United States of America

Federal Trade Commission

Painting the Privacy Landscape:
Informational Injury in FTC Privacy and Data Security Cases

Maureen K. Ohlhausen[1]

September 19, 2017

Thank you to the Federal Communications Bar Association for hosting this luncheon. I am really looking forward to the discussion with Julie. I expect we will talk about a number of different topics that relate to FTC and FCC matters. But first, as the chairman of the primary federal consumer protection agency, a few thoughts on consumer privacy.

I want you to imagine that each FTC privacy or data security case is a different dot of paint in a pointillist painting of privacy law. We often examine each case or dot in detail and isolation. But today, I want us to step back and take in the wider landscape so we can identify important patterns. Specifically, I will discuss what the painting shows us about "informational injury," which is my name for the various types of consumer injury addressed in our privacy and data security cases.

The canvas for this painting is, of course, the FTC's legal framework, so I'll begin there. Then, I'll identify five patterns of injury, with example cases from each. Next, I will highlight important remaining questions and announce an FTC workshop to discuss those questions.

First, the canvas. 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

[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. I would like to thank Neil Chilson for his important contributions to this speech.

brought more than 500 privacy and data security related cases, both online and off. We continue to be active under my leadership. In fact, in just the past month we've announced six important privacy or data security cases: Uber, TaxSlayer, Lenovo, and three cases enforcing obligations under the EU-US Privacy Shield agreement.[2]

The FTC takes a case-by-case law enforcement approach to protecting consumers' privacy and data security. We also enforce rules under a number of 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. (As a quick aside, let me tout our Division of Consumer and Business Education's efforts in the wake of the Equifax data breach announcement. Their quick, helpful advice to consumers made the FTC the most visited federal government website last week.)

Our primary privacy and data security tool is enforcement under our Section 5 authority to protect consumers from deceptive or unfair acts or practices. This approach has worked very well. One benefit is that it limits the need for policymakers to predict the future. This is especially important in the complex, fast changing technology industry and in areas such as privacy where consumers have disparate and evolving expectations and preferences. Case-by-case enforcement focuses on real-world facts and specifically alleged behaviors and injuries. As such, each case integrates feedback on earlier cases from advocates, the marketplace and, importantly, the courts. This ongoing process preserves companies' freedom to innovate with data use. And it can adapt to new technologies and new causes of injury.

---

[2] *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-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.

As the FTC has applied unfairness and deception authority to the facts in each privacy or data security case, it has developed a body of decisions. Think again of a painting, but one that is still being painted. Although one might disagree with a specific position in any one case, over time, patterns emerge, with some principles quite established and others newer and being tested. This process isn't flawless, but it is functional, and its emergent, adaptive nature matches the dynamism of the marketplace.

But, as with any emergent process, we can benefit from stepping back from the canvas to assess the whole picture. Such perspective helps us see patterns and deviations from those patterns. It allows us to distill lessons. And it can help identify areas that could benefit from additional thinking and exploration.

So let's step back and take in the bigger picture. Not of the entire scope of privacy law – this is a luncheon, after all, not a weeklong retreat. Let's focus on one specific aspect of FTC privacy and data security cases: consumer injury.

I've chosen to focus on consumer injury for a very pragmatic reason. Not only is consumer injury part of our Section 5 unfairness standard, it is just plain good policy. Government does the most good with the fewest unintended side effects when it focuses on stopping substantial consumer injury instead of expending resources to prevent hypothetical injuries. So understanding consumer injury in the context of privacy and data security is very important for the Commission.

To be clear, I am not questioning the fundamental structure of the FTC's approach, any more than a painter, by stepping back, is erasing his painting. Instead, I am seeking perspective that will help us apply that framework to future cases. And let me also emphasize that this is *not* a discussion of the *legal* question of what constitutes a "substantial injury" under our unfairness

standard. My topic today may inform the substantial injury question, but I am speaking more broadly. Indeed, many of the cases I will mention are deception cases, or allege both deception and unfairness. Substantial injury isn't a prong of the deception legal analysis, which focuses instead on materiality. However, regardless of the legal authority being used, the Commission, as a matter of good governance, should always consider consumer injury in determining what cases to pursue.

Therefore, I want to catalogue for you the types of privacy harms that the FTC has addressed in the past. Rather than try to deduce a definition of injury from first principles, I am taking an inductive approach by reviewing the canvas of our cases for patterns.

Type of Injury. In my review of our privacy and data security cases, I have identified at least five different types of consumer informational injury. Certain of these types are more common. Many of our cases involve multiple types of injury. Courts and FTC cases often emphasize *measurable* injuries from privacy and data security incidents, although other injuries may be present. And to be clear, not all of these types of injury, standing alone, would be sufficient to trigger liability under the FTC Act.

Deception Injury or Subverting Consumer Choice. We bring many of our privacy and data security cases under our deception authority, with a familiar and well-established theory of harm. In such cases, the complaint alleges that a company misled consumers through material claims about a product or services's privacy or security features. From an injury standpoint, a company's false promise to provide certain privacy or data security protections harms consumers like any false material promise about a product. The consumer is injured if he or she would have chosen differently but for the deceptive claim.[3] For example, consider our 2011 case against

[3] FTC Statement on Deception 6 (Oct. 14, 1984) (appended to *Cliffdale Assocs.*, 103 F.T.C. 110 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

Google. There we alleged that the company had represented to new Gmail users that it would only use their signup information to provide web-based email service. Among other things, the complaint alleged that the company instead used this signup information to populate its new social networking service without seeking additional permission.[4]

One can also think of deception as harming consumers by undermining their choices. If a company covertly subverts a consumer's privacy choice, it deprives that consumer of the benefit of that choice. For example, consider our case against digital advertising company Turn.[5] The FTC's complaint alleged that Turn deceived consumers by tracking them online and through their mobile applications, even after consumers took steps that they believed, and Turn claimed, would opt them out of such tracking.

Financial Injury. Putting aside the harm from deception, the most frequent type of injury in our privacy cases is financial. There are several sub-categories of financial injury. In some cases, fraudsters use consumers' private data to steal money from consumers. 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.[6] The consumers in those cases lost money to fraud that could have been prevented by the defendants, and the defendants may have indirectly profited from the fraud.

---

[4] Google, Inc., FTC File No. 102-3136 (2011), https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter.

[5] Turn, Inc., FTC File No. 152-3099 (2016), https://www.ftc.gov/enforcement/cases-proceedings/152-3099/turn-inc-matter.

[6] *FTC v. Blue Global, LLC,* No. 2:17-cv-02117 (D.Ariz. filed June 3, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3225/blue-global-christopher-kay; *FTC v. LeapLab LLC*, No. CV-14-02750 (D. Ariz. filed Dec. 22, 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 (D. Nev. Filed Aug. 7, 2015), https://www.ftc.gov/enforcement/cases-proceedings/132-3253-x150055/sequoia-one-llc.

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 for a large number of hotel customers.[7] And in the recent TaxSlayer case, the breached tax return information allegedly resulted in fraudulent tax filings, delaying consumers' receipts of their tax refunds.[8]

Sometimes the financial loss is less direct. For example, many of our data breach cases deprive consumers of their time or other valuable resources. Consumers who are victims of a data breach often spend significant amounts of time reporting identity theft, pursuing mitigation strategies, and dealing with other fall out.

In other cases, a data security problem results in the partial or complete loss of an otherwise useful asset. For example, some of our cases against adware vendors and similar actors alleged that they installed software that rendered the users' computers at least partially unusable.[9] Some of our Internet of Things cases are similar. For example, TRENDNet produced Internet-connected security cameras with a major security flaw that allowed anyone with the IP address to access the video feed.[10] Few people would knowingly purchase and use a device with such a flaw. Those who did purchase the devices were deprived of the product's use until a software update was deployed.

Health or Safety Injury. The third category is consumer health or safety injuries. Consider, for example, the news reports of at least one suicide associated with the data breach of

---

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

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

[9] *See* DirectRevenue, LLC, FTC File No. 052-3131 (2007), https://www.ftc.gov/enforcement/cases-proceedings/052-3131/directrevenue-llc-et-al; *FTC v. Zuccarini (d/b/a Cupcake Party)*, No. 01-CV-4854 (E.D. Pa. 2001), https://www.ftc.gov/enforcement/cases-proceedings/012-3095-x010063/zuccarini-john-dba-cupcake-party-et-al.

[10] TrendNet, Inc., FTC File No. 122-3090 (2014), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

infidelity-promoting website Ashley Madison.[11] Although such extreme effects are rare, we have other examples of serious health and safety informational injuries. For example, we brought a case against Accusearch for selling illegally-obtained personal telephone records of individuals. In that case, we had evidence that stalkers and abusive former spouses used this information to surveil and harass individuals.[12] In addition, we 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.[13]

Unwarranted Intrusion Injury. Some of our efforts at the FTC have involved a fourth category of injury that I described as "unwarranted intrusions." Indeed, this type of informational injury was the primary motivation for the creation of the Do Not Call registry, one of the most popular FTC initiatives ever.[14] More recently, consider our case against national rent-to-own company Aaron's. The company agreed to settle charges that it knowingly played a direct role in its franchisees' installation and use of certain software on rental computers. That software secretly monitored consumers, enabling employees to take webcam pictures of consumers in their homes, often in private situations.[15]

Reputational Injury. Finally, some of our cases involve a fifth category, reputational injury, which in our cases generally overlaps with other types of injury. To be clear, we have never brought an unfairness case based only on reputational injury. But in some of our deception

---

[11] 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.
[12] *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.
[13] 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.
[14] J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. Chi. L. Rev. 109, 109 (2008).
[15] Aaron's, FTC File No. 122-3264 (2013), https://www.ftc.gov/enforcement/cases-proceedings/122-3256/aarons-inc-matter.

cases, the effect on reputation is part of why a deceptive claim is material to consumers. Our first online privacy case dealt with this kind of injury when pharmaceutical company Eli Lilly allegedly deceived consumers by disclosing, without their permission, an email list of more than six hundred consumers using Prozac.[16] Sometimes the reputational injury triggers another kind of harm. For example, publicized sensitive information about an individual's psychological or medical condition or social activities could lead an employer to fire that individual. In other cases, the reputational injury is distinct from other injuries. For example, the release of information about certain medical conditions might harm one's reputation, but it could also lead to medical ID theft, which would be a financial harm.

So there it is: deception that undermines consumer choices; financial; health and safety; unwarranted intrusion; and reputational harm. This is not an exhaustive list of the types of injury that can occur from a privacy or data security problem. But these types of injury have been identified in the FTC's privacy and data security cases, even if certain of these types have not been an independent basis for liability.

Other Characteristics of Injury. Of course, the *type* of injury isn't the only relevant injury characteristic that influences whether the FTC will bring a privacy or data security case. For example, we also consider the strength of evidence linking the problematic practices and injury. Typically, we observe that injury is caused by misuse of the information once collected or distributed. The FTC also considers the magnitude of injury. We look both at the magnitude of individual injury, as well as in total. Small individual injuries to a large group of consumers can trigger scrutiny. Finally, under our unfairness authority the Commission considers both realized injuries as well as those that are likely. A discussion of each of these other dimensions

[16] Eli Lilly and Co., FTC File No. 012-3214 (2002), http://www.ftc.gov/enforcement/cases-proceedings/012-3214/eli-lilly-company-matter.

of informational injury, as well as the connections between them, could fill several speeches. That's why I've focused today on the type of injury.

Conclusion and Next Steps. So let's review. The key takeaway is that the FTC has brought privacy and data security cases to address practices causing several different types of consumer injury, typically financial injuries and health and safety injuries. Our deception cases always involve harm to consumer sovereignty from a broken promise about a material term, and can cover an even broader range of informational injuries.

This analysis raises several important questions. Is this list of injuries representative? When do these or other informational injuries require government intervention? Perhaps most importantly, how does this list map to our statutory deception and unfairness authorities?

These are critical and challenging questions. That's why I am announcing today that the FTC will host a workshop on informational injury on December 12 of this year. This workshop will bring stakeholders together to discuss these issues in depth. I have 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. Ultimately, the goal is to inform our case selection and enforcement choices going forward. I hope you all will consider participating and attending. Our website will have a more detailed announcement in the coming days.

So, with that, thank you again for having me, and I look forward to the discussion and your questions.