KEYNOTE REMARKS OF COMMISSIONER TERRELL MCSWEENY[1]
Consumer Protection in the Age of Connected Everything
New York Law School, New York, NY
February 3, 2017

Good afternoon, everyone. Thank you, Professor Elvy, for that generous introduction. I'm happy to be here today. Today I am going to talk about how a 100-year-old federal consumer protection agency is going about protecting consumers in the digital age.

As we all know, the Internet of Things is growing rapidly. Thanks to the increasing processing capacity of increasingly smaller circuits, we're now hooking up everything from light bulbs to toothbrushes. Today, there are twice as many Internet-connected devices as people on the planet. By 2020, that number is expected to grow to thirty-eight *billion*.[2] By 2025, the value of these devices and the ecosystem they operate in is estimated to exceed four *trillion* dollars per year.[3]

It's not just the number of devices and their value to the economy that is expanding: increasingly, manufacturers are experimenting with different types of devices to connect to the Internet of Things. These range from the fantastic – self-driving cars and drones – to the mundane: toasters and hairbrushes.

Thanks to all this connectivity, the Internet is no longer just a communications network. It is a global, ambient, always-on system that is a vital connection to conveniences of modern life. It is no longer just a sector of our economy – it now touches nearly every sector. We have never seen this much change in this short a period on this many fronts – and it poses some real challenges for policy makers, regulators, and enforcers.

How do we optimize rapid innovation to remain a world leader in the development of new technology while mitigating some of the consequences of all this change – addressing digital divides, insuring data sets are high quality and representative, increasing digital readiness, and protecting jobs, privacy and security? How do we respond to changing social norms around data sharing? How do we make sure that consumers, who want to benefit from all of this innovation, have choices and transparency within it? What additional protections do consumers need? As the technology gets smarter, how and when do we protect human agency?

The Federal Trade Commission is at the forefront of these issues. As many of you know, the FTC is the nation's primary federal law enforcement agency for consumer privacy and data

---

[1] The views expressed in this speech are my own and do not necessarily reflect those of the Commission or any other Commissioner.
[2] Press Release, Juniper Research, 'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020 (July 28, 2015), https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.
[3] JAMES MANYIKA ET AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS 7 (McKinsey Global Institute, 2015), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

security. We are a relatively old agency, established more than 100 years ago. When the Commission was founded by the Wilson administration, the primary concern was countering the concentrated economic power of trusts and monopolies.

While the FTC is first and foremost a law enforcement agency, it was also charged with shaping policy for a competitive market. Today we do that by issuing reports, holding workshops, making ourselves available to relevant stakeholders, and through the cases we bring. The Commission also has a uniquely broad mandate to keep the marketplace fair for competition and consumers. We have used our flexible power under Section 5 of the FTC Act to keep pace with innovation and the market as it develops. We've followed consumers as they have moved from consuming in the brick-and-mortar world to the digital one.

The Commission recognizes that consumers benefit from connectivity in all aspects of their lives. Connectivity can increase productivity and convenience, with devices that allow consumers to do anything from monitor their health to order laundry detergent with a request to a smart butler. But increased connectivity means more points of access for hackers and other malicious actors who exploit low-cost hardware equipped with inadequate security measures.

A proliferation of devices without screens or user interfaces mean that consumers may not be provided with adequate privacy notices, and that relatively intimate data may be gathered from them without their knowledge. Sometimes, even by companies with whom they have no direct relationship.

Manufacturers and service providers are finding ways to track consumers across multiple devices, often without disclosing they are doing so.[4] The FTC just released a report on so-called cross-device tracking. Some of this tracking – for example, listening to an audio book on multiple devices – is quite useful and fairly obvious to users. But much of it occurs without our knowledge and often companies combine the information from a consumer's multiple devices to create a detailed, personal profile that is sold to third parties, mostly for personalized advertising.[5]

The Commission's report found that many companies also are not explicitly discussing their cross-device tracking practices in their privacy policies. As companies increasingly track consumers across not only desktops and smartphones but other smart devices – like TVs – it is important that companies not only reassess their approaches to privacy but also simplify consumer choices wherever possible and get affirmative consent from consumers before cross-device tracking on sensitive topics like health, finances, geolocation, and children's information.

The FTC has previously issued a report on data brokers – companies that collect consumers personal information and resell that information to others – and the role that they can

[4] FED. TRADE COMM'N, CROSS-DEVICE TRACKING: A STAFF REPORT (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
[5] *Id.*

play in combining and analyzing data about consumers to make potentially sensitive inferences.[6] In that report, the FTC also recommended providing consumers with more chances to opt-out and with the affirmative power to consent before sensitive information is collected and shared with data brokers. These recommendations, I believe, remain important but will likely require legislation to implement.

As our connections deepen and widen, thanks to IoT, offering and honoring people's choices about their data – particularly their sensitive data – is becoming more complex. But that is no reason not to offer the choice – and the control that comes with it – and arguably in this environment it is more important than ever.

Recent FTC privacy cases have focused on this issue. In *Turn*, a digital advertising company settled charges that it misled consumers that they could reduce the extent to which the company tracked them.[7] In *InMobi*, the FTC alleged that the mobile advertising network was using technology to track geolocation even when consumers had denied permission to access their location information.[8]

Compounding the privacy concerns raised by cross-device tracking is that personal data, once collected, may not always be properly secured. We have all seen the high-profile hacks of major companies, including high profile attacks on IoT like cars and medical devices. These have far-reaching effects. In a recent survey of American households, one in five reported being victimized by security breaches.[9]

It's no wonder then, that consumer confidence in the security and privacy of their data is low. In the same survey, eighty-four percent had concerns about online privacy and data security.[10] And in a recent Pew survey 91 percent of American consumers said they felt they have lost control of their data.[11] Consumer concern is heightened by business practices that often leave them in the lurch: IoT products may not have patch support or the same life expectancy as other connected products, and these limitations are not always communicated clearly to consumers.

These concerns have real-life consequences that can affect consumer demand for IoT. Almost half of consumers surveyed said they are less likely to use certain online services because of their privacy concerns,[12] and there is evidence that those same worries are slowing the

---

[6] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[7] *Turn, Inc.*, Matter No. 1523099 (Dec. 20, 2016) (proposed consent), https://www.ftc.gov/enforcement/cases-proceedings/152-3099/turn-inc-matter.

[8] *United States v. InMobi Pte Ltd.*, No. 3:16-cv-3474 (N.D. Cal. filed June 22, 2016), https://www.ftc.gov/enforcement/cases-proceedings/152-3203/inmobi-pte-ltd.

[9] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMMS. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[10] *Id.*

[11] Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RESEARCH CTR.: FACTTANK (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[12] Goldberg, *supra* note 8.

pace of IoT adoption.[13] Consumers are repeatedly saying that data security is a top barrier to purchasing connected devices. In other words, good security is good for business.

For many, the risks posed by insecure devices may seem trivial: what does it matter if a hacker can see what color settings I like on my IoT lightbulb? But security of devices isn't just about individuals. With billions of devices connected to the Internet, the risk for abuse and destructive behavior is tremendously high. We've already seen denial-of-service attacks launched from IoT devices like routers and internet-connected video cameras. These attacks have the potential not just to disable websites but also critical infrastructure. Insecure devices connected to the Internet can be exploited in a matter of minutes.

And insecure IoT devices are especially vulnerable to ransomware attacks, which will hold hostage not only our data, but our cars, refrigerators, or factories. Helping consumers mitigate IoT ransomware attacks is something enforcers, policy-makers and industry are just beginning to grapple with – but I predict this will be a growing consumer protection issue in the future.

Sometimes the most harmful attacks go unnoticed or don't immediately seem harmful to an individual consumer. What can a homeowner do if her router is used in a denial-of-service attack? Will she even know beyond noticing a degredation in quality of her connection? Or might the inconvenience of fixing the security breach outweigh the harm she herself perceives?

That's why the FTC is active in this field. We have taken enforcement actions against hardware producers whose security flaws put hundreds of thousands of customers at risk. We've held companies accountable if they make deceptive claims about their security practices.

Just in the past few years, we've taken enforcement actions against two router manufacturers – D-Link[14] and ASUS[15] – who we alleged had inadequate security practices; and against TRENDnet,[16] an electronics company who we alleged misrepresented the security of their video cameras. These and other FTC security cases have alleged security failures such as: hard-coded or default login credentials; command injection vulnerabilities; exposure of a private key; transmission or storage of login credentials in clear text; and failure to perform security testing or reviews of software.

The Commission also launched the "Start with Security" Initiative in 2015.[17] We want companies to think about consumer privacy and security before it ever gets to the point of a data breach or FTC enforcement.

---

[13] ACCENTURE, IGNITING GROWTH IN CONSUMER TECHNOLOGY (Jan. 5, 2016), https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf.
[14] *FTC v. D-Link*, No. 3:17-cv-00039 (N.D. Cal. filed Jan. 5, 2017), https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link.
[15] *ASUSTeK Computer Inc.*, No. C-4587 (July 18, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.
[16] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[17] Fed. Trade Comm'm, Start with Security (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

So we're asking IoT companies to consider ten simple steps to secure consumer data:

- Start with security – build products with security in mind;
- Control access to data sensibly – and think about whether you really need to collect and keep all of the data;
- Require secure passwords and authentication;
- Store sensitive personal information securely and protect it during transmission;
- Segment your network and monitor who's trying to get in and out;
- Secure remote access to your network;
- Apply sound security practices when developing new products;
- Make sure service providers implement reasonable security measures;
- Put procedures in place to train employees and to keep security current and address vulnerabilities that may arise; and
- Secure paper, physical media and devices.

These may sound straightforward, but time and again I see cases where even these basic principles haven't been followed. So part of the solution to this lies with us at the Commission helping to educate businesses about good, common-sense privacy practices. We are dedicated to fostering a positive security culture for IoT devices because we believe that when questions of security are primary in product development and marketing, everybody wins.

The Commission is also using new tools – like competitions – to stimulate innovations to help consumers. In January we launched our IoT Home Inspector Challenge, offering a $25,000 prize for new systems to help consumers secure their home networks and IoT.[18]

But it's not just about business: we're working to educate consumers as well. Through decades of computer use, many home users understand the basics of digital hygiene. Things like "don't open suspicious links or download unknown files," and "keep a current anti-virus program." But what proactive measures should they take when their computer is inside a bagel toaster or a children's toy?

A consumer may be justified in treating it the same way she treats any other appliance or toy: plug it in and forget about it. Here, it is critical that consumers understand the additional risks they face when using Internet-connected devices in their homes and know what steps they need to take to protect themselves.

Security comes at a cost, and in some cases, consumers may wish to pay less for a less-secure device. That is their right, and the free market will provide them those options. But decisions about cost and security must be made freely, with all the relevant information. Businesses must take proactive steps to provide clear and accurate information on what data is being collected, how it is used, and for how long. Consumers also must have information on the expected lifetime of the device, software support, and how to receive security updates, if those are provided.

[18] Press Release, Fed. Trade Comm'n, *FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices* (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security.

For instance, I have real concerns about Internet-connected devices that are "bricked" without warning or notice to the consumer. This is especially worrisome as devices become more central to consumers' day-to-day lives. A consumer might buy an analog thermostat expecting it to last ten or more years, and she might understandably have the same expectation of its IoT equivalent. Manufacturers must either make clear to consumers what to expect from their devices or conform to reasonable consumer expectations. The FTC is watching this area closely.

The FTC has done much to bolster consumer confidence and ensure industry compliance with best practices. But our work alone is not enough. The rapid spread of connected devices into the most far-flung and intimate aspects of daily life means that the FTC alone cannot provide all the needed tools to maintain a fair and open market.

While I can only speak for myself, I believe it would be a strong disservice to both consumers and industry to step back from the progress we've made in recent years. Progress that supports innovation and technology development. Progress that makes the marketplace fair for consumers *and* competitors, as was intended when the FTC was founded those many years ago.

There are many areas for improvement with IoT devices, and an industry-wide need to find effective solutions for security and privacy. The FTC, along with Congress and the Administration, must work together with expert regulators – like the FCC, FDA, FAA, and NHTSA – and with industry and consumer groups to develop a sustainable model for integrating IoT into our lives as a productive and positive force and not as obstacles or frustrations. I still believe the surest way to set clear industry-wide standards would be through the passage of comprehensive data security and privacy legislation.

The creation, storage, and use of all the data generated by our hyperconnectivity can lead to overt challenges – like discrimination – and more subtle ones. The data we create feed algorithms that affect consumer choice, implicating laws and public policy along the way. As the machines running algorithms get smarter, this technology raises questions regarding the roles of human beings in decision making – what choices do we want to hang onto and which ones are we comfortable essentially automating or turning over to artifical intelligence?

For years FTC and privacy advocates have talked about privacy by design – and now security by design. I think it is time for a conversation with industry about data governance and, ultimately, ethics by design. The basic requirements should include (1) transparency; (2) choice; (3) explainability – understanding what tech is doing; (4) testing; (5) data quality; and (6) remediation or mitigation when necessary.

There is a new Administration and a new Congress in Washington – and new leadership at the FTC, but I see no need to politicize consumer protection. Our Commission is historically bipartisan and independent – devoted to protecting the markets and the innovators and consumers within them from unfair and deceptive acts and practices. That mission is as important today as it was 100 years ago.

Thank you.