TELECOMMUNICATIONS INDUSTRY ASSOCIATION
TIA SPRING POLICY SUMMIT 2016
Washington, D.C.
March 9, 2016
Keynote Remarks of Commissioner Terrell McSweeny

Good afternoon. I am honored to be here today at your annual conference. I want to thank the Telecommunications Industry Association for the invitation, and for organizing this wonderful event.

Before I begin, I will start with my usual disclaimer that the views I express in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.

The Telecommunications Industry Association has had a long history of organizing industry members and entrepreneurs in the information and communications space. Your work is immensely helpful to me and my colleagues because we often look to industry to inform our decision-making process. Here in this room, we have experts who live and breathe information technology every day, so the combined expertise here is highly valuable to me as a policymaker.

So what does the FTC do, and why should you be interested in our work? The FTC was founded over 100 years ago to police unfair and deceptive practices in the economy. We pride ourselves on keeping pace with the marketplace, so when consumers shifted from analog to digital, we followed suit and began to use our existing authority to look at cases of unreasonable data security and deceptive privacy practices.

As we've developed an expertise in these issues, we have also become one of the lead agencies in working with our international partners on global data flows. Just last month, we announced an agreement with Europe to sustain trans-Atlantic data flows with the new US-EU Privacy Shield Framework.

As we become more globalized in the way we share our data, your organization, its member companies, and the FTC all share a common responsibility: to protect consumer privacy in our rapidly changing technological world. The explosion of innovation in the past decade has forever changed our society, allowing businesses to better service their customers, teachers to better educate their students, and cities to better handle public safety crises and improve how government functions.

In the drive to build smarter homes, cars, and cities, we have generated the creation of thousands of new and useful connected devices, leading to the so-called era of the "Internet of

Things" (IoT). According to some estimates, the number of connected devices is expected to reach 50 billion by 2020, with the potential to create an impact of up to $6.2 trillion annually by 2025.[1] Hewlett Packard last year released a report arguing that IoT devices are likely to become more ubiquitous in our everyday lives than mobile phones are today.[2]

This is especially likely as more and more IoT devices become embedded in our lives. Wearing an Internet-connected health monitor is now routine for many people, as is the ability to connect our homes. We have connected sprinkler systems, connected ovens, and connected vacuum cleaners, and each week it seems there's a new connected toy reaching the marketplace.

Alongside the many benefits that the Internet of Things delivers, we are also faced with the potential for malicious exploitations of the personal data we store in our devices. 60% of our devices have vulnerabilities in just the user interface alone, meaning there is well-founded room for concern when it comes to our privacy and security.[3]

Unfortunately, consumers are finding this out the hard way. Every year, the FTC receives hundreds of thousands of complaints related to privacy concerns, which consistently ranks at the top of the list of consumer complaints we receive. Last week, in fact, we revealed in our annual Consumer Sentinel report that identity theft was the second most reported consumer complaint in 2015, jumping by more than 150,000 in number, or up 47% from the previous year.[4] The Bureau of Justice Statistics estimates that 17.6 million Americans were victims of identity theft in 2014 – which is nearly 7% of the entire population in the U.S.[5]

As the nation's leading consumer protection agency, the FTC works tirelessly to combat identity theft and consumer concerns about privacy. A few weeks ago, we unveiled our new and improved IdentityTheft.gov website. Consumers who may be victims of identity theft can now use the one-stop site to make free personalized recovery plans, complete with pre-filled letters and forms, interactive guidance, and step-by-step instructions. These improvements will help

---

[1] Dave Evans, Cisco, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything* (Apr. 2011) at 3, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf; James Manyika et al., MCKINSEY GLOBAL INSTITUTE, *Disruptive technologies: Advances that will transform life, business, and the global economy* (May 2013) at 51, http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Business%20Technology/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx.

[2] Hewlett Packard Enterprise, *Internet of things research study* (2015) at 3, http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[3] *Id.* at 4-5.

[4] Press Release, Fed. Trade Comm'n, FTC Releases Annual Summary of Consumer Complaints (Mar. 1, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer-complaints.

[5] Erika Harrell, U.S. DEPT. OF JUSTICE, BUREAU OF JUSTICE STATISTICS, Victims of Identity Theft, 2014 (Sept. 2015) at 1, http://www.bjs.gov/content/pub/pdf/vit14.pdf.

victims gain faster, streamlined access to credit bureaus, local law enforcement, and the IRS, easing their road to recovery.[6]

The FTC also uses its consumer protection mandate to bring action against individuals and entities that enable or perpetrate these attacks. To date, we have brought over 50 privacy cases, 60 data security cases, and 130 spam and spyware cases.[7]

In August, we won a huge victory when the Third Circuit upheld the FTC's authority to bring our case against Wyndham Hotels and Resorts. We alleged that the hotel chain's poor security practices unfairly exposed consumers' financial information in a string of three breaches that amounted to more than $10.6 million in consumer loss.[8] Wyndham challenged our ability to bring this case and lost. The court ruled that our Section 5 authority covers the ability to prohibit unfair data security practices, affirming the FTC's role in carrying out our vital data security mission.

A few weeks ago, we also brought a case against a router company, ASUSTek Computer. In our complaint, we argued that the company's routers had flawed security systems and insecure cloud setups, leaving consumers' connected storage devices open for exploitation. Not only were customers' sensitive information exposed to the internet, but they were also left vulnerable to hackers who could turn off firewalls, change the settings from "private" to "public," and redirect consumers to malicious websites.[9]

These cases demonstrate our fervent belief that in the digital age, protecting consumers means maintaining safe and secure networks. It is increasingly necessary to ensure consumer protection goes hand in hand with technological innovation. If companies neglect security as they provide new innovations, the public's appetite for new technology will dampen.

At the FTC, we encourage businesses to embrace security by design. This means thinking about security at the earliest stages of the product's development and providing throughout its lifecycle. In our "Start with Security" guide targeted to the business community, we outline a host of methods designed to encourage companies to consider security at the onset,

---

[6] *See* Press Release, Fed. Trade Comm'n, FTC Announces Significant Enhancements to IdentityTheft.gov (Jan. 28, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/ftc-announces-significant-enhancements-identitytheftgov.

[7] Fed. Trade Comm'n, *Privacy and Data Security Update: 2015* (Jan. 2016) at 2, 4, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2015/privacy_and_security_data_update_2015-web_0.pdf.

[8] Memorandum Op., *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. 2015) at 6, https://www.ftc.gov/system/files/documents/cases/150824wyndhamopinion.pdf.

[9] *See* Compl., Fed. Trade Comm'n, In the Matter of ASUSTeK Computer, Inc. (Feb. 23, 2016), https://www.ftc.gov/system/files/documents/cases/160222asuscmpt.pdf.

including creating a culture of security within the company, crafting a multi-layered approach to security, encouraging solid password hygiene, and utilizing standard encryption techniques.[10]

It is not enough to put security safeguards in the beginning and hope for the best. Rather, we encourage entrepreneurs to check in frequently, keeping their security measures as up-to-date and proactive as possible. We have brought cases against companies that didn't improve their security features, including one particular matter where we challenged a company for failing to update their anti-virus software, leaving opportunities for data and information to be compromised.[11]

We are also encouraging industry to do more. Personally, I am a believer in the work of establishing relationships with security researchers, or "white hat hackers," to help companies find and fix problems before they can be exploited by criminals.

There is, of course, no one-size-fits-all approach to privacy and security. Reasonable security standards can vary between industry and product, and depends on a multitude of factors – including what kind of data is being collected, where it's being stored, and how often it's being gathered.

Still, there is a baseline of steps that companies can take to safeguard consumer data. Encryption is one such start. I commend the many companies that have defaulted to using this technique for the information and data they store.

However, I believe more can be done to encourage end-to-end encryption – which is a valuable data security tool for consumers. I am mindful of the important national debate between law enforcement and civil libertarians over the use of encryption. While I understand the national security and law enforcement arguments, I have yet to meet a technologist or developer that says backdoors are harmless or don't present a security problem for consumers.

Mandating backdoors and exceptional access systems will weaken consumer data security and chill innovation at a time when we can ill-afford it. Consumers are safer using

---

[10] Fed. Trade Comm'n, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015) at 1-3, https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf; *See also* Lesley Fair, ASUS case suggests 6 things to watch for in the Internet of Things (Feb. 23, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/02/asus-case-suggests-6-things-watch-internet-things; Fed. Trade Comm'n, *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[11] *See* Press Release, Fed. Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers Data (Mar. 27, 2008), https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx.

encrypted technologies. If we are ever going to have effective telemedicine, connected cars, or secure financial payment systems, we cannot also legislate vulnerabilities into our devices.

Furthermore, the technologies that allow for encryption are already in the marketplace. Mandated backdoors will only push these technologies overseas, or make it impossible for consumers to secure their data even while criminals continue to use available technologies or develop their own.

As the San Bernardino case brings this encryption debate under a national spotlight, I am reminded how important it is to bring all stakeholders to the table. We must learn to navigate these challenges together and continue the constructive dialogue between us as policymakers, and you as industry leaders. In our endlessly connected world, we must all work together to ensure that consumers are well protected from vulnerabilities that can leave all of our data and personal information exposed.

Thank you again for having me here today. I'm happy to answer any questions.