United States of America

Federal Trade Commission

PrivacyCon 2018 Opening Remarks

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

February 28, 2018

Introduction

Thank you all, and welcome to PrivacyCon 2018. This week has been a whirlwind week at the FTC. On Monday, we won big in the 9th Circuit, which confirmed that our jurisdiction can reach the non-common carrier actions of Internet Service Providers.[2] Yesterday we announced that PayPal settled FTC charges that Venmo misled consumers about the ability to withdraw funds and manage privacy settings.[3] And today, we have not just PrivacyCon but also a big release that I'll talk about shortly. And it's only Wednesday! Tomorrow, we will have another big roll out, so keep your eyes peeled.

---

[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] *Fed. Trade Comm'n v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. Feb. 26, 2018), https://www.ftc.gov/system/files/documents/cases/att_enbanc_5-16585.pdf.
[3] FTC Press Release, "PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act," Feb. 27, 2018, https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

In such busy times, PrivacyCon couldn't happen without a talented team. Although there are too many people for me to thank individually, I would like to thank Kristen Anderson and the whole Bureau of Consumer Protection team, Tim Daniels and the whole Bureau of Economics team, our amazing events coordinator Kristal Peters, and the media team and paralegals.

This is the FTC's third annual PrivacyCon. Privacy is a fast-moving field and much has changed since the second PrivacyCon in January of 2017. I'm going to hit on three main points today. I'll summarize our work in privacy and data security in the past year, particularly our focus on the economics of privacy. Building on that focus, I'll summarize my key takeaways from our informational injury workshop last December. Finally, I'll talk about how this PrivacyCon is a fitting capstone to my year as the Acting Chairman.

First, the FTC has been extremely active in privacy and data security work over this past year. We've brought important cases against Uber, Lenovo, VTech, and, just this week, Venmo, among others.[4] We brought our first three actions to enforce the EU-US Privacy Shield agreement.[5] We are investigating the Equifax data breach. Similarly, we have been very active in our policy work. We held workshops and issued staff perspectives on the privacy and data security implications of connected cars and of educational technology.[6] And of course, there was our Informational Injury workshop, which I'll discuss in detail shortly.

---

[4] *See* Uber Tech., Inc., FTC File No. 152-3054 (2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3054/uber-technologies-inc; Lenovo, Inc., FTC File No. 152-3134 (2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc; VTech Elecs. Ltd., FTC File No. 162-3032 (2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited; PayPal, Inc., FTC File No. 162-3102 (2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter.

[5] *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.

[6] *See* FTC Event, "Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles," June 28, 2017, https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected; FTC Event, "Student Privacy and Ed Tech," Dec. 1, 2017, https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech.

But first, the latest big news: just this morning we released a report on Mobile Security Updates that explores how smartphones and tablets receive patches for vulnerabilities discovered in their operating system software.[7] We based this on information gathered from eight mobile device manufacturers through our "6(b)" authority, which requires companies to furnish answers to specific questions. Following a number of press reports about delays or lapses in mobile phone patching, we sought companies' information about how and when they deploy software updates to their devices. The report is full of useful information about how security updates are deployed to mobile devices, and the various roles manufacturers, carriers, and consumers play in a successful update. We studied company responses to assess how fast they roll out updates, what factors affect the number and speed of updates, and how price, popularity, and age of devices affect manufacturers' decisions to issue updates. The report contains key lessons learned and offers recommendations for government and industry. For example, it suggests steps that manufacturers should consider taking to deliver security updates to users faster. And it suggests ways government, industry, and advocacy groups can work together to help consumers understand the importance of security updates and their role in the process. Our Bureau of Economics also supplied a lengthy appendix with analyses that underpin the findings of the report. It is an in-depth, sophisticated report and I applaud the dedicated staff - especially Elisa Jillson and Devesh Raval - who worked so diligently to produce it. I hope you all will set some time aside to read it.

[7] *See* FED. TRADE COMM'N, MOBILE SECURITY UPDATES: UNDERSTANDING THE ISSUES, Feb. 28, 2018, https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

As many of you know, over the past year I have sought to explore the benefits of applying an economic approach to privacy and data security issues. Today's lineup reflects that emphasis, and I look forward to hearing from our panelists who have pursued this type of analysis.

But what does an economic approach look like? It decidedly is not just about numbers, measurements, and formulas. That's mathematics. Many economists use math, but economics isn't simply about math. Economics is about real people making choices about how to use limited resources to get what they need and want through exchanges in the marketplace. Economists seek to discover general principles about those individual exchanges and how, in aggregate, those exchanges affect society.

Thus, an economic approach to privacy means applying the tools of economic analysis to help understand how and why companies collect information, what exchanges are taking place, and the likely consequences of certain arrangements regarding private information. What makes information valuable? How valuable is it? Does the value depend on who holds it and why? Why and how do people exchange information? How can information be put to its highest value use? Does it matter who gets to decide the highest value use? How do markets in information develop and what are their flaws?

These are important economic questions. And they are key privacy questions, too. I glad to say that at the FTC we've already been looking at privacy and data security using economic thinking.

The most visible result of this work was December's Informational Injury Workshop.[8] This full-day workshop sought to better identify the qualitatively different types of injury to consumers from privacy and data security incidents. It examined different definitions of informational injury and when government intervention is warranted. It explored frameworks for how we might approach quantitatively measuring such injuries and estimate the risk of their occurrence. And it sought to understand better 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.

Let me share my key takeaways from that event.

First, it is clear that privacy and data security incidents can and have caused injuries that do not involve solely financial loss. The first panel discussed real stories about such injuries. These included, medical identity theft affecting medical treatment, and doxing, which is the public dissemination of private facts leading to extortion or stalking. This reminds me of our case early this year against MyEx.com, a revenge porn site.[9] The site urged users to get revenge by posting intimate pictures of others, and then would charge the pictured individuals for taking down the photos. People who were featured on this site suffered real harm in addition to the money they paid to remove intimate images and personal information. Many lost jobs or job opportunities, and were threatened, stalked, and harassed.

[8] *See* FTC Event, "Informational Injury Workshop," Dec. 12, 2017, https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop.
[9] Emp Media Inc. (MyEx.com), FTC File No. 162-3052 (2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3052/emp-media-inc-myexcom.

The panel also talked about increased risks to health and safety that can arise from the revelation of people's real-time location. The takeaway is clear: consumers can suffer injury from privacy and data security incidents and that injury isn't limited to loss of money. This is also consistent with longstanding FTC case law and with the Commission's Deception and Unfairness statements.[10]

Second, although it was clear that injury is more than just financial loss, there was wide disagreement on the second panel about what else comprises a privacy or data security injury. All agreed that certain uses of sensitive data can cause injury, even if the harm was not financial. However, some had more expansive views of injury, including concepts such as breaching the boundary between one individual and another; revelation to others of something private; increased risk or likelihood of a future cost; or contravening a person's expectations without any benefit to them.

Some of these definitions of injury were consistent with previous FTC actions but some would sweep in nearly any information collection. The extremely wide range of conflicting conceptions of injury demonstrates that defining injury is a key issue in the privacy debate.

Despite the experts' wide-ranging and conflicting definitions of injury, there was general agreement that government intervention ought to be tied to injury, whatever the definition. All panelists agreed that some injuries do not warrant government intervention, although they differed significantly on when intervention might be warranted – again, largely based on how they defined injury. All panelists agreed that countervailing benefits have to be evaluated as well. Panelists also agreed that there were tradeoffs to both ex post and ex ante interventions.

[10] FTC Statement on Deception (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; FTC Statement on Unfairness (Dec. 17, 1980) (appended to *International Harvester Co.*, 104 F.T.C. 949, 1070 (1984)), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

The fourth topic of the day was measuring injury. To paraphrase one of the panelists, there are easy cases and there are hard cases; unfortunately, most of them are hard cases.[11] Research in this area is challenging. While people say they care about privacy in the abstract, what they do when faced with actual choices is often very different. This isn't necessarily because consumers don't know what they think; instead, consumers balance a huge range of product and service dimensions when making choices. Privacy is but one important dimension of products. Others include price, convenience, quality, and other factors. Different individuals will make different tradeoffs when faced with those many dimensions.

So when trying to measure injury, there are many things one might consider: the type of injury, the sensitivity of the data, the magnitude, the frequency, and the causal link to a particular firm or practice. Each of these raises significant challenges. There is interesting work on each of these dimensions. But we certainly need more research.

I also note that different types of measurement might be appropriate for different purposes. In the law enforcement space, for example, tools might differ depending on whether the goal is selecting cases, demonstrating liability, or calculating damages.

Overall, my key takeaway from the measurement panel was that not everything that can be measured matters, and not everything that matters can be measured. But we ought to measure the things we can and think hard about how to objectively and consistently evaluate the things we cannot. After all, if we cannot measure - or even estimate - the injury we are trying to address, how can we tell if we are directing government action effectively?

[11] FTC Event Transcript and Video, Informational Injury Workshop - Panel 4: Measuring Injury, Dec. 12, 2017, https://www.ftc.gov/news-events/audio-video/video/informational-injury-panel-4-measuring-injury.

The Informational Injury workshop was another chapter of a conversation and research agenda that is only getting started. Today's PrivacyCon continues that exciting conversation. PrivacyCon has a couple of purposes, as I see it. First, it helps the FTC stay up-to-date with novel and interesting research that can inform our privacy and data security missions. Second, PrivacyCon provides a forum for highlighting emerging issues and bringing them into the conversation. Today's program will fulfill both purposes.

The emphasis of previous PrivacyCons has been technological developments. Today's program continues that developing tradition. Panels one and four contain ten presentations describing how technology can exacerbate or alleviate privacy and security risks. As I've already mentioned, this year we also emphasize economic questions, with ten papers in panels two and three that explore consumer perception and behavior, firm incentives, and market characteristics. I think this cross-disciplinary approach is essential. Lawyers, technologists, and economists can learn a lot from each other – and given the challenges consumers face on the privacy and data security front, we need to take advantage of crosscutting research. Doing so will help consumers, industry, and the FTC better understand how to protect privacy and data security.

I am also gratified that during the lunch period we will be able to showcase, in our poster session, the work of early career academics and students. And I am pleased that attendees will have the chance to interact with representatives from government agencies that fund privacy and data security research as well. Both the poster session and the funders will be in the conference rooms just across the hall during the lunch hour.

To summarize, it's been a big year in privacy and data security at the FTC. We've accomplished a lot for consumers, and we have a lot of work to do going forward. PrivacyCon is an important part of that work. So I thank all of you for being here today, best of luck to the presenters, and I look forward to a productive day.