Bureau Director's Opening Remarks
Data Security Hearing

Andrew Smith
December 11, 2018

Good morning everyone. Welcome to the FTC's hearing on Data Security, the ninth session in the Commission's Hearings on Competition and Consumer Protection in the 21st Century. I want to begin by thanking all of the workshop participants for taking the time from their busy schedules to share their expertise, and all of you for coming today. I would also like to thank Elisa Jillson, Jim Trilling, and Jared Ho from our Bureau of Consumer Protection, Mike LeGower and Marc Luppino from our Bureau of Economics, and many staff in the Office of Policy Planning.

I. Introduction

Today, as we talk about data security in the 21st century, we have a chance to think about the current state of data security and about how it is likely to change in the future. To understand where we are now, and where we're headed, it's helpful to look to the past.

Data security vulnerabilities, in the broadest sense, are nothing new. As long as there has been sensitive data, there have been threats to it – whether it came in the form of a counterfeit wax seal on messages during the Middle Ages,[1] which allowed political foes to countermand the king's commands, or in the manner of wartime spies out of a John Le Carré novel, who compromised information networks, stole letters and falsified maps to undermine the enemy.

Digital data security vulnerabilities are also nothing new: They've been around since the the advent of computers and the Internet. In the 1970s, the so-called "Creeper Worm" virus infected the ARPANET, the precursor to the Internet, and copied itself to remote systems,

[1] William Blackstone, Commentaries on the Laws of England, Volume 2, § 82(5).

displaying the message: "I'm the creeper, catch me if you can!"[2] In 1986, two brothers created what some have called the world's first PC malware, nicknamed "the Brain."[3] This virus traveled via floppy disk, infecting one computer at a time as the disk changed hands, greeting users of affected computers with the salutation "Welcome to the Dungeon."[4]

The ARPANET and floppy disks are now a distant memory, but computer viruses and malware certainly are not. One security lab reported last year that, on a *daily* basis, it detected 350,000 malicious files.[5] By one estimate, malware costs the U.S. economy over $100 billion a year.[6]

In fact, malware and various forms of online attack are now so prevalent that it's become a truism that there are only 2 kinds of companies: those that have been hacked and those that don't know that they've been hacked. By one count, there were more than 1,250 data breaches last year,[7] with 4.5 *billion* records compromised.[8] In just the last two weeks, we've heard announcements of major breaches at household brands.

II. Why Are We Here?

With the rise of online banking, e-commerce, smartphones, and connected homes, and the prospect of connected cars and artificial intelligence, digital data security has never been more important. The FTC is working diligently to protect consumers by promoting the security of their data and devices. The FTC approaches data security in three ways:

- First, policy work. For example, two weeks ago, FTC Commissioners testified before Congress about what data security enforcement tools the FTC is using and what

[2] https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/
[3] http://news.bbc.co.uk/2/hi/technology/4630910.stm
[4] https://en.wikipedia.org/wiki/Brain_(computer_virus)
[5] https://www.av-test.org/en/statistics/malware/
[6] https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
[7] https://www.bna.com/2017-year-data-b73014473359/
[8] https://www.pcmag.com/news/364226/data-breaches-compromised-4-5-billion-records-in-first-half

additional tools it could use to protect consumers' data. Today's hearing is part of the Commission's policy work. The record developed today will help to inform the Commission further on how best to use its tools to promote appropriate data security.

- Second, education. The FTC publishes business education pieces, like Start with Security, that help businesses to design and maintain reasonable data security programs. As one Chief Information Security Officer put it, a hacker only needs to be lucky once to breach a company's defenses. A company defending against daily attacks, on the other hand, has to be lucky *every day*. The FTC's education pieces help companies to fortify their defenses so that it's not just luck at play.
- And third, enforcement. The FTC has settled more than 60 data security cases on issues ranging from IoT to children's data to financial records. There's more to come, in each of those areas. For example, in January, FTC staff will be going to trial in *D-Link*, a case centered on IoT security.

There's no question that the FTC has been actively policing data security practices. But how should we square the FTC's work in this area with reports of increased number and size of breaches? On one hand, perhaps the current approach to security is working, and the apparent uptick in breaches is just a result of the move of more data online, the greater sophistication of attackers, and the well-documented shortage of security personnel. On the other hand, perhaps the swell of breaches indicates that the current approach to data security requires some serious rejiggering. Or, perhaps the middle ground is correct: the current approach is solid, but we need more of it, powered by different tools.

That's why we're here today. We are here to think hard about the state of data security and data security regulation and about how we can improve them. We need to ask tough questions:

- First, what are the incentives to invest in data security – and are they enough?
- Second, what does consumer demand for security look like – and can it meaningfully drive data security investment? Should we expect consumers to participate meaningfully in securing their own information?
- Third, we rely on data security assessments to measure security levels. What's the best way to inform stakeholders – whether it's security personnel, executives, boards, cyber insurers, card issuers, or regulators – of the state of security at a particular company?
- Fourth, what regulatory and enforcement approaches are working and how can they be improved?
- And, finally, we want to take a hard look at the FTC: Are the available tools up to the task of effectively identifying and rectifying data insecurity?

III. Hearing's Agenda

We're going to tackle these big questions over the course of this two-day hearing. This morning, we'll start by focusing on data breaches. Marc Spitler from Verizon Security Research will present on the Data Breach Investigations Report, the annual chronicle of data breaches and their causes. Next, Sebastien Gay from Georgetown's Economics Department will describe his work on how some firms internalize the cost of data breaches – whether their stock price takes a hit and how firms mitigate that potential impact. And, finally, Al Pascaul from Javelin Strategy and Research will describe some markers of how data breaches affect consumers.

This afternoon, we'll turn to two panel discussions. The first will discuss the incentives to invest in data security – ranging from consumer trust to compliance obligations to market incentives like cyber insurance – and explore how companies make those investment decisions. The second panel will explore consumer demand for security. During this discussion, we'll hear about emerging security ratings that allow consumers to compare the security of products. We'll then hear from panelists about the extent to which it makes sense to count on consumers to shop on security.

Tomorrow, another panel will tackle data security assessments. Assessors from a variety of backgrounds – from Big 4 accounting to security boutiques to cyber insurance firms – will react to a series of hypothetical assessment situations. In these hypos, panelists will address thorny issues like who defines the proper scope of an assessment, how a company with a tight budget and big problems should gage security, when to look to inside expertise and when an outside perspective is better.

Next, Commission Rebecca Kelly Slaughter and Joshua Corman—the co-founder of the @IamTheCavalry security initiative—will talk about the threat landscape: what is going on and what threats are just now emerging. Commissioner Slaughter and Mr. Corman will talk about what companies, consumers, and the FTC should do in the face of these threats.

That afternoon, panelists will turn to policy, with a pair of panels on the U.S. approach to data security and FTC data security enforcement. Building on discussions earlier in the day, these panels will take a hard look at what regulatory approaches are working, what's falling short, and how the current approaches could be improved. Following these panels, my colleague Maneesha Mithal from the FTC's Division of Privacy and Identity Protection will provide closing remarks.

IV. Conclusion

We have a lot to cover, with presenters and panelists who have thought a lot about these important issues. I'd now like to turn it over to Jared Ho in the Division of Privacy and Identity Protection and Marc Luppino in the Bureau of Economics, who will start us off with a series of presentations about data breaches. Thank you for coming today and for helping us to think about the state of data security.