CSAW Policy Competition Submission

Expanding FTC Authority to Seek Consumer Redress for Intangible Privacy Harms

By Austin Mooney, Katie Morehead, and Julian Flamant

I. Introduction

When it comes to negative externalities for improper data security, not all data is created equal. If financial data, such as credit card numbers, is stolen by hackers, this often has direct economic consequences, such as the draining of bank accounts through fraudulent purchases and transfers. Because these consequences can be quantified and calculated, they are largely internalized by private-sector actors due to their financial liability. For example, it is estimated that Target paid more than $110 million to banks settle various lawsuit brought against it following the 2013 breach of its payment card system.[1] By contrast, when the data that is stolen in a breach is not financial in nature, a challenge arises in determining how much compensation to award the consumer for their harms. Further, consumers have great difficulty getting into court with such cases in the first place: the lack of tangible economic consequences often leads to courts dismissing claims as a result of a failure to meet the constitutional burden of standing.[2] The lack of compensation for nonfinancial harms suffered has led to a negative externality which we seek to address through our policy proposal. Specifically, we propose that the Federal Trade Commission be given new authority to calculate the value to consumers of nonfinancial harms arising from data breaches and seek consumer redress. In the following pages, we define the

[1] Ahiza Garcia, Target Settles $39 Million Over Data Breach, CNN Money (Dec. 2, 2015, 5:48 pm), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

[2] *See* Robert D. Fram, Simon J. Frankel and Amanda C. Lynch, *Standing in Data Breach Cases: A Review of Recent Trends*, Bloomberg BNA (Nov. 9, 2015), http://www.bna.com/standing-data-breach-n57982063308/.

market failure caused by nonfinancial privacy harms, explain why the FTC is the best agency to address these harms, and sketch a legislative proposal that would endow the FTC with the ability to correct this market failure.

II. Nonfinancial Privacy Harms

While financial harms often arise as a consequence of data breaches, they do not represent the only type of harms that can be suffered as a result of a breach. Invasion of privacy and exposure of private information to the public are all harms that can occur during a data breach. As an example of nonfinancial harm, Ashley Madison, an adult dating website, was hacked in 2015, ultimately resulting in the email address and account details for thirty-two million of the site's members being exposed to the public.[3] The hackers claim their motivation behind the attack was not only due to the fact they morally opposed to Ashley Madison's mission of arranging affairs between married individuals, but also because the website kept user information they were paid to delete by privacy conscious users.[4] On the surface, exposure of one's email address and account information might not even reveal information that is not already public. However, the fact that the email addresses were linked to this specific website for affairs meant that the registered users were going to be labeled as adulterers by society. Additionally, since Ashley Madison did not remove the data when paid to do so by users, users that took care to protect their privacy were exposed. If that user wishes to sue Ashley Madison, they will have to list their names on the lawsuit, which only further exposes them to the

[3] Robert Hackett, What to know about the Ashley Madison Hack, Fortune (Aug. 26, 2015, 7:24 am), http://fortune.com/2015/08/26/ashley-madison-hack/.
[4] *Id.*

limelight.[5] The company does not suffer any harms beyond having to report the data breach to authorities. Instead the consumer bears all the costs of the harms.

Another example of consumers bearing the nonfinancial harms of a data breach involved insecure baby monitors. Hackers tapped into baby monitors in order to scare children or see what was going on inside the house. Companies such as TrendNet, which produced the cameras, failed to use security standards such as requiring passwords or encrypting the data being transferred.[6] Parents reported that their children were being screamed at through cameras and that the cameras were watching them move through the house.[7] Without the FTC enforcement action that took place, the consumers who were hacked would have had no way to recoup from their invasion of privacy and the company would not have suffered any harms, making it unlikely to encourage them to use better security in the future.

III. The Agency Approach to Addressing Externalities

Using administrative agencies to counteract negative externalities is far from a novel concept. For example, much of the Environmental Protection Agency's (EPA) regulatory authority is widely thought to be justified by the need for an agency to assess and counteract negative externalities caused by pollution.[8] The EPA uses its regulatory authority to increase the private cost of a company's consumption or production of pollution which in turn decreases the amount of pollution a company is willing to produce.[9] A similar approach should be taken in

[5] Robert Hackett, Ashely Madison Hacking Victims Face a Big Decision, Fortune, (Apr. 20, 2016, 8:51 pm), http://fortune.com/2016/04/20/ashley-madison-data-breach-lawsuit-names/.
[6] Federal Trade Commission, In the Matter of TrendNet, Inc, Docket No. C-4426, (Jan. 16, 2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.
[7] Kashmir Hill, Watch Out, New Parents - Internet-Connected Baby Monitors are Easy to Hack, Fusion, (Sept. 2, 2015), http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/.
[8] *See, e.g.*, David A. Westbrook, *Liberal Environmental Jurisprudence*, 27 U.C. Davis L. Rev. 619, 647-48 (1994).
[9] Robert Crandall, Pollution Controls, Library of Economics and Liberty, (2008) http://www.econlib.org/library/Enc/PollutionControls.html.

addressing nonfinancial harms caused by data breaches. The government should increase the cost of being exposed to a data breach so companies will be encouraged to take steps to mitigate potential breaches.

In the case of negative externalities caused by insufficient data security measures, we argue that the best agency to correct this problem is already in existence: the Federal Trade Commission (FTC). This is the case for two reasons: (1) the FTC has a long history and expertise in the field of privacy and data security and (2) the FTC's has economic and antitrust expertise that would easily transfer over to solving the problem of calculating the costs of nonfinancial data breaches.

A. The Federal Trade Commission as an Authority on Data Security

The FTC derives its expertise in the field of data security in large part through its extensive history of bringing enforcement actions against companies for violations Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices."[10] In terms of data security, the FTC has sued companies for both unfair and deceptive practices.[11] For example, a company's failure to follow the statements outlined in their privacy policies is considered a deceptive practice. Similarly, the FTC has found that certain data security practices are considered unfair regardless of what is in the company's privacy policy.[12]

i. Wyndham and LabMD

Two recent cases illustrate the FTC's authority in matters of data security: *FTC v. Wyndham* and LabMD, Inc. In *FTC v. Wyndham*, the FTC found that Wyndham had

[10] 15 U.S.C. § 45
[11] See generally Data Security, Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last accessed Sept. 30 2016).
[12] Daniel Solove & Paul Schwartz, Consumer Privacy and Data Protection 287 (2015).

unreasonably poor data security practices that resulted in three different breaches.[13] Wyndham first argued that the FTC lacked the authority to regulate cybersecurity practices. The court held that Wyndham received fair notice that there could be a potential application of the unfairness standard under Section 5 in regards to its data security practices.[14] The court also held that the FTC had proved that the lax data security practices Wyndham employed sufficiently met the "substantial injury" standard of the unfairness doctrine.[15] The Wyndham case affirmed the FTC's authority to prosecute cybersecurity violations under Section 5.

LabMD v. FTC further illustrates the FTC's expertise in this area.[16] LabMD is a medical testing company that the FTC believes failed to reasonably protect the security of their customers' personal data and medical information. In the first incident, billing records for over nine thousand consumers were found on a peer-to-peer file-sharing network and in the second incident sensitive consumer information was found in the hands of identity thieves.[17] In July of 2016, the FTC reversed the ALJ ruling and concluded that LabMD's Data Security practices were unreasonable and constitute an unfair or practice that violated Section 5.[18]

ii. Educational efforts

The FTC's expertise in data security is further evidenced by its extensive efforts to create business and consumer educational materials on the subject. For example, the FTC has released a document called "Start with Security" in an effort to provide companies with a straightforward

[13] First Amended Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PGR (D. Ariz. filed Aug. 9, 2012) http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.
[14] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 248 (3d Cir. 2015).
[15] Id. at 258.
[16] LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015).
[17] Id. at 1277.
[18] FTC, Commission Finds LabMD Liable for Unfair Data Security Practices, (July 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

guide on what bad security practices companies employed in past FTC cases and what companies can do to avoid making the same mistake.[19] The guide divides the cases up into ten main topics: start with security; control access to data sensibly; require secure passwords and authentication; store sensitive personal information securely and protect it during transmission; segment your network and monitor who's trying to get in and out; secure remote access to your network; apply sound security practices when developing new products; make sure your service providers implement reasonable security measures; put procedures in place to keep your security current and address vulnerabilities that may arise; and secure paper, physical media, and devices. [20] Under each topic the FTC explains how a past case fits into the category.

Since the FTC is the main regulator in this space, many companies look to them for guidance on how to create a reasonable security program.

B. The FTC's Economic Expertise

In addition to being the premier agency authority on data security, the FTC possesses extensive economic expertise that makes it an ideal candidate for calculating and counteracting negative externalities. First, the FTC was founded in 1914 as an antitrust agency, meaning that its economic expertise extends to its inception.[21] Secondly, the FTC has a Bureau of Economics, which "helps the FTC evaluate the economic impact of its actions by providing economic analysis for competition and consumer protection investigations and rulemakings, and analyzing the economic impact of government regulations on businesses and consumers."[22] Finally, the

[19] Federal Trade Commission, Start With Security: A Guide For Business 1 (2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[20] Id.
[21] Federal Trade Commission, About the FTC, (2016) https://www.ftc.gov/about-ftc.
[22] Federal Trade Commission, Bureau of Economics (2016), https://www.ftc.gov/about-ftc/bureaus-offices/bureau-economics

FTC has a history of conducting consumer surveys of the sort that would allow for precise calculation of the value of consumer harms.[23]

IV. Legislative Solution

For the foregoing reasons, the FTC is the ideal agency to be tasked with the administration of a program that corrects the market failures brought about by insufficient data security practices. The best way to task the FTC with this authority would be through new legislation. Our ideal legislative proposal has two basic provisions: (1) a mandate that the FTC direct its Bureau of Consumer Protection and Bureau of Economics to work in tandem to conduct economic analysis of the value of nonfinancial harms from data breaches and (2) authority to seek consumer redress against companies for breaches that result in such nonfinancial harms. The following sections sketch out these aspects of the proposed legislation.

A. Research Mandate

In order to properly internalized the costs borne by consumers as a result of data breaches, this cost must be calculated to a reasonable degree of certainty. Accordingly, the first part of our legislative solution directs the FTC to use its existing authority and expertise to conduct economic research into the costs of associated with the harms created by nonfinancial data security breaches. Although we do not purport to know the best method of conducting such research, a good starting place would be to commission willingness to pay (WTP) and willingness to accept (WTA) consumer surveys. Such surveys, which ask consumers to express their preferences with certain tradeoffs, are able to calculate approximate monetary values of

[23] See, e.g., Keith B. Anderson, Federal Trade Commission, Consumer Fraud in the United States, the Third FTC Survey (Staff Report April 2013), https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf.

otherwise unquantifiable goods.[24] Were the FTC to conduct such surveys with respect to consumer preferences for keeping their data secure, it could develop a schedule of monetary values consumers place in different types of data. From this schedule, the FTC could then calculate the cost of any given breach to consumers.

Naturally, consumer attitudes toward the loss of different types of data may change over time. Accordingly, built into our proposed research mandate would be a renewal clause that mandates that research be re-evaluated on a recurring basis. The specific timeframe for this renewal could be calculated based on existing data of changes in consumer preferences. In lieu of such calculation, a five-year timeframe seems reasonable.

B. Redress Authority

The legislation will vest the FTC with the authority to fine companies whose data security practices violate the statute. The FTC will then use the money to provide consumers with redress for the noneconomic harms they have suffered. The definition of noneconomic harms will be defined within the statute to exclude direct calculable financial harms but include harms such as invasion of privacy, exposure of private facts to the public and exposure of sensitive non-financial information such as healthcare data. The fines levied against the company will be calculated by the Bureau of Economics within the FTC, as explained under the research mandate. The redress will be distributed in the same way the FTC currently disburses the redress they receive.[25] The FTC would also be assigned a budget within the statute in order to help

[24] Trudy Cameron & Michelle James, Estimating Willingness to Pay from Survey Data: An Alternative Pre-Test-Market Evaluation Procedure, Journal of Marketing Research, 389 (Nov. 1987), https://www.jstor.org/stable/3151386?seq=1#page_scan_tab_contents.
[25] Federal Trade Commission, Recent FTC Cases Resulting in Refunds, (2016), https://www.ftc.gov/enforcement/cases-proceedings/refunds.

finance their ability to conduct the research necessary to levy the fines against the companies in violation of the act.