Raising the Standard: Bringing Security and Transparency to the Internet of Things?

Open Technology Institute
New America
July 26, 2018

Remarks of Commissioner Rebecca Kelly Slaughter[1]

Thank you to the Open Technology Institute and the New America Foundation for hosting today's important event. It is an honor to be here and I welcome the opportunity to talk about the need for collaborative action to safeguard consumer trust and security in the evolving world of IoT.

The year 2017 brought an estimated 8.4 billion connected things to the world.[2] That number is expected to reach more than 20 billion by 2020.[3] By 2025, the value of these devices, and the ecosystem in which they operate, is estimated to exceed four *trillion* dollars per year.[4] These devices touch all sectors – the military, manufacturing, healthcare, utilities, autos, and of course, the home. In fact, we know that consumer applications are the largest and fastest-growing category of connected devices.[5]

Like most of you, I follow these developments not just from a policy perspective but as a consumer.

I have personally benefitted from the early adoption of some basic connected devices – I love being able to use my smart watch to pay for things when I inevitably forget my wallet. I truly appreciate being able to control my thermostat from my phone when I inevitably forget to set it properly (perhaps you can sense a theme in my life?)

Clearly, I would make good use of being able to look inside my "smart" fridge from my phone as I trudge down the milk aisle.[6] (Or the ice cream aisle). And as someone who spends too

---

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

[2] Press Release, Gartner Inc., *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.

[3] *Id*.; 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.

[4] JAMES MANYIKA ET AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS, at 7 (McKinsey Global Institute, 2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[5] *See supra* n. 2.

[6] Brian X. Chen, *To Invade Homes, Tech Is Trying to Get in Your Kitchen*, NY Times, (Mar. 25, 2018), *available at* https://www.nytimes.com/2018/03/25/technology/smart-homes-tech-kitchen.html ("Samsung, the No. 1 phone maker that popularized smartphones with extra-large screens, this year unveiled a new version of Family Hub, a

much time on the road, the potential for connected cars to bring about less traffic, fewer accidents,[7] and one day less driving altogether[8] is very tantalizing.

As a parent, I am especially sensitive to the combination of opportunity and risk posed by connected devices for children. My kids ask our home assistant to set timers that help mediate disputes over sharing toys, and I have learned the hard way that these same devices can be asked to play some crude playground songs (to my children's delight and my horror). As someone balancing a variety of disparate bedtimes at home, it has certainly crossed my mind to just ask Alexa to be the one to read Good Night Moon for the fifth time.[9] And the educational potential of interactive connected toys is almost limitless.

But so are the risks. Imagine if someone hacked into my baby monitor and started spying on (or talking to) my baby? What if a company were collecting data on my children's conversations with their connected toys without our knowledge or consent? These aren't random hypotheticals – there has been public reporting on both of these cases.[10]

Those examples point to the bigger issue here: with all of this cutting edge and truly transformative technology comes legitimate concern about the potential risks these devices pose to our safety, our autonomy, and our privacy. The many benefits of IoT devices may be delayed or foreclosed if consumers cannot trust them. Building that trust starts with two fundamental components: 1) ensuring that the devices are reasonably secure and (2) ensuring that consumers have a clear and accurate picture of what data their devices collect and how that data is stored and used. Poorly designed IoT devices, and poor privacy controls by their manufacturers, jeopardize the privacy of their users and create opportunities for attackers to steal data or assume device control.

The hacking of connected devices can cause profoundly personal risks that can literally follow us into our homes. The New York Times recently reported a new trend in domestic abuse cases tied to the rise of smart home technology.[11] Internet-connected locks, speakers, thermostats, lights and cameras are now also being used as a means for harassment, monitoring, revenge and

---

smart refrigerator that understands voice commands and sports a 21.5-inch touch screen. The appliance has three built-in cameras, which can beam live images of the fridge's contents to a phone.").

[7] FED. TRADE COMM'N, THE CONNECTED CARS WORKSHOP: THE FEDERAL TRADE COMMISSION STAFF PERSPECTIVE, (Jan. 9, 2018), https://www.ftc.gov/reports/connected-cars-workshop-federal-trade-commission-staff-perspective.

[8] CBInsights, *33 Industries Other Than Auto That Driverless Cars Could Turn Upside Down*, CBInsights Research Briefs, (May 24, 2018), *available at* https://www.cbinsights.com/research/13-industries-disrupted-driverless-cars/ ("It's all but a certainty that autonomous or driverless vehicles will be widely used in the United States at some point over the next two decades. Already, over two dozen major corporates including Google, Apple and Mercedes Benz are hard at work building their own self-driving vehicles.").

[9] Emily DeJeu, *6 Ways The Amazon Echo Will Transform Your Child's Bedtime Routine*, The Baby Sleep Site, (last visited July 26, 2018), *available at* https://www.babysleepsite.com/sleep-training/amazon-echo-bedtime-routine/.

[10] Ryan Grenoble, *Hacked Baby Monitor Caught Spying On 2-Year-Old Girl In Texas*, Huffington Post, (Aug. 13, 2013), *available at* https://www.huffingtonpost.com/2013/08/13/hacked-baby-monitor-houston-texas-parents_n_3750675.html; Lauren Walker, *Privacy Advocates Call Talking Barbie 'Surveillance Barbie,'* Newsweek, (Mar. 13, 2015), *available at* https://www.newsweek.com/privacy-advocates-want-take-wifi-connected-hello-barbie-offline-313432.

[11] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, NY Times, (June 23, 2018) *available at* https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

control.[12] Imagine trying to break free from an abusive relationship in which your abuser not only imprisons you with physical and emotional intimidation—but also uses your very home to control and undermine you. It is horrifying, and yet terrifyingly real for too many people.

While the immediate risk may seem less concrete in the area of privacy than security, the former is no less important an issue for connected devices. Our law and our rhetoric often treat the two issues as distinct, with privacy having to do with the protection of information a user would prefer not to share and security referring to the protection of data the release of which could risk user safety. But the world of IoT shows us that the line between privacy and security is not bright; it is not even blurry. The two concepts are overlapping and intrinsically related: there can be no assurance of privacy without sound security and most security vulnerabilities pose threats to privacy.

To play out the domestic violence example above: if someone has a connected home alarm, the device manufacturer may well be collecting data on the time and frequency of its use, and sharing or selling that data to a third party. Without adequate privacy policies that address data collection, retention, storage and sharing, an abusive partner could request, buy, or even steal that information, and the user's security is jeopardized. So it is important that consumers have meaningful, accurate and understandable information about their device security, as well as data sharing, in order to make informed decisions.

We are at a critical point in the IoT era in terms of getting privacy and security right. At the precipice of exponential growth, we have the opportunity both to thoughtfully develop products that start and stay secure, and to educate consumers early on about how to assess the risks of connected devices, how to choose brands that take privacy and security seriously, and how to maintain device security with patches over the lifespan of the product.

I cannot overstate the importance of getting this right, now. If we build appropriate security and disclosure standards into the infrastructure of this emerging ecosystem, we will not only protect consumers better from the start, we will avoid having to rebuild and redesign the rules of the road from scratch – an outcome that would be far more disruptive to both consumers and innovative product designers.

Unfortunately, there are a few basic troublespots the FTC has observed in the marketplace for connected devices.

First, we're continuing to see some very basic failures in product design and pre-release testing. We encourage and expect companies to consider security at the outset, understand well-known vulnerabilities affecting their class of products, and take advantage of low-cost, widely available measures to protect against them. I'm particularly concerned by easily avoidable problems, for example connected devices that come with default passwords (or don't require a password at all).

Second, while pre-release testing is important, we understand that such testing will not catch all problems. Vulnerabilities will occur that companies may not have foreseen. Companies should make sure that, among other things, they have a process in place to identify and address credible alerts about potential vulnerabilities.

Third, once vulnerabilities are identified after a product's release, there are often challenges in the deployment of updates and patches. In some cases, patches may be available, but not

[12] *Id*.

deployed to consumers in a timely manner. In other cases, consumers themselves may be overwhelmed about how to keep up with patches. In yet other cases, companies may not support devices at all after a certain period. In all of these cases, devices are left compromised. Companies need to think critically from the get-go about how to maintain security over the lifespan of the device and be on the same page with consumers about the length of that lifespan.

We all need to work together to troubleshoot these issues. The FTC has an important role to play in prodding industry to address these issues, as I will detail in a minute. But our work is substantially complemented by the development of robust, meaningful assessment tools by the public and industry – the Digital Standard aims to be just such a tool.

The **Digital Standard,** first established in the spring of 2017, presents an opportunity for multiple stakeholders to create and continually refine a testing system to evaluate how well products are meeting consumer expectations regarding information security and privacy.[13]

The FTC has long been a supporter of self-regulatory standards, provided that those efforts genuinely raise the bar for the products to which they relate and that reliance on those standards gives consumers material information. The concept of the Digital Standard is particularly promising because it has a consumer-facing deliverable – in other words, it is designed to be news consumers can actually use, rather than the type of legalese too many people have become accustomed to clicking through.

I am hopeful that clear, reliable information about device security will allow consumers to make informed decisions about the products they put in their homes before the point of purchase – and in that way meaningful security can deliver a competitive edge to responsible producers.

On the other side of the equation, product evaluations using the Digital Standard or similar criteria should help to encourage manufacturers to, as we like to say at the FTC, start with security. Consumer Reports' evaluation of smart TVs using the Digital Standard found that a relatively unsophisticated hacker could change channels, play offensive content, or crank up the volume on millions of smart TVs. No doubt these findings were as informative to manufacturers as they were to consumers.[14]

So what additional roles does the FTC play in this collaborative space?

Perhaps most obviously, we have an important enforcement mission, the exercise of which promotes security and privacy. We've brought a number of cases regarding connected devices, including routers,[15] baby-monitors,[16] smart TVs,[17] and most recently, connected toys.[18] And,

---

[13] *See* https://www.thedigitalstandard.org/ (last visited July 26, 2018).

[14] Consumer Reports, *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds*, (Feb. 7, 2018), *available at* https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/.

[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] *FTC v. VIZIO, Inc., and VIZIO Inscape Services, LLC.*, No. 2:17-cv-00758 (D.N.J filed Feb 3, 2017), https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.

when companies claim that they have adopted self-regulatory standards, we can hold them liable under our deception authority if they do not live up to those commitments.

The FTC also functions as a facilitator of security innovation through research, reports, data analysis, and numerous workshops, symposiums and conferences. Recent workshop topics include smartTVs, drones, connected cars, and EdTech. We also routinely partner with other governmental agencies, co-hosting events and providing comment.

The FTC also challenged the public to create a technical solution that consumers could use to guard against security vulnerabilities in IoT devices in their homes.[19] With the assistance of an expert panel of five judges, the FTC awarded top prize to a mobile app that would scan a user's home Wi-Fi and Bluetooth networks to identify connected devices, flag devices with vulnerabilities and provide instructions on how to update each device's out-of-date software.

I am proud of the work the FTC is doing in this area, but I also think we should always consider what we can do better. One great idea – supported by former Commissioner McSweeny – is to elevate our technological expertise into a formal Bureau of Technology at the FTC. I believe that would be a valuable way to ensure we have a deep bench of technologists who can help spot issues and evaluate cases across our mission – in both competition and consumer protection.

And, in the spirit of self-reflection, the FTC is also hosting a series of public hearings this fall on 21st century challenges to our missions of consumer protection and competition.

We are seeking public comment on these hearings and I encourage you all to consider submitting your thoughts, in particular your observations of challenges and opportunities in the IoT space, as well as your views on how our responsibility to protect consumers by promoting privacy and security might intersect with our mission to promote competition.

Thank you again to New America and OTI for hosting this event and I look forward to hearing from the group of true experts to discuss collaboration furthering security in the IoT space.

---

[18] *U.S. v. VTech Electronics Ltd. et al.*, No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited.

[19] Press Release, Federal Trade Commission, *FTC Announces Winner of its Internet of Things Home Device Security Contest*, (July 26, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.