Data Breach Harms—Bringing in the Courts, or Leaving Them Out?

Author : Tal Zarsky

Date : February 19, 2019

Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 **Tex. L. Rev.** 737 (2018).

As more and more of our daily activities and private lives shift to the digital realm, maintaining digital security has become a vital task. Private and public entities find themselves in the position of controlling vast amounts of personal information and therefore responsible for assuring such information does not find its way to unauthorized hands. In some cases, there are strong incentives to maintain high standards of digital security, as security breaches are a real pain. When reports on such breaches are made public, they generate reputation costs, lead to regulatory scrutiny and often call for substantial out-of-pocket expenses to fix. Unfortunately, however, the internal incentives for maintaining high security standards are often insufficient motivators. In such cases, the security measures taken are unfitting, outdated and generally unacceptable. These are the instances where legal intervention is required.

There are several possible regulatory strategies to try and improve digital security standards. One option calls for greater transparency regarding breaches that led to personal data leakage and other negative outcomes. Another option calls upon the government to set data security standards and enforce them, at least in key sectors (more on these two options and their limitations, below). Yet an additional central form of legal intervention is through private litigation and the court system. However, key doctrinal hurdles in the United States currently make it extremely difficult to sue for damages resulting from security breaches. In an important recent paper, Daniel Solove and Danielle Citron, two prominent privacy scholars, explain what these hurdles are, how to overcome them, and why such doctrinal changes are essential.

As the authors explain, the key to many of the challenges of data security litigation is the concept of "*harm*", or lack thereof. A finding of actual, tangible harm is crucial for establishing standing, which requires demonstrating an injury that is both concrete and actual (or at least imminent). Without standing, the case is thrown out immediately without additional consideration. Additionally, tort-based claims (as opposed to some property-based claims) require a showing of harm. And when examining data security claims, courts require tangible damages to prove harm. Security-related harms are often considered intangible. Therefore, many data security-related lawsuits are either immediately blocked or ultimately fail.

The complex issue of harm, standing and data security/privacy has been recently addressed by the U.S. Supreme Court in *Clapper v. Amnesty International USA* (where the Court generally rejected "hypothetical" injuries as sufficient to establish standing) and more recently in *Spokeo Inc. v. Robins*. In this latter case (addressing the standing and the FCRA) the Court has, at least in principle, recognized that intangible harms could be considered as sufficiently "concrete" if they generate the risk of real harm, and thus provide plaintiffs with standing. Furthermore, an additional case—*Frank v. Gaos*—is currently before the Supreme Court. While this latter case focuses on the practice of *cy pres* settlements in class actions, it appears to incidentally yet again raise questions related to standing, harms and digital security/privacy—this time with regard to referrer headers.

In response to the noted challenges security litigation faces, the authors call upon courts to enter the 21st century and accept changes to the doctrines governing the establishment of harm. They convincingly show that security breaches indeed create both harm and anxiety—but of somewhat different form. In fact, they assert, some courts have already begun to recognize harms resulting from data security breaches. For instance, courts have found that a "mere" increased risk of identity theft constitutes actual harm (even before such theft has occurred) when the data has made

its way to the hands of cyber-criminals. The authors prod courts to push further in their expansion of the harm concept in the digital age. They note three major forms of injury which should be recognized in this context: (1) the risk of future injury, (2) the fact that individuals at risk must take costly (in time and money) preventive measure to protect against future injury, and (3) enhanced anxiety.

To make this innovative argument, the authors explain that data security breaches create unique concerns which justify the expansion of the concept of harm. For instance, they explain that damages (which might prove substantial) resulting from data breaches could be delayed. Therefore, recognizing harm at an earlier stage is essential. In addition, they argue that the risk of security harms might deter individuals from engaging in important and efficiency-enhancing activities such as seeking new employment opportunities and purchasing a new home. This is yet another strong argument for immediately creating a cause of action through the recognition of harm.

Judges are usually cautious about creating new rules, especially in common law systems. Yet the authors explain that in other legal contexts, such as medical malpractice, similar forms of intangible harms have already been recognized. They refer to cases based on actions that increased a chance of illness or decreased the chance of recovery. These have been recognized as actual harms—instances somewhat analogous to personal data leakage and the harms that might follow.

Yet broadening the notion of data "harm" has some downsides, such as attempts to "cheat" and manipulate by plaintiffs. This is because intangible harms are easier to fake or fabricate, and because the definition of intangible harm might be too open-ended. In addition, broadening the notion of harm might lead to confusion for the courts. To mitigate some of these concerns, the authors introduce several criteria to assist courts in establishing and assessing harm in this unique context. These include the likelihood and magnitude of future injury as well as the mitigating and preventive measures those holding the data have taken.

Finally, the authors confront some broader policy questions pertaining to their innovative recommendations. Litigation, of course, is not the only way to try and overcome the problems of insecure digital systems. It probably isn't even the best way to do so. I have argued elsewhere that courts are often an inadequate venue for promoting cybersecurity objectives. Litigation is costly to all parties. It also might stifle innovation and end up merely enriching the parties' lawyers. In addition, judges usually lack the proper expertise to decide on these issues. Furthermore, in this context, ex post court rulings are an insufficient motivator to ensure that proper security measures will be set in place ex ante, given the issue's complexity and the difficulties of proving causation (i.e. the linkage between the firm's actions or omissions and the damages that follow at a later time).

The authors would probably agree with these assertions and indeed acknowledge most of them in their discussion. Nonetheless, they argue that other regulatory alternatives such as breach notification requirements and regulatory enforcement suffer from flaws as well. This is, no doubt, true. Breach notifications might generate insufficient incentives for data collectors to minimize future breaches, as users might be unable or unwilling to voice or act on their disappointment with the flawed security measures adopted. And data security regulatory enforcement might suffer from the usual shortcomings of governmental enforcement—it being too minimal, not up to date and at times subject to capture. Litigation, the authors argue, could fill a crucial void when other options fail. They state that "data-breach harms should not be singled out" as problematic relative to other kinds of legal harms. Therefore, courts should have the option to find that harm has been caused and thus additional legal actions must be taken when they have good reasons to do so.

Using doctrinal barriers (such as refraining from acknowledging new forms of harm) to block off specific legal remedies is an indirect and somewhat awkward strategy. Yet it is also an acceptable measure to achieve overall policy goals. The authors convincingly argue that (all) judges should have the power to decide on a case's merits, yet by doing so the authors inject uncertainty into the already risky business of data security. If this proposal would be ultimately accepted, let us hope that judges use this power responsibly. If Solove and Citron's proposals are adopted, judges should look beyond the hardship of those victimized by data breaches and consider the overall interests of the digital

ecosystem before delivering their judgement in digital security cases.

Cite as: Tal Zarsky, *Data Breach Harms—Bringing in the Courts, or Leaving Them Out?*, JOTWELL (February 19, 2019) (reviewing Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 **Tex. L. Rev.** 737 (2018)), https://cyber.jotwell.com/data-breach-harms-bringing-in-the-courts-or-leaving-them-out/.