

CARDOZO LAW REVIEW  
*de•novo*

INTRODUCTION

DATA BREACHES: MOVING FORWARD,  
PRACTICALLY

*Cindy E. Zuniga*<sup>†</sup>

In 2013, approximately 70 million Target consumers were victims of a major data breach in which hackers stole personal information that included names, mailing addresses, credit and debit card information, phone numbers, and email addresses.<sup>1</sup> Most recently, the “Sony Hack” revealed confidential information on some of the company’s top executives and Hollywood celebrities through data that included personal emails and salary information.<sup>2</sup> Unfortunately, these incidents reveal a snapshot of data breach occurrences in the past decade.<sup>3</sup>

*Cardozo Law Review de•novo*’s online symposium: Data Breaches: Moving Forward, Practically focuses on proactive steps that policymakers, regulators, the judiciary, and businesses can take to address the array of issues arising from data breaches. The online symposium features articles from Lauren Henry, Adam Lamparello,

---

<sup>†</sup> Head *de•novo* Editor, *Cardozo Law Review*, Volume 36. J.D. Candidate (June 2015), Benjamin N. Cardozo School of Law; B.S., Stony Brook University, 2012. I would like to thank the authors for their wonderful contributions and dedication to the symposium. I would also like to thank our *de•novo* Editor, Ken Contrata, for his endless support throughout this year.

<sup>1</sup> See *Data Breach FAQ*, TARGET, <https://corporate.target.com/about/shopping-experience/payment-card-issue-faq> (last visited May 19, 2015).

<sup>2</sup> See Rachel Emma Silverman & Ben Fritz, *Data Breach Sets Off Upheaval at Sony Pictures: Morale Plummets as Some of Studio’s Systems Remain Offline*, WALL ST. J. (Dec. 4, 2014, 10:14AM), <http://www.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799>.

<sup>3</sup> For a list of the greatest data breaches in the past decade, see Elizabeth Palermo, *10 Worst Data Breaches of All Time*, TOM’S GUIDE (Feb. 6, 2015, 7:00AM), <http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html>.

Peter Yu, and David Thaw.

Lauren Henry begins the discussion by delineating the relationship between information privacy and data security. Although the author admits that the two fields are related, she cautions against treating the two the same, as they have different objectives that can, at times, put the fields in opposition to one another. Ms. Henry provides readers with her observations on the implications of such an analysis.

Adam Lamparello narrows his focus on consumers and their ability to recover damages associated with online data breaches. The author criticizes the standing, third-party, and reasonable expectation of privacy doctrines as inadequately safeguarding privacy rights. Professor Lamparello argues that judiciary modifications on these doctrines are necessary to fully compensate consumers for harms resulting from online data breaches.

Peter Yu turns our attention to concerns stemming from abroad by examining the ongoing debate on China's intrusive efforts to steal trade secrets and propriety data from U.S. businesses. Professor Yu offers five suggestions on how to construct a more positive debate that will move us forward by helping identify ways to reduce online hacking and data breaches, while enhancing protection of trade secrets and propriety data.

Finally, David Thaw considers the function and effects of data breach notification regulatory regimes from the perspective of cybersecurity. Professor Thaw discusses a bifurcated notification regime that could be adopted at the federal level. Such a regime will serve the dual purpose of protecting consumers through breach notification while mitigating the potential risks of "over-notification."

In our ever-evolving digital landscape, data breaches and leaked personal information have increasingly become a lamentable fact of life. The symposium aims to serve as a platform for ideas targeted at preventing, dealing with, and curing the effects of data breaches. These articles provide practical suggestions that policymakers, regulators, the judiciary, and businesses should consider while addressing these concerns in our digital age.