Insight

What Exactly Constitutes a Privacy Harm?

WILL RINEHART | JUNE 1, 2016

The Supreme Court's recent ruling on *Spokeo v Robbins* resurrected the fundamental question of privacy regulation. What exactly constitutes privacy harm? While the highest court didn't go far in answering this question, in the coming years, actions from the courts, the Federal Trade Commission (FTC) and Congress will likely lay down the contours of privacy harm. In doing so, the limits of privacy law will be set, thus determining the scope of innovation in high tech.

The *Spokeo* case stems from a dispute over an online profile by Spokeo, a company that aggregates data on people from both online and offline sources. Thomas Robbins sued the company claiming they included inaccurate information in his online profile, which violated the Fair Credit Reporting Act (FCRA). Spokeo had indicated that Robbins was wealthy, married, in his 50s, and worked in a technical field. Because none of these characteristics are correct, Robbins claimed that it limited his ability to get a job. The district court dismissed Robbins case, claiming that he could not show any actual harm from Spokeo's inaccurate information, and thus didn't have standing. There was logic to this ruling. Robbins filed a no-injury class action suit, alleging that the harm came not from some particular injury, but because Spokeo had violated the FCRA statute. After an appeal, the case found itself at the Supreme Court.

Justice Alito wrote the 6-2 decision which instructed the lower court to again review the issue of standing. As the opinion explained, Robbins needs to have an "injury in fact" that is both "concrete and particularized." To bring a class action suit, there has to be a concrete injury even if there is a statutory violation. The Court further noted that a concrete injury isn't necessarily synonymous with a tangible one. Indeed, "intangible injuries can nevertheless be concrete." Yet, the Supreme Court didn't go so far as to define the boundaries of these concrete, yet intangible, harms.

The problem of defining harm is one of the most important in privacy law, and so the tangible and intangible distinction matters. For example, let's say there was a data breach and bank information from countless consumers was leaked. Eventually, these details could land in the hands of a criminal, who charged credit cards to make purchases. In this case, it is fairly easy to show harm in the replacement costs and headache for consumers.

The 2013 Target data breach is a prominent example of this. All told, the breach cost the retailer $252 million. In the weeks following the initial reports, sales slipped 5.3 percent and profits dropped 46 percent. Consumers wary of Target's reputation stayed away from the retailer, leading to a 7 percent -8 percent decline in traffic.

But what happens if the data is leaked, but isn't used for nefarious purposes? Is it still a privacy harm? The courts are split on this question. For the First and Third Circuits, these kinds of hypothetical harms to identity theft aren't actionable, while the Seventh and Ninth Circuits have recognized allegations of future harm. The FTC, the agency primarily tasked with privacy and data security, recently lost a case in front of their own administrative law judge, in part because of this issue. As the judge noted, the FTC's enabling statute "requires proof of something more than an unspecified and hypothetical 'risk' of future harm," yet the agency was unable to supply them.

Privacy harms are often difficult to ascertain because privacy itself is a nebulous term. While the context of the interaction is important, personal preferences play a key role in determining those actions that people cite as violations. But consumers have shown a propensity to give up information for very little in return. As one seminal study noted, "most subjects happily accepted to sell their personal information even for just 25 cents." What one gathers from reading these reports is that people will often state a preference for privacy, and yet will be very willing to trade information for little to nothing. These harms seem to be relatively costless.

How the courts decide will in turn create a legal line in the sand, limiting the use of certain kinds of data. Because data is the asset on which companies are built, data use limitations translate into limits to innovation. The proper way to understand privacy laws is to understand them in balance with costs to innovation, which is shown time and again. In the US, children's web sites

While *Spokeo* was anticipated to be an important case, the decision was narrow. The Court provided little guidance for the lower courts, leaving unanswered key questions in privacy law. What still remains to be decided could determine the future direction of innovation in the U.S. For those that care about continued development in the high tech space, ensuring the courts don't cast too wide a net will be the best policy.