COMMENTARY

Extending Privacy Harms Toward a Non-Economic Perspective

Authors _ Christopher Muhawe (cmuhawe2@illinois.edu), University of Illinois, College of Law, and **Masooda Bashir** (mnb@illinois.edu), University of Illinois at Urbana Champaign, School of Information Sciences

Addressing data breach harms has become a great challenge in the administration of privacy law in the United States. Several data breach cases have been dismissed by US courts because the victims cannot prove cognizable harm. The current US legal system emphasizes that data breach victims must prove that they have suffered an "injury in fact," which means that the injury suffered must be concrete and particularized. Data breach harms are futuristic and hard-to-quantify, reasons for which they may not fit in the "injury in fact" requirement. Furthermore, victims of data violations have attempted to plead economic loss to prove the harm suffered, but with no success. This article suggests a new approach that aims at addressing privacy harms without necessarily proving economically quantifiable harm.

With recent advancements in communication technologies, the digital realm has dramatically changed our daily lives and how we communicate with each other. Following the COVID-19 pandemic stay-at-home orders, reliance on digital platforms and communication has reached an all-time high and has influenced most human activities throughout the world. In the developed and privileged parts of the world, we started attending virtual classes, virtual doctors' visits, virtual weddings, and virtual funerals in the comfort of our homes (Kessel et al. 2021). The virtual world has seemingly become a new normal, and this has resulted in a fusion of our private and professional lives.

This dependence on digital realms also means that both private and public organizations collect massive amounts of personal data, and this has presented both opportunities and challenges (Sun et al. 2020). The virtual world thrives on data as its fuel (Luca and Bazerman 2020). Private and public organizations have become strongrooms of massive sensitive private data, including names, dates of birth, social security numbers, religious affiliations,

political party affiliations, banking histories, location data, shopping histories, home addresses—the list is endless (Matsakis 2019). As the appetite to collect has grown, data misuse and data breaches have also increased (Ponemon Institute 2020). Examples of data violations are unauthorized access to an individual's electronic health records, stolen social security numbers, and misuses of addresses, biometric data, and phone numbers (Matsakis 2019).

However, the majority of data misuse and data breach legal cases in the United States have been unsuccessful (Citron and Solove 2021) or dismissed under the current legal system, as claimants have failed to prove injury resulting from privacy violations. Data breach cases are often dismissed for lack of "injury in fact" sufficient to support a finding of cognizable harms (Citron 2010; 2016).

Faced with the challenge of satisfying the "injury-in-fact" requirement, US courts have attempted to use the traditional economic injury perspective to look at privacy harms. Litigants of privacy harms have often found themselves trying to fabricate harms to prove that they have suffered an economic loss (Fisher 2013). This approach has yielded no positive results. Most victims of privacy violations do not experience clear and instant pecuniary or reputational harms, which makes it difficult to prove the economic loss requirement (Citron 2010). The traditional economic perspective (Martecchni 2016) under the law denies victims of privacy violations a chance of recovering damages as the harms mostly attach in the future and are hard to quantify.

In addition, the economic loss rule provides that a plaintiff cannot recover in court without demonstrating a personal or property injury to which such losses attach (*Four Directions Air, Inc. v. United States* 2007). With the nature of privacy harms, this hurdle is insurmountable to overcome as is. We believe that the current legal approach in addressing privacy harms is inadequate and narrow, as well as predisposed to further abstraction given the unique nature of privacy violations.

Furthermore, this approach is devoid of the realities that are presented by the negative and long-lasting effects of a privacy violation (Johnson 2005). Hence, viewing privacy harms from a purely economic perspective negates the fact that data breaches may result in harms that are difficult to measure and quantify. It also runs counter to the functions of individual privacy, which are the promotion of liberty, selfhood, autonomy; the promotion of human social relations; and the furtherance of the existence of a free society (Gavison 1980). At the same time, the functions of privacy influence self-determination, and there is no economic value that can be placed on self-determination.

Therefore we propose that the US law should evolve to address these computer-enabled harms without necessarily requiring victims to prove the traditional economic harm. Our proposal recommends that data holders stand in a privileged position and should be vested with a duty to take utmost care in securing data (Solove and Citron 2018).

Breach of this duty should be addressed as a privacy violation without necessarily proving an economically quantifiable injury to the victims of data violations. We premise this approach on the fact that private and public entities stand in a privileged position of technical know-how and with vast resources of collecting, storing, and processing data for which they should provide adequate security (Kesan and Hayes 2019). In addition, these entities have access to our most personal and private information, and therefore an expectation of good stewardship of such data would be a socially responsible duty (Rosenbaum 2010). Thus we propose that the law should evolve to embrace a new approach with a view of holding the data-steward entities responsible for the utmost protection of the data subjects' data. To this extent, a cause of action/claim would be presented as

1. The data holder (defendant) has a duty to protect data in their custody.
2. If this duty has been violated by the data holder resulting in a violation of the data subject's privacy; then
3. the data holder is liable for neglect of their duty, and the defendant need not prove any economic harm resulting from a breach of this duty.

Otherwise, we will have increasing instances where data collectors will intentionally or negligently use deficient data protection measures that expose data subjects' information to potential breaches, yet the data collectors are not held accountable. For example, in the case of *FTC v. Wyndham Worldwide Corp.* (2015), Wyndham failed on the basics of protecting clients' data when it stored its customers' credit card information in clear readable text rather than using encryption and used default user names and easily guessed passwords for access to servers, among other failures. This resulted in a data breach that aided access to more than 619,000 customer accounts' unencrypted data.

We propose that the US courts should recognize a legal duty to adequately secure the data subjects' information,

and failure to do so should translate into a violation of the data subjects' privacy. This approach will enable courts to shift from a position of addressing data harms from only an economic perspective, because not all privacy harms can be expressed in economic terms.

References

Citron, Danielle Keats. 2010. "Mainstreaming Privacy Torts Recommended Citation." *California Law Review* 98, no. 6: 1805-52.

———. 2016. "The Privacy Policymaking of State Attorneys General." *Notre Dame Law Review* 92, no. 2: 747-815.

Citron, Danielle Keats, and Daniel J. Solove. 2018. "Risk and Anxiety: A Theory of Data Breach Harms." *Texas Law Review* 96, no. 4: 737-86.

Citron, Danielle Keats, and Daniel J. Solove. 2021. "Privacy Harms." GWU Legal Research Studies Research Paper No. 2021. https://ssrn.com/abstract=3782222.

Fisher, John A. 2013. "Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach." William & Mary Law School Scholarship Repository. https://scholarship.law.wm.edu/wmblr/vol4/iss1/7/.

Four Directions Air Inc. v. U.S. 2007. 5:06-CV-283.

FTC v. Wyndham Worldwide Corp. 2015. 799 F.3d 236.

Gavison, Ruth. 1980. "Privacy and the Limits of Law." *Yale Law Journal* 89, no. 3: 421-71.

Johnson, Vincent R. 2005. "Cybersecurity, Identity Theft, and the Limits of Tort Liability." http://www.key.com/html/A-11.2.1.html.

Kesan, J. P., and C. M. Hayes. 2018. "Liability for Data Injuries." *Journal of Illinois Law Review* 2019: 295-363.

Kessel, Patrick van, Chris Baronvaski, Alissa Scheller, and Aaron Smith. 2021. "How the COVID-19 Pandemic Has Changed Americans' Personal Lives. Pew Research Center." Pew Research Center, March 8. https://www.pewresearch.org/2021/03/05/in-their-own-words-americans-describe-the-struggles-and-silver-linings-of-the-covid-19-pandemic/.

Luca, Michael, and Bazerman Max H. 2021. *The Power of Experiments: Decision Making in a Data-Driven World*. Cambridge, MA: The MIT Press.

Martecchini, Thomas. 2016. "A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After Clapper v. Amnesty International USA." *Michigan Law Review* 114, no. 8: 1472-96.

Matsakis, Louise. 2019. "The WIRED Guide to Your Personal Data (and Who Is Using It)." *Wired*. https://www.wired.com/story/wired-guide-personal-data-collection/.

Nissenbaum, Helen. 2011. "A Contextual Approach to Privacy Online." *Journal of American Academy of Arts & Sciences* 140, no. 4: 32-48.

Ponemon Institute. 2020. "Cost of a Data Breach Report 2020 | IBM." https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

Rosenbaum, Sara. 2010. "Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access." *Health Services Research* 45, no. 5: 1442–55. https://doi.org/10.1111/j.1475-6773.2010.01140.x.

Sun, Huidong, Mustafa Raza Rabbani, Muhammad Safdar Sial, Siming Yu, José António Filipe, and Jacob Cherian. 2020. "Identifying Big Data's Opportunities, Challenges, and Implications in Finance." *Mathematics* 8, no. 10: 1738. https://doi.org/10.3390/math8101738.