United States of America

Federal Trade Commission

Remarks at the FTC Informational Injury Workshop

Maureen K. Ohlhausen[1]
Acting Chairman, U.S. Federal Trade Commission

December 12, 2017

Thank you all for being here for today's workshop on informational injury. I'd like to thank all the staff who have worked so hard to make this workshop possible. A special thanks to Doug Smith and Dan Wood from the Bureau of Economics, and to Cora Han and Jacqueline Connor from the Bureau of Consumer Protection. The four of you exemplify the inter-bureau, cross-disciplinary cooperation that is a unique strength of the FTC and that is particularly important for complex topics like informational injury. To start with the fundamentals, informational injury is my term for the harms consumers may suffer from privacy and data security incidents. In a speech in September on "painting the privacy landscape" at the FTC, I described some of the types of injury to consumers that the FTC has encountered in its privacy and data security cases over the years.[2]

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.
[2] Maureen K. Ohlhausen, "Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases,"(Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

I also announced my three goals for this workshop. First, better identify the qualitatively different types of injury to consumers and businesses from privacy and data security incidents. Second, explore frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence. And third, better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information. My ultimate is goal is to use what we learn today to guide FTC case selection and policy work going forward.

Our discussions will explore the types of negative outcomes that arise from the unauthorized access or misuse of consumer data and consider factors in assessing consumers' informational injury. We will also examine business and consumer perspectives on the benefits, costs, and risks of collecting and sharing consumer information. Finally, we will grapple with how to measure informational injuries.

Before we get to those important discussions, I would like to touch briefly on the FTC's role in privacy and data security, and talk about why this workshop is both timely and important.

As I never tire of saying, the FTC is the primary U.S. enforcer of commercial privacy and data security obligations. We take that charge very seriously. We've brought more than 500 privacy and data security related cases, both online and off.[3] Under my leadership, this work has continued. Since this summer, we have announced six important privacy or data security cases: Uber, TaxSlayer, Lenovo, and three cases enforcing obligations under the EU-US Privacy Shield agreement.[4]

---

[3] Letter from Edith Ramirez, Chairwoman, Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers, and Gender Equality, European Commission, at 3 (Feb. 23, 2016), https://www.ftc.gov/system/files/documents/public_statements/927423/160229ftc_privacyshieldletter.pdf.

[4] *See* FTC Press Release, "Three Companies Agree to Settle FTC Charges They Falsely Claimed Participation in EU-US Privacy Shield Framework," Sept. 8, 2017, https://www.ftc.gov/news-events/press-releases/2017/09/three-

Our primary privacy and data security tool is case-by-case enforcement under Section 5 of the FTC Act to protect consumers from deceptive or unfair acts or practices. One significant benefit of this approach is that it limits the need for policymakers to predict future developments in the marketplace. This is especially important in the complex, fast changing technology industry and in areas such as privacy, where consumers have a wide range of evolving expectations and preferences. Case-by case enforcement focuses on real-world facts and specifically alleged behaviors and injuries. Each case integrates feedback on earlier cases from consumers, industry, advocates, and, importantly, the courts. This ongoing process recognizes that markets, consumer expectations, and consumer benefits and risks evolve with new technologies, and it protects consumers while allowing innovation to occur.

In addition to Section 5, we enforce rules under several specific statutes, such as Gramm Leach Bliley and the Children's Online Privacy Protection Act. And we offer copious amounts of consumer and business education on these topics.[5]

Given the FTC's past record, you may ask, "Why hold a workshop on informational injury now?" I've chosen to focus on consumer informational injury for two key reasons.

---

companies-agree-settle-ftc-charges-they-falsely-claimed; Lenovo, FTC File No. 152-3134 (2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc; TaxSlayer, LLC, FTC File No. 162-3063 (2017), https://www.ftc.gov/enforcement/cases-proceedings/162-3063/taxslayer; Uber Tech., Inc., FTC File No. 152-3054 (2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc.

[5] *See, e.g.*, FTC, Consumer Information, https://www.consumer.ftc.gov/ (last visited Dec. 12, 2017); FTC, Business Center, https://www.ftc.gov/tips-advice/business-center (last visited Dec. 12, 2017); FTC, IdentityTheft.gov, https://www.identitytheft.gov/ (last visited Dec. 12, 2017).

First, in making policy determinations, injury matters. Although the free market is a powerful institution for improving human welfare, consumers can and do suffer injury from some business practices. Government does the most good with the fewest unintended side effects when it focuses on addressing actual or likely substantial consumer injury instead of expending resources to prevent trivial or purely hypothetical injuries. We need to understand consumer injury to weigh effectively the benefits of intervention against its inevitable costs.

Thomas Lenard, in his comment for the Technology Policy Institute, argued this point quite nicely, noting that privacy benefits us because it reduces harms from information misuse. But if there are no harms, then data use restrictions impose only costs and no benefits.[6]

Policymakers and enforcers, therefore, need to understand how, and how much, consumers are injured by various practices involving the collection, use, and disclosure of consumers' information. More precisely, we need a framework for principled and consistent analysis of consumer injury in the context of specific privacy and data security incidents. The FTC's Deception and Unfairness Statements provide such frameworks for thinking about consumer injury generally, but it is worth exploring more deeply how those frameworks apply in the specific setting of privacy and data security.[7]

Speaking of unfairness, the second reason I've chosen to focus on consumer injury is because it is a key part of our Section 5 unfairness standard. The focus of our discussion today is on defining consumer informational injury as a descriptive and economic matter. But I hope that

[6] Comments of Thomas Lenard, Technology Policy Institute at 2, (Oct. 26, 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/10/00008-141502.pdf.

[7] *See Fed. Trade Comm'n*, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction, 104 F.T.C. 1070, 1071 (1984) (*appended to In re* Int'l Harvester Co., 104 F.T.C. 949 (1984)) https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; *Fed. Trade Comm'n*, Policy Statement on Deception (*appended to In re* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

what we learn can help guide the future application of the unfairness standard's "substantial injury" prong.

As for why hold the workshop now, as I've mentioned, the FTC has been a very active privacy and data security enforcer. Many of our cases appropriately focus on the most egregious, low hanging fruit, where the harms were obvious the affected consumers, the FTC, and often to the defendants. For example, we have a series of cases such as LeapLabs, Sequoia One, and the recent Blue Global case that involve data providers who sold sensitive credit and payment information when they knew or should have known that the buying party was a fraudster who was going to misuse the information.[8] There are other types of cases involving direct financial loss for consumers. For example, the Wyndham data breaches allegedly resulted in identity theft and fraudulent charges to consumers.[9] In the recent TaxSlayer case, the breached tax return information allegedly resulted in fraudulent tax filings, delaying consumers' receipts of their tax refunds.[10]

[8] *Fed. Trade Comm'n v. Blue Global, LLC and Christopher Kay*, No. 2:17-cv-02117-ESW (D.Ariz. filed July 3, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3225/blue-global-christopher-kay; *Fed. Trade Comm'n v. LeapLab LLC*, No. CV-14-02750-PHX-NVW (D. Ariz. filed Dec. 23, 2014), https://www.ftc.gov/enforcement/cases-proceedings/142-3192-x150060/sitesearch-corporation-doing-business-leaplab; *Fed. Trade Comm'n v. Sequoia One, LLC*, No. 2:15-cv-01512-JCM-CWH (D. Nev. Filed Aug. 7, 2015), https://www.ftc.gov/enforcement/cases-proceedings/132-3253-x150055/sequoia-one-llc.

[9] *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-SPL (D. Ariz. filed June 26, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf..

[10] TaxSlayer, LLC, FTC File No. 162-3063 (2017), https://www.ftc.gov/enforcement/cases-proceedings/162-3063/taxslayer.

But as technology and business models continue to evolve, we have and are likely to continue to face more challenging scenarios that involve harms other than financial loss. For example, we took action against Accusearch for selling illegally-obtained personal telephone records of individuals, where we had evidence that stalkers and abusive former spouses used this information to surveil and harass individuals.[11] We also brought a case against the operator of a revenge porn website whose posting of highly sensitive intimate photos and personal information generated threats to and other harassment of victims.[12] Consider also the news reports of at least one suicide associated with the data breach at infidelity-promoting website Ashley Madison.[13]

A strong framework for assessing consumer injury in such cases will serve two purposes. First, it will help us think critically as we monitor new technologies and data uses for potential consumer injury. Second, it will help establish criteria by which we can judge if privacy and data security enforcement is the proper tool to address a practice, or if other mechanisms, perhaps even other agencies, institutions, or laws would be better equipped to address any particular negative outcome.

[11] *Fed. Trade Comm'n v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009), https://www.ftc.gov/enforcement/cases-proceedings/052-3126/accusearch-inc-dba-abikacom-jay-patel.

[12] Craig Brittain, FTC File No. 132-3120 (2015), (unfairly and deceptively acquired and posted intimate images of women, then referred them to another website he controlled, where they were told they could have the pictures removed if they paid hundreds of dollars), https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter.

[13] Laurie Segall, *Pastor Outed on Ashley Madison commits Suicide*, CNNMoney (Sept. 8, 2015), http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/index.html.

I believe our discussion today will help ensure we have such a framework. First, we need to examine more thoroughly the range of injuries that can occur from privacy and data security incidents. We're generally familiar with the direct financial injuries from identity theft, for example. We've also seen examples of unwarranted health and safety risk, and intrusion into seclusion. Our first panel today will talk about the different kinds of injuries suffered by consumers because of privacy incidents and data security breaches.

Second, we need to understand the key factors that matter in assessing injury from privacy and data security violations. Some obvious ones are the type of data involved, the magnitude of harm, and the distribution of injury. But what else? And are the same factors relevant in both the privacy and data security contexts? What is the relationship between risk and injury? Finally, when is FTC intervention appropriate? Our second panel will tackle these issues.

Third, we can benefit from learning about how companies weigh the potential benefits and costs of collecting and using information, and how this affects the decisions they make about protecting or restricting such information. Similarly, how do consumers weigh the benefits and costs of sharing information? Our third panel will dig into these issues.

Finally, we seek a better understanding of how to quantify consumer informational injury. There's an old saying, often attributed to management expert Peter Drucker: "What gets measured gets managed. If we want to manage privacy and data security injuries, we need to be able to measure them. Our fourth panel will discuss the challenges of quantifying informational injury and how we can tackle those challenges.

At the end of the day, Andrew Stivers, Deputy Director of our Bureau of Economics, who has already done some valuable work on these issues, will provide closing remarks.

This workshop is the next step in an ongoing conversation about consumer informational injury and how we can address it effectively, both here at the FTC and in the marketplace. This is going to be a fascinating discussion, and I again thank all of you for joining us.