Do Try This at Home: Starting Up with Security
Keynote at FTC's Start with Security Event
U.S. Federal Trade Commissioner Julie Brill
Seattle, Washington
February 9, 2016

Good morning. Thank you, Chuck Harwood, for such a warm introduction. I am delighted to be in Seattle for this third installment of the FTC's Start with Security series. Today's excellent program is the result of the hard work of FTC staff from the Northwest Regional Office here in Seattle, staff in the Division of Identity Protection in Washington, and many people here at the University of Washington. I would particularly like to thank Ryan Calo, Bill Covington, Emily McReynolds, and Elizabeth Scallon for their help in making this event possible. Many others worked with you, and I appreciate their help as well.

As consumers move more of their lives online, their data is moving with them. We are connecting nearly everything – from cars and buildings to clothing and light bulbs – to the Internet. Cisco reports that there are 25 billion networked devices in the world today and predicts that there will be 50 billion by 2020.[1] These sensors, along with our smartphones, tablets, and computers, generate twice as much data today as they did two years ago, and this trend is expected to continue. Sensors that are so small and efficient that they can power themselves with ambient radio waves are becoming a reality.[2] As a result, data is becoming cheaper to collect and keep, it is coming from an incredibly diverse range of sources – including the physical world around us – and our ability to analyze all of this data is constantly improving. Connected devices, and the data that they generate, create exciting possibilities to solve major social and economic challenges in areas ranging from health care and the environment to education and transportation. And, of course, they give consumers the chance to do things that are new, convenient, and downright cool.

But there are risks from these massive data sets. A lot of the data from connected devices and mobile apps is personal data, and some of it is highly sensitive. When personal data is misused or ends up in the wrong hands, it can cause real harm. Security lapses involving financial information can lead directly to financial losses for consumers or their being targeted for other scams. Breaches of health information can harm consumers' job prospects and compromise their privacy and that of their families. And the unwanted, unexpected exposure of information about activities in consumers' homes can reveal information about a physical space that we all regard as deeply private – and the law strongly protects.[3]

---

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] BBC News, Tiny Chip That Powers Itself from Radio Waves (Dec. 8, 2015), *available at* http://www.bbc.com/news/technology-35038430.

[3] *See, e.g.*, Kyllo v. United States (finding warrantless collection of infrared images of a suspect's home violated the Fourth Amendment).

Unfortunately, data security breaches are occurring more frequently, and identity theft has become all too common. In 2014, the FTC received nearly 500,000 identity theft complaints[4] – making identity theft our number one complaint category for the 15th year in a row.[5]

As a result, data security is a top priority for the FTC, which is the nation's leading consumer protection agency. Eighty years ago, Congress gave the FTC authority to protect consumers from a broad range of "unfair or deceptive acts or practices."[6] When a company deceives consumers about the security protections that it provides, or fails to provide reasonable security and thus crosses the line into unfair practices, then the FTC may step in. Over the past 15 years or so, the FTC has used this authority to bring nearly 60 data security cases. Some of these actions have targeted global Internet giants whose brands are household names.[7] But we have also brought actions against an array of small companies. These days, many small app and device developers are creating products and services that are handling sensitive personal information, which if not properly secured can cause substantial harm to consumers. Small companies can also get big very quickly. Neither new technologies nor small companies get a pass under the FTC Act. So, trying to "fly under the radar" as a small company is not a strategy that I recommend.

Now that I have your attention, here is one way to explain a little more about the FTC's reasonable security standard. We do not expect perfect security. Let me put the difference between reasonable security and perfect security into perspective. The FTC has investigated hundreds of security breaches, but we have brought enforcement actions in only a fraction of those instances. The fact that a company suffers a security breach does not mean that it will face an FTC enforcement action. On the other hand, the FTC has brought actions against companies for creating[8] or failing to close[9] vulnerabilities that created unreasonable risks to consumers, even though there was no evidence of an actual breach.

---

[4] FTC, Consumer Sentinel Network Data Book for January – December 2014 3 (Feb. 2015), *available at* https://www.ftc.gov/enforcement/consumer-sentinel-network/reports.

[5] Tom Risen, *Identity Theft Remains Top Threat*, U.S. NEWS & WORLD REPORT (Mar. 2, 2015 3:38 PM), *available at* https://www.ftc.gov/enforcement/consumer-sentinel-network/reports.

[6] 15 U.S.C. § 45(a).

[7] *See, e.g.*, FTC, Press Release, Oracle Agrees to Settle FTC Charges It Deceived Consumers About Java Software Updates (Dec. 21, 2015), available at https://www.ftc.gov/news-events/press-releases/2015/12/oracle-agrees-settle-ftc-charges-it-deceived-consumers-about-java; Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf; HTC America, Inc., C-4406 (F.T.C. June 25, 2013) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf; Twitter, Inc. C-4316 (F.T.C. Mar. 2, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

[8] *See* HTC, *supra* note 7.

[9] See 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.

So what is "reasonable security"? Reasonable security requires companies to be aware of the amount and sensitivity of personal data that they process, and to take security measures that are appropriate for the data and for the size and complexity of their businesses. This is perhaps the best way for companies to better understand how security breaches could affect their customers and themselves. The FTC also expects ongoing assessments to be part of continuing process of identifying new risks and adjusting their security practices accordingly. Since data security risks differ for each company, no single prescription for a security process or program will work for all companies.[10] But some general features of a reasonable security program apply to many different companies.

For example, companies should build security into their products from the beginning of their development process.[11] Design reviews, code reviews, and testing for vulnerabilities are all ways to detect and fix security issues on an ongoing basis.[12] Training employees to handle personal data appropriately, and implementing appropriate technical and administrative safeguards to protect personal data, are also critical steps to take.[13] It is also important for companies to have a structure in place to receive and act on vulnerability reports. After all, testing and review may not catch every vulnerability before a product goes to market, but companies should take appropriate action to respond to information that they receive about vulnerabilities.[14] Finally, the FTC encourages companies to take a hard look at what kinds of personal data they are collecting and retaining.[15] Avoiding a "collect it all now, sort it out later" approach is not only a good way to reduce security risks but also a strongly pro-privacy step.

Avoiding an enforcement action is not the only reason to take security seriously right from the start. Implementing and maintaining reasonable security measures is a good business decision in its own right. Security is an essential element of consumer trust. If you tell consumers that you're going to keep their information secure, consumers will expect you to make good on that promise. In fact, even if you don't tell consumers anything about security, they will still expect you to keep their data secure.

The other part of the business case for starting with security is that your company will need to address data security eventually. Fixing a wobbly timber is much more difficult once a

---

[10] *See, e.g.*, FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf ["Commission Statement on Data Security"].

[11] *See* FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD iii (staff report) (2015), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [IOT REPORT].

[12] *See* FTC, Careful Connections: Building Security in the Internet of Things (Jan. 27, 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things#Tools ["Careful Connections"].

[13] *See* Commission Statement on Data Security, *supra* note 10.

[14] *See* Careful Connections, *supra* note 12 (recommending that companies "[m]aintain a channel where security researchers or consumers can reach you about a risk they've discovered in one of your products") (bold in original omitted).

[15] IOT REPORT, *supra* note 11, at iii.

house is built around it. Suppose your company grows rapidly by attracting millions of users overnight, or your service becomes part of a bigger system, project, or company. Once this happens, it only becomes more difficult to go back and improve security because of the demands of more users, the additional security challenges of a more complex environment, and the business expectations of a more mature company. Some companies, I suspect, never go back to address vulnerabilities once they have taken off. But the vulnerabilities are still there, and, if exploited, the results can be devastating for a company's brand, valuation, and relationships with consumers and business partners.

There is a more positive, less defensive business case for security. I am glad to see many companies recognize that providing better privacy and security tools to consumers is a business opportunity in itself. For example, companies are offering more services that allow individuals to encrypt their communications, and these services are getting more user-friendly. This field is still emerging. Many secure communications services are easy to use only to the extent that consumers communicate with users of the same service. If consumers want to communicate between different services, they may be stuck using tools that only a few select experts can use properly. Creating tools that avoid some of these limitations could serve consumers very well.

As today's event makes clear, we also believe it's important to hear about the challenges that technologists face with security in practice. One message that we have heard loud and clear over the past few years is that companies would like clearer guidance from us about our data security enforcement standards. As a result, the FTC is putting a lot of effort into providing guidance based on the data security shortcomings that led to our past cases. The most comprehensive form of this guidance is in our *Start with Security* guide, which offers ten examples of alleged security lapses that led to FTC enforcement actions.[16] We also took a deep dive into security issues surrounding connected devices in our report about the Internet of Things, highlighting technical suggestions to help companies address data and device security issues as they develop their software, services, and devices.[17] And we held a privacy and security research conference last month that gave companies, academics, and civil society a great opportunity to exchange ideas about cutting edge data security challenges and solutions.[18]

Of course, it is important to give consumers usable security tools, and encourage them to use these tools, so they can do their part to enhance their security. Two important consumer data security tools are two factor authentication and credit freezes. Two factor authentication has become more available, and easier to use, over the past few years. The FTC and other agencies at the state and local level need to do more to encourage consumers to use two factor authentication wherever available. And freezes on a consumer's credit report can prevent third parties from obtaining the credit report and opening a fraudulent account in the consumer's name. Credit bureaus allow adults to freeze their credit reports, but more should be done in this

[16] *See generally* FTC, Start with Security (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[17] *See* Careful Connections, *supra* note 12.

[18] FTC, PrivacyCon (Jan. 14, 2016), *available at* https://www.ftc.gov/news-events/events-calendar/2016/01/privacycon.

area to make credit freezes more usable and available, including to children who are particularly vulnerable to identity theft.

Once a consumer becomes a victim of identity theft, we need to provide usable tools to help them quickly deal with the consequences. Rapid action by consumers can help in two ways. First, consumers can stop further abuse of their identities. Second, reports from consumers are vital to local, state, and federal law enforcement agencies that can pursue identity thieves. The FTC recently unveiled a powerful new set of tools on the website identitytheft.gov that can help with all of this.[19] When consumers report identity theft through identitytheft.gov, the site now offers personalize steps that the consumer should take, based on her particular circumstances.[20] The site also automatically generates affidavits and letters that the consumer can send to credit bureaus, businesses, the police, and the IRS.[21] These new enhanced tools will help consumers more effectively prevent further damage to their identities and credit histories, and the notifications will help law enforcement agencies build cases against the thieves.

In closing, I want to say a special thank you to all of you for coming to this event. Your participation in this important discussion is part of the critical effort we must all engage in to improve data and device security, and help consumers better navigate this complex issue.

[19] *See* FTC, Identity Theft Recovery Steps, *available at* https://identitytheft.gov/ (last visited Feb. 8, 2016).

[20] *See* FTC, Press Release, FTC Announces Significant Enhancements to IdentityTheft.gov (Jan. 28, 2016), *available at* https://www.ftc.gov/news-events/press-releases/2016/01/ftc-announces-significant-enhancements-identitytheftgov.

[21] *See id.*