This is the value that individuals place on the knowledge that a natural resource exists in a pristine state, even if they never directly make use of that resource.

This theory of damages rose to prominence with the 1989 Exxon Valdez oil spill in Alaska. Although there was relatively little direct economic harm to individuals from the spill, estimates of damages based on lost existence value were huge — one study[7] calculated the aggregate lost existence value to be $2.8 billion (Exxon eventually settled for $507 million). Lost environmental existence value has been explicitly ruled to be compensable[8], and now calculations of these intrinsic values are common in discussions of damages in environmental cases.

It is easy to draw parallels between the intrinsic value of the environment and the intrinsic value of privacy. In the privacy setting, an individual’s “existence value” comes from the knowledge that their personal data is secure and untouched by unauthorized third parties, and damages arise when the individual discovers this is no longer true, even if there is no direct financial harm from the data sharing or data breach.

We are aware of two possible approaches to measuring the intrinsic value of privacy: contingent valuation (CV) and conjoint analysis.[9]

CV studies are based on sets of survey questions that ask respondents whether they would be willing to pay specific amounts to preserve something of value to them. For instance, in the Exxon Valdez case survey respondents were asked about their willingness to pay for a safety program that would prevent a similar spill in the future. One could imagine also applying CV studies to privacy cases — for instance, in a data breach case survey respondents could be asked about their willingness to pay for additional security features to prevent data breaches.

However, CV methods are controversial, not least because they often produce implausibly large estimates of damages.[10] More importantly, CV studies are “stated preference” studies, designed for the study of public goods where there are no markets in which consumers can reveal their valuations. Most economists regard these studies as weaker than “revealed preference” studies, where the valuations of consumers are revealed through the tradeoffs they make in the marketplace. Since most privacy cases arise from market transactions involving private goods, the best approach to estimating the intrinsic value of privacy is to study how consumers approach tradeoffs between privacy and cost. Conjoint analysis is ideally suited to this task.
Conjoint analysis is a survey-based technique often used in market research to determine the relative values consumers place on the various features of a good or service, and has been used as the basis for calculating classwide damages in previous cases. To estimate the intrinsic value of privacy in a conjoint analysis, we can simply treat a privacy policy or data security measures as another feature of the good or service in question.

As an example of this approach, in our own work[11] we estimated the value of privacy for customers of streaming video services. We designed a survey that presented a series of choices from among different hypothetical streaming video services. Each of these hypothetical streaming video services had a monthly cost, as well as a variety of features (the number of movies available, how quickly content became available after appearing in the theaters, etc.). Among these features was a privacy policy — each of the hypothetical services might share no information with third parties, share usage information (such as movies watched), or share both usage and personally identifying information (such as email addresses).

By studying the choices our survey respondents made from among these services, we were able to estimate the value they placed on privacy. We found that respondents were willing to pay an average monthly premium of about $6 to avoid sharing their usage and personally identifying information.

The willingness to pay estimates from a conjoint analysis could then be used to estimate damages, with the actual calculation depending on the definition of the “but-for” situation where customer privacy was not violated.[12]

Techniques for placing a value on privacy are still being developed, and there are many issues still to be addressed, such as differences in the intrinsic value of privacy across different types of data (e.g., movie rentals vs. health information). Despite this, conjoint analysis studies such as our study described above provide an accepted and scientifically valid framework for estimating damages based on the intrinsic value of privacy, and will become increasingly common should this become an accepted part of data sharing or data breach cases.

—By Garrett Glasgow and Sarah Butler, NERA Economic Consulting

Garrett Glasgow, Ph.D., is a senior consultant and Sarah Butler is a vice president in NERA’s San Francisco office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[5] Among other things, the complaint claims as damages the “[Loss of value resulting from] the difference between the price Plaintiff and the Class paid in reliance upon Defendant’s duty/promise to
secure its members’ [personally identifying and personal health information], and the actual services — devoid of proper protection mechanisms — rendered by Defendant.” Juliano v. Anthem, Complaint, 5 February 2015.


[9] Some plaintiffs have claimed damages based on the intrinsic value of a customer’s personal information. For instance, the plaintiffs in the Zappos.com case estimated the intrinsic value of their personal information through a study of black market prices for personal records. However, this is not a measure of the intrinsic value of privacy – there is a distinction between the value of a customer’s personal information to a third party and the value the customer places on his or her own privacy.

[10] In environmental cases, many survey respondents appear to treat the willingness to pay survey questions as an opportunity to express their anger or dismay related to the environmental damage by stating a large dollar figure, without regard to household budgets or the scale of the problem.


[12] For instance, if a company used the unauthorized sale of customer data to subsidize prices, this would lead to a different “but-for” scenario and a lower estimate of damages than if the company sold the data and kept the profits.

All Content © 2003-2015, Portfolio Media, Inc.