On the Front Lines: The FTC's Role in Data Security

U.S. Federal Trade Commissioner Julie Brill

Keynote Address Before the Center for Strategic and International Studies, "Stepping into the Fray: The Role of Independent Agencies in Cybersecurity"

September 17, 2014

Thank you, Jim, for that kind introduction. And thank you to the Center for inviting me to address you this afternoon. It is a pleasure to speak with a group that has such depth and breadth in security issues.

We live in a networked world. We Americans depend on constant connections to work, relax, and toggle between the two. Communications networks synchronize our critical infrastructure, including our electricity, water, hospitals, buses and transportation systems. And we're rapidly moving toward an Internet of Things, which will put everything from our washers and dryers to our cars online. These developments hold promises small and great, from allowing us to save us a few steps to turn off the lights, to using our resources more efficiently.

All of these connections bring risks along with benefits. Over the past year, it seems that we haven't gone more than a few days without hearing about a major security breach involving consumers' financial data or other sensitive information.[1] Verizon's latest Data Breach Investigations Report records nearly 1,400 breaches in 2013.[2] Retailers,[3] hospitals,[4] and universities[5] have all been targets. And federal agencies have taken their hits as well.[6] The scale of breaches has kept pace with Moore's Law, and at the same time we're putting more and more sensitive information online. This means that the stakes in the security game are continuously increasing.

---

[1] *See* Brian Krebs, *Why So Many Card Breaches? A Q&A*, Krebs on Security (Aug. 15, 2014), http://krebsonsecurity.com/2014/08/why-so-many-card-breaches-a-qa/.

[2] Verizon, *2014 Data Breach Investigations Report* 2, http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

[3] *See* Krebs, *Why So Many Card Breaches?*, *supra* note 1.

[4] *See* Jose Pagliery, *Hospital Network Hacked, 4.5 Million Records Stolen*, CNN MONEY (Aug. 18, 2014, 3:25 PM), http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/index.html.

[5] *See* Elizabeth Weise, *Calif. Attorney General Focuses on Retailers' Data Theft*, USA TODAY (Feb. 27, 2014), *available at* http://www.usatoday.com/story/tech/2014/02/27/california-data-breaches-hit-213-million-accounts/5868191/ (noting a reported security breach at the University of California, Davis Health System).

[6] *See generally* Gov't Accountability Office, Testimony Before the S. Cmte. on Homeland Security and Gov't Affairs, GAO-14-487T (Apr. 2, 2014), *available at* http://www.gao.gov/assets/670/662227.pdf.

Consumers expect companies to protect their information. Data security protections are increasingly like keeping the lights on. Consumers might not notice when they work, but they sure notice when they fail.[7]

Data security is one of our top consumer protection priorities. In our enforcement actions and policy initiatives, we focus on the harms that consumers may suffer when companies fail to keep information secure.[8] Unauthorized access to data puts consumers at risk of fraud, identity theft, and even physical harm. Data can reveal information about our health conditions, financial status, or other sensitive traits. Security is also an essential part of maintaining consumers' privacy, which is another top consumer protection priority at the FTC.

I'd like to convey two main messages about our data security enforcement. First, we enforce a flexible standard of reasonable security.[9] Second, the FTC is the only federal agency with the authority to enforce such a standard across broad swaths of the U.S. economy. Our reasonable security standard adapts to rapid changes in both technology and security threats, allowing us to apply this standard to both older technologies as well as technologies that are just emerging.

Putting the FTC's Data Security Enforcement in Context of other Recent Governmental Efforts

The FTC plays a unique role in the broad effort to keep computers, networks, and people secure. For more than a decade, we have used all of our tools – including law enforcement, policy initiatives, and consumer and business education – to prevent and remedy the harms that can result from *personal* information falling into the wrong hands. [10]

Over the past few years, other governmental experts have turned their attention to answering difficult questions about the legal, economic, political, and military aspects of cybersecurity. The Obama Administration has been active on this front, reaching important milestones with the Executive Order on critical infrastructure cybersecurity[11] and NIST's

---

[7] I have adapted a quotation from the FTC's recently serving senior legal advisor, Andrea Matwyshyn, *See* Issie Lapowsky, *We'd All Benefit If Celebs Sue Apple over the Photo Hack*, WIRED (Sept. 4, 2014, 6:30 AM), http://www.wired.com/2014/09/law-apple-photo-hack/ (quoting Matwyshyn as saying "For consumers, . . . data security is increasingly like heat in winter.").

[8] *See generally* FTC, Prepared Statement on Protecting Personal Data from Cyber Attacks and Data Breaches Before the S. Cmte. on Commerce, Sci., and Transp. (Mar. 26, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf.

[9] *See id.* at 6-7 ("[T]he FTC's approach to reasonableness is process-based rather than a checklist of specific technologies or tools."). *See also* FTC, Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[10] *See* Statement Marking the FTC's 50th Data Security Settlement, *supra* note 9.

[11] President Barack Obama, Exec. Order 13636—Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Framework for Improving Critical Infrastructure Cybersecurity.[12] I applaud the Administration's efforts and its use of an inclusive process to develop these policies.

The core of the NIST *Framework* is about risk assessment and mitigation. In this regard, it is fully consistent with the FTC's enforcement framework. One of the pillars of reasonable security practices that the FTC has established through our settlements in more than 50 data security cases is that assessing and addressing security risks must be a continuous process. There is no single, right way to do these assessments; it depends on the volume and sensitivity of information the company holds, the cost of the tools that are available to address vulnerabilities, and other factors.[13] By identifying different risk management practices and defining different levels of implementation, the NIST *Framework* takes a similar approach.[14]

FTC Data Security Enforcement Over a Decade in Time and Many Generations of Technology

The main legal authority that the FTC uses in the data security space is Section 5 of the FTC Act,[15] which gives us the ability to stop unfair or deceptive acts or practices. We first applied Section 5 to data security issues in 2002, back in the day when, to paraphrase Tom Friedman, 4G was a parking spot, an app was something high school seniors sent to colleges, clouds were in the sky, twitter was for birds, and Skype was a typo.[16] The world of 2002 is truly the distant past, yet Section 5 remains a highly effective tool for protecting consumers' information.

The FTC's data security enforcement actions initially focused on deception. Recognizing that consumers' data was valuable to them and potentially harmful if obtained by fraudsters, identity thieves, and other malicious actors, companies began to promise to consumers that they would keep this data secure. Those promises were, and are, material to consumers' choices about whether to use a product or service. After all, who would entrust their information to a company that doesn't protect it? When companies don't live up to their promises, the FTC may

---

[12] NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[13] *See* FTC, Statement for Hearing on Protecting Personal Information from Cyber Attacks and Data Breaches 3, S. Comm. on Commerce, Sci., and Transp. (Mar. 26, 2014), http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf.

[14] *See* NIST FRAMEWORK, *supra* note 12, at 7 ("The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. . . . Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, ...").

[15] 15 U.S.C. § 45. The FTC also has data security enforcement authority under the Gramm-Leach-Bliley Act and the Safeguards Rule, Fair Credit Reporting Act, the HIPAA HITECH Act, and the Children's Online Privacy Protection Act and its implementing rule.

[16] Nathan Gardels, *Tom Friedman: The 401k Society*, WORLDPOST (Jan. 28, 2014, 2:59 PM), http://www.huffingtonpost.com/2014/01/27/tom-friedman-401k-society_n_4676301.html. *Id.*

step in. From the very beginning, our view has been that a promise to keep information secure has to be backed up by reasonable and appropriate processes and practices.[17]

Within a few years, it became clear that the FTC's ability to stop unfair practices under Section 5 would have its place alongside deception in our efforts to ensure reasonable security protections for consumer data. The key difference between unfairness and deception is that unfairness may be applicable even in the absence of a representation or omission in information presented to consumers. In 2005, we brought our first data security case under a pure unfairness theory, following a breach that exposed the sensitive personal information of thousands of consumers.[18] In the language of our unfairness standard, this company's data security practices caused, or were likely to cause, a substantial injury that consumers could not reasonably avoid and were not outweighed by benefits to consumers or competition.[19] These days, of course, it's not unusual to read about breaches that involve records about millions, or tens of millions, of consumers. The scale of breaches has changed, but the legal principles we seek to enforce have not.

In our settlements and guidances, the Commission has outlined reasonable security practices while emphasizing that companies need to implement these practices in a way that is appropriate for their businesses. These practices include:[20]

- Do a risk assessment. Companies should know what information they have, how it flows through their enterprise, what kind of access employees and third parties have to this information, and what vulnerabilities could compromise its confidentiality, integrity, or availability.

- Minimize personal information about consumers. Limiting the consumer information that companies collect and retain to what is necessary to fulfill legitimate business needs will help reduce unnecessary security risks.

- Implement technical and physical safeguards. Security measures like firewalls, strong passwords, and limiting the circumstances under which sensitive personal information may be stored on laptops are important but not sufficient. Protecting information "the old fashioned way" – by ensuring that back up tapes, CDs,

---

[17] *See* FTC, Microsoft Settles FTC Charges Alleging False Security and Privacy Practices (Aug. 8, 2002), http://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-and-privacy (quoting then-Chairman Timothy Muris as saying "[c]ompanies that promise to keep personal information secure must follow reasonable and appropriate measures to do so. It's not only good business, it's the law. Even absent known security breaches, we will not wait to act.").

[18] BJ's Wholesale Club, Inc., Case No. C-4148 (Sept. 20, 2005), http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf (decision and order).

[19] FTC, POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980), *available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[20] *See* FTC Statement on 50th Data Security Settlement, *supra* note 9, at 1. *See also* FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Nov. 2011), *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.

external hard drives, USB thumbdrives and the like are locked up, and securely destroyed when no longer needed – is a risk reducing complement to security measures deployed on computers and networks.

- Train employees to handle personal information properly.

- Have a plan in place to respond to any security incidents that occur.

This is not a standard of perfect security. FTC staff investigates hundreds of breaches, and so far we have brought 53 cases under Section 5. We tend to bring an action when we find systemic failures in a company's data security practices. So the fact that there's an isolated vulnerability in a product or service that a company offers, or even the fact that a company suffers a breach, does not mean that the FTC will come calling, let alone file a lawsuit.

Some of the FTC's actions are against companies that are themselves victims of hacking or other malicious actions. But this does not and should not relieve companies of the need to provide reasonable security. After all, it is the company that decides what data to collect, how to use it, and when – if ever – to get rid of it. Holding companies accountable for their practices and the representations they make is entirely appropriate and consistent with how we apply Section 5 to other commercial activities.

Using Section 5 to Address New Data Security Challenges

Today, consumers are moving more of their activities to smartphones and connected devices. These phones and devices are producing an increasing amount of sensitive data, including user generated health information. Our recent data security cases show that Section 5 is up to the task of protecting consumers in this rapidly changing environment. Let me focus on three emerging areas that seem particularly salient in our data intensive economy, beginning with mobile.

Mobile

Mobile devices and apps provide convenience, entertainment, and a platform for us to connect to one another in new and exciting ways. But when apps fail to provide reasonable security, they can leave a broad range of sensitive personal information at risk.

For example, earlier this year, the FTC brought enforcement actions against two popular apps: Credit Karma and Fandango.[21] We alleged that these apps contained flawed implementations of the Secure Sockets Layer (SSL) protocol, which is a common means for encrypting data in transit.[22] Specifically, we alleged that the Credit Karma and Fandango apps were susceptible to "man in the middle attacks," in which an impostor could pose as a legitimate

[21] FTC, Press Release, Fandango, Credit Karma Settle FTC Charges That They Deceived Consumers by Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.

[22] *Id.*

data recipient and collect highly sensitive information from consumers – including Social Security numbers in the case of Credit Karma, and credit card information in the case of Fandango.[23] These companies were not tripped up by bad luck. Our complaints allege that they overrode more secure default settings and failed to test adequately what would happen after they did so.[24]

The FTC also brought an action against the mobile app Snapchat, which allows consumers to send photos or videos that disappear after just a few seconds.[25] Or so Snapchat told its users. The part of the FTC's complaint that seemed to draw the most attention was the allegation that, despite the company's representations, recipients were able to save "snaps" indefinitely using a few simple techniques.[26] But we also alleged that the app exposed consumers' mobile phone numbers,[27] and left consumers vulnerable to being impersonated by other Snapchat users.[28] Thus the Snapchat case raises both significant privacy issues, and reminds us that security – which includes controls to keep information confidential – is critical to effective privacy protections.

As a group, these three cases show that the FTC's framework for holding companies to a standard of reasonable data security readily applies to the mobile environment.

Internet of Things

Let's turn to the Internet of Things. While connected devices can provide innovative services, they must do so in a way that does not violate consumer privacy or leave personal information vulnerable to exposure. Some of the data coming from connected watches, appliances, clothes, and other everyday devices could reveal a lot about our health, activities in our home, or other highly sensitive aspects of our lives.[29] Protecting this information from unauthorized access and disclosure is paramount. I am concerned that some of the lessons of the recent past aren't being applied to these exciting new technologies. A recent study by HP found

---

[23] *Id.* *See also* Credit Karma, Case No. C-4480, at ¶ 6 (F.T.C. Aug. 13, 2014) (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Fandango, LLC, Case No. C-4481, at ¶ 6 (F.TC. Aug. 13, 2014) (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

[24] Credit Karma Complaint, *supra* note 22, at ¶¶ 16-18; Fandango Complaint, *supra* note 23, at ¶ 19.

[25] *See* FTC, Press Release, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[26] Snapchat, Inc., FTC File No. 132 3078, at ¶¶ 6-19 (May 8, 2014) (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf.

[27] *Id.* at ¶¶ 30-33.

[28] *Id.* at ¶¶ 34-45.

[29] *See* Julie Brill, Comm'r, FTC, The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control (Mar. 14, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/289531/140314fordhamprivacyspeech.pdf; Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. (forthcoming 2014).

that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[30]

The first case we brought in the Internet of Things area was against TRENDNet, which makes Internet-connected video cameras.[31] Our complaint alleges that TRENDNet's cameras were vulnerable to having their feeds hijacked.[32] And, indeed, around 700 private video feeds, some of which included images of children and families going about their daily activities in their homes, were hacked and publicly posted as a result of the company's allegedly lax security practices.[33] As more devices become connected to the Internet, the potential for more information about the most intimate details of our lives to slip into the wrong hands grows unless appropriate safeguards are put into place.

Health Information

Finally, let me focus on health information. Our recent cases show that we're serious about enforcing protections for sensitive information. There is broad agreement that information about consumers' health and medical conditions is sensitive and that consumers suffer harm when this information is unexpectedly revealed. Companies that collect this information need to recognize its sensitivity and provide safeguards to match.

In two recent cases, the FTC had reason to believe that companies failed to provide such safeguards. Last fall, we announced a settlement with Accretive Health in a case that stemmed from the theft of an unencrypted laptop from an employee's car.[34] This one laptop contained 20 million pieces of health-related information about 23,000 patients.[35] But the case wasn't about the lost laptop: It was about the company's failure to adequately train employees, to limit the data contained on the laptops, and to implement reasonable technical security safeguards.[36] And earlier this year, we announced a settlement with GMR Transcription Services, which used a

---

[30] HP, *Internet of Things Research Study* 2 (July 2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[31] *See* FTC, Press Release, FTC Approves Final Order Settling Charges Against TRENDNet, Inc. (Feb. 7, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

[32] TRENDNet, Inc., Case No. C-4426 (F.T.C. Feb. 7, 2014), at ¶ 8 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[33] TRENDNet Complaint, *supra* note 32, at ¶¶ 9-11.

[34] FTC, Press Release, Accretive Health Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (Dec. 31, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/accretive-health-settles-ftc-charges-it-failed-adequately-protect.

[35] *Id.*

[36] Accretive Health, Inc. Case No. C-4432, at ¶¶ 6-7 (F.T.C. Feb. 5, 2014) (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf.

contractor that left wide open the door to notes from medical exams and other highly sensitive medical information, allowing them to be indexed by Internet search engines.[37]

Taking a Broader View of Data Security Through Policy Initiatives

Let me take a step back and talk about policy. Policy initiatives are another important aspect of the FTC's data security efforts. Those of you who are familiar with our work know that we are adept at identifying emerging challenges in many areas of consumer protection. Data security is no different. We recently held two public workshops that explored emerging data security issues. At our June 2013 workshop on mobile security, panelists from industry and academia took a comprehensive look at security in the mobile environment.[38] The topics included identifying and closing software vulnerabilities during the development process, making devices harder to crack if they are lost or stolen, and making user interfaces to security features more consumer-friendly. This last point is critical. Just as privacy experts have recognized that interfaces for providing choice mechanism need some rethinking in the mobile environment, so do the means for providing options to consumers to manage their security settings need to become more consumer-friendly.

Second, in November 2013, the FTC held a full-day workshop on the Internet of Things.[39] While some companies are taking a strong leadership role in securing the highly sensitive data from connected devices, many of the workshop's participants raised questions like those raised by the HP study I just mentioned[40] – questions about whether other companies are paying appropriate attention to securing the data from connected devices. Will companies that, for decades, have manufactured "dumb" appliances take the steps necessary to secure the vast amounts of personal information that their newly smart devices will generate? Will companies design their devices and services to provide appropriate levels of security not only in isolation but also as part of a highly complex and interconnected new ecosystem? These are issues that the FTC is watching closely.

Finally, while the FTC's current enforcement authority and our capacity to develop policy recommendations and best practices in connection with new technologies all play a critical role in providing U.S. consumers with some assurance that companies will keep their information secure, I believe that we need more tools to protect consumers in this area. Along with my fellow Commissioners, I believe that Congress should strengthen the FTC's data security authority by giving us new tools to address these issues. The Commission's unanimous recommendation to Congress includes a call for civil penalty authority, rulemaking authority,

---

[37] FTC, Press Release, FTC Approves Final Order in Case Against GMR Transcription Services (Aug. 21, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services.

[38] FTC, Mobile Security: Potential Threats and Solutions (June 4, 2013), http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutionshttp://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions.

[39] FTC, Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013), *available at* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[40] HP, *Internet of Things Research Study*, *supra* note 30.

and jurisdiction over nonprofits. These elements would place the Commission in a stronger position to deter violations and protect consumers nationwide.[41]

* * * * *

Technology has changed dramatically since the early days of the FTC's privacy and data security enforcement. The FTC's general, flexible consumer protection authority has played an important role stopping and remedying fraud, identity theft, and a broad array of privacy violations as these technological changes have been underway.

We at the FTC cannot address every data security challenge that the United States faces, but we will strive to ensure that companies that collect information about consumers – whether in more traditional ways, or through the mobile ecosystem, the Internet of Things, or other exciting new mechanisms – keep this data secure. Consumers expect – and deserve – no less.

[41] *See* FTC, Senate Commerce Testimony, *supra* note 12, at 10-12.