NEW YORK LAW SCHOOL

NYLS Law Review

Vols. 22-63 (1976-2019)

Volume 62
Issue 2 *Exploring the Things in the Internet of Things: Implications For Business, Consumers, and the Law*

Article 1

January 2018

Consumer Protection in the Age of Connected Everything

Terrell McSweeny

VOLUME 62 | 2017/18

TERRELL MCSWEENY

Consumer Protection in the Age of Connected Everything

62 N.Y.L. Sch. L. Rev. [•] (2017–2018)

ABOUT THE AUTHOR: Terrell McSweeny is a Commissioner of the Federal Trade Commission (FTC). Prior to joining the FTC in 2014, McSweeny served as Chief Counsel for Competition Policy and Intergovernmental Relations for the U.S. Department of Justice Antitrust Division. She joined the Antitrust Division after serving as Deputy Assistant to President Barack Obama and Domestic Policy Advisor to Vice President Joe Biden from January 2009 until February 2012, advising on policy in a variety of areas, including health care, innovation, intellectual property, energy, education, women's rights, criminal justice, and domestic violence. McSweeny's government service also includes her work as Senator Joe Biden's Deputy Chief of Staff and Policy Director in the U.S. Senate, where she managed domestic and economic policy development and legislative initiatives, and as Counsel on the Senate Judiciary Committee, where she worked on issues such as criminal justice, innovation, women's rights, domestic violence, judicial nominations, immigration, and civil rights. McSweeny delivered this article as a speech at a symposium titled "Exploring the Things in the Internet of Things: Implications for Business, Consumers, and the Law," which took place at New York Law School on February 3, 2017.

The Internet of Things (IoT)[1] is growing rapidly. Thanks to the increasing processing capacity of ever-smaller circuits,[2] we are now hooking up to the internet everything from light bulbs to toothbrushes.[3] In 2015, there were twice as many IoT devices as people on the planet.[4] By 2020, that number of devices is expected to grow to more than thirty *billion*.[5] By 2025, the value of these devices and the ecosystem they operate in is estimated to exceed four *trillion* dollars per year.[6]

IoT devices are not only expanding in number and increasing in value to the economy, but also diversifying in kind. More and more, manufacturers are experimenting with different types of devices to connect to the IoT.[7] These range from the fantastic, like self-driving cars and drones, to the mundane, like toasters and hairbrushes.[8] 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.[9] It is no longer just a single sector of our

1. While no universal definition exists, the IoT generally refers to scenarios where "objects, sensors and everyday items not normally considered computers" are connected to the internet and have computing capabilities, which allows "these devices to generate, exchange and consume data with minimal human intervention." Karen Rose et al., Internet Soc'y, The Internet of Things: An Overview 15 (2015), https://www.internetsociety.org/sites/default/fileswp-content/uploads/2017/08/ISOC-IoT-Overview-20151014_020151221-en.pdf.

2. *Id.* at 13 & 24 n. 21.

3. Eric A. Taub, *Diving Headfirst into the Internet of Things*, N.Y. Times (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/diving-headfirst-into-the-internet-of-things.html.

4. In 2015, there was an installed base of 15.4 billion IoT devices, Sam Lucero, IHS Tech., IoT Platforms: Enabling the Internet of Things 5 (2016), https://cdn.ihs.com/www/pdf/enabling-IOT.pdf, while the world population was 7.3 billion people. *The World Population Prospects: 2015 Revision*, United Nations Dep't Econ. & Soc. Aff. (July 29, 2015), http://www.un.org/en/development/desa/publications/world-population-prospects-2015-revision.html.

5. Lucero, *supra* note 4.

6. James Manyika et al., McKinsey & Co., The Internet of Things: Mapping the Value Beyond the Hype 2, 7 (2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (follow "Full Report (PDF–3MB)" hyperlink).

7. *See* Louis Columbus, *Roundup of Internet of Things Forecasts and Market Estimates, 2016*, Forbes (Nov. 27, 2016, 1:06 PM), https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#773724fc292d ("By 2017, 60% of global manufacturers will use analytics to sense and analyze data from connected products and manufacturing and optimize increasingly complex portfolios of products.").

8. Lee Rainie & Janna Anderson, Pew Research Ctr., The Internet of Things Connectivity Binge: What Are the Implications? 2, 15 (2017), http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/06/06115754/PI_2017.06.06_Future-of-Connectivity_FINAL.pdf.

9. *See generally* James Manyika & Charles Roxburgh, McKinsey Glob. Inst., The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity (2011) https://www.mckinsey.com/industries/high-tech/our-insights/the-great-transformer (follow "Full Report (PDF–230KB)" hyperlink) (discussing how the internet drives social and economic growth).

economy; it now touches nearly every sector.[10] We have never seen this much change in this short a period on this many fronts, and it poses real challenges for policy makers, regulators, and enforcers.[11]

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? How do we address digital divides, ensure data sets are high quality and representative, increase digital readiness, and protect 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 technology gets smarter, how and when do we protect human agency?

The Federal Trade Commission (FTC) is at the forefront of these issues.[12] The FTC is the nation's primary federal law enforcement agency for consumer privacy and data security.[13] It is a relatively old agency, established in 1914 by President Woodrow Wilson.[14] At its inception, the agency's primary concern was countering the concentrated economic power of trusts and monopolies.[15] Over time, the mission of the FTC expanded to include protecting consumers from unfair and deceptive acts and practices.[16] As modern consumers migrated online, the FTC followed, adapting to protect consumers in the digital age.[17]

The FTC influences policy and practices by bringing enforcement actions against companies in violation of the law, issuing reports, holding workshops, and making itself available to relevant stakeholders.[18] The FTC also has a uniquely broad mandate

10. *Id.* at 3 ("The [i]nternet has enabled fundamental business transformations that span the entire value chain in virtually all sectors and types of companies—not just online ones.").

11. *See id.* at 3, 9.

12. *See generally* Fed. Trade Comm'n, Privacy & Data Security Update: 2017 (2018) [hereinafter Privacy & Data Security Update], https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (examining a variety of tools the FTC uses to protect consumers' privacy and personal information).

13. *See id.* at 1; *see also About the FTC*, Fed. Trade Commission, https://www.ftc.gov/about-ftc (last visited Apr. 1, 2018) [hereinafter *About the FTC*].

14. *Our History*, Fed. Trade Commission, https://www.ftc.gov/about-ftc/our-history (last visited Apr. 1, 2018) [hereinafter *Our History*].

15. *See About the FTC*, *supra* note 13.

16. *See id.*

17. *See generally* Privacy & Data Security Update, *supra* note 12 (summarizing the FTC's privacy and data security work in 2017).

18. *Id.* at 1; *see also, e.g.*, Lorrie Cranor, *FTC Goes to DEF CON*, Fed. Trade Commission: Tech@FTC (Aug. 1, 2016, 5:18 PM), https://www.ftc.gov/news-events/blogs/techftc/2016/08/ftc-goes-def-con (explaining how FTC staff attend security and hacker conferences to learn from privacy and security researchers, inform researchers of the agency's interests, and encourage researchers to contact the agency); Lesley Fair, *"Start with Security" Starts in San Francisco*, Fed. Trade Commission: Bus. Blog (Aug. 19, 2015, 11:33 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/start-

to keep the marketplace fair for competition and consumers.[19] It uses its flexible power under Section 5 of the FTC Act[20] to keep pace with innovation and the market as it develops.[21]

Consumers benefit from connectivity in all aspects of their lives.[22] For example, connected devices allow today's consumers to do anything from monitor their health to order laundry detergent.[23] Increased connectivity, however, means more points of access for hackers and other malicious actors who exploit low-cost hardware equipped with inadequate security measures.[24]

Moreover, a proliferation of devices without screens or user interfaces means that consumers may not be provided with adequate privacy notices and that relatively intimate data may be gathered from consumers without their knowledge.[25] Increasingly, manufacturers and service providers are finding ways to track consumers across multiple devices, often without disclosing they are doing so.[26] Some of this tracking—for example, listening to an audio book on multiple devices—is quite useful and fairly obvious to users.[27] But much of the tracking occurs without

---

security-starts-san-francisco (discussing a series of free events hosted by the FTC as part of its "Start with Security" initiative, designed to help businesses learn about data security).

19. Privacy & Data Security Update, *supra* note 12, at 1.

20. Section 5 of the FTC Act provides that "[t]he [FTC] is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(2) (2012).

21. Privacy & Data Security Update, *supra* note 12, at 1, 17–18.

22. Elizabeth Gasiorowski-Denis, *How the Internet of Things Will Change Our Lives*, Int'l Org. for Standardization (Sept. 5, 2016), https://www.iso.org/news/2016/09/Ref2112.html (exploring the benefits of connectedness and IoT devices, such as "having better information [and] more control and insight into the everyday things that we need to function").

23. *See, e.g.*, Rose et al., *supra* note 1, at 8; Andrew Gebhart, *What is Alexa?*, CNET (July 26, 2017, 1:45 AM), https://www.cnet.com/news/what-is-alexa/.

24. *See* Fed. Trade Comm'n, Start with Security: A Guide for Business 7–12 (2015) [hereinafter Start with Security], https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (providing businesses with guidance on data security based upon lessons learned from past FTC cases).

25. *See* Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 22 (2015) [hereinafter Internet of Things: Privacy & Security in a Connected World], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (providing recommendations for privacy and security measures associated with the IoT).

26. *See* Fed. Trade Comm'n, Cross-Device Tracking 8 (2017) [hereinafter Cross-Device Tracking], 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 (examining ways to apply the FTC's privacy principles to cross-device tracking). *See also* Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (2014) [hereinafter Data Brokers], https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf (summarizing the results of a study conducted by the FTC on the data collection practices of certain data brokers).

27. Cross-Device Tracking, *supra* note 26, at i, 5.

consumer knowledge, and often, companies known as "data brokers" combine information from a consumer's separate devices to create a detailed, personal profile with potentially sensitive inferences.[28] Data brokers then sell that profile to third parties, mostly for personalized and targeted advertising.[29]

As tracking consumers across a multitude of smart devices, including smartphones, and even televisions, increases, it is important that companies reassess their approaches to privacy, simplify consumer choices wherever possible, and obtain affirmative consent from consumers.[30] The FTC further recommends that companies protect against unfettered information aggregation by data brokers by providing consumers with more chances to opt-out of data collection and with the choice to affirmatively opt-in before sensitive information is collected and shared.[31]

As IoT-enabled connectivity deepens and widens, offering and honoring consumers' choices about their data becomes more complex and more important.[32] Recent FTC enforcement has focused on ensuring consumers have adequate notice about and choice of when their sensitive information is collected and used.[33]

For example, in *Turn, Inc.*, a digital advertising company settled charges that it misled consumers into thinking consumers could reduce the extent to which the company tracked them.[34] Turn's privacy policy informed consumers that they could prevent targeted advertising[35] by using browser settings to block or limit cookies;[36]

28. Data Brokers, *supra* note 26, at iv–v, 11–18.

29. *Id.* at 26–30.

30. Cross-Device Tracking, *supra* note 26, at 15.

31. *See id.* at 13–15. These recommendations remain important but will likely require legislation to implement. *See* Data Brokers, *supra* note 26, at viii–ix, 49.

32. *See* Cross-Device Tracking, *supra* note 26, at 15–16.

33. *See* Privacy & Data Security Update, *supra* note 12, at 2, 5–6.

34. No. 152-3099, 2016 WL 7448417 (F.T.C. Dec. 14, 2016); *FTC Approves Final Consent Order with Online Company Charged with Deceptively Tracking Consumers Online and Through Mobile Devices*, Fed. Trade Commission (Apr. 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-consent-order-online-company-charged [hereinafter *FTC Approves Final Consent Order*].

35. Targeted advertising is accomplished through tracking internet users:

> When a person views a product on a retail Web site, the user's browser submits information about what he is looking at to third-party advertising networks, such as doubleclick.net. The information is stored in a browser cookie . . . . Users can clear these cookies periodically to clear out their record with ad networks. If that person later clicks on another site in the same advertising network, ads for the product the user viewed at the first retail site could show up. The ad is targeted to the user in hopes of drawing him back to purchase the product.

Darla Cameron, *How Targeted Advertising Works*, Wash. Post (Aug. 22, 2013), https://www.washingtonpost.com/apps/g/page/business/how-targeted-advertising-works/412/.

36. Most commonly used to track web activity, cookies are "messages that web servers pass to your web browser when you visit internet sites." *Cookies*, MCS Creative Ltd., http://mcs-creative.co.uk/cookies.html (last visited Apr. 1, 2018). Internet browsers will store each message in a small file, containing information about the consumer's visit to the website. *Id.* When another page is requested from the server, the browser sends the message, or cookie, back to the server. *Id.*

however, Turn continued to track consumers even after consumers opted out through blocking or deleting cookies.[37] In *United States v. InMobi Pte Ltd.*, a mobile advertising network settled charges that it was using technology to track geolocation even when consumers, including children, had denied permission to access their location information.[38]

Privacy concerns raised by IoT and data-intensive services are compounded when data is not properly secured.[39] Hacks of major companies,[40] including high-profile attacks on the IoT,[41] have far-reaching effects. One in five American households has reported being victimized by security breaches.[42] It is no wonder then, that consumers have expressed little confidence in the security and privacy of their data—in 2015, eighty-four percent of American households using the internet were concerned about online privacy and data security.[43] In 2016, ninety-one percent of American consumers felt they had lost control of their data.[44] Americans' fears are heightened

37. *FTC Approves Final Consent Order*, *supra* note 34.

38. No. 3:16-cv-3474 (N.D. Cal. June 22, 2016); *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*, Fed. Trade Commission (June 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

39. *See* Cross-Device Tracking, *supra* note 26, at 9.

40. Major companies have been hacked over the past few years; Yahoo and Target were hacked in 2013. Sruthi Ramakrishnan & Nandita Bose, *Target in $18.5 Million Multi-State Settlement Over Data Breach*, Reuters (May 23, 2017, 12:39 PM), https://www.reuters.com/article/us-target-cyber-settlement/target-in-18-5-million-multi-state-settlement-over-data-breach-idUSKBN18J2GH; Kaveh Waddell, *Yahoo Suffers History's Biggest Known Data Breach*, Atlantic (Dec. 14, 2016), https://www.theatlantic.com/technology/archive/2016/12/hackers-steal-data-from-more-than-a-billion-yahoo-accounts/510716/. Home Depot was hacked in 2014. Jonathan Stempel, *Home Depot Settles Consumer Lawsuit Over Big 2014 Data Breach*, Reuters (Mar. 8, 2016, 11:33 AM), http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z. Anthem was hacked in 2015. Michael Hiltzik, *Anthem Is Warning Consumers About Its Huge Data Breach. Here's a Translation.*, L.A. Times (Mar. 6, 2015, 10:34 AM), http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html.

41. Cars and medical devices are among the IoT devices that have been targeted by security researchers looking to expose weaknesses in digital objects and their systems. Andy Greenberg & Kim Zetter, *How the Internet of Things Got Hacked*, Wired (Dec. 28, 2015, 7:00 AM), https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/. While these attacks were performed by security researchers, the risk of malicious attacks is real. *Id.* In one American university, the campus Information Technology Security Team discovered that more than five thousand of the school's IoT devices—"everything from light bulbs to vending machines"—were hacked and programmed to search for websites related to seafood, slowing and even blocking legitimate access to the network. Verizon, Data Breach Digest 47 (2017), http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf.

42. *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, Nat'l Telecomm. & 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.

43. *Id.*

44. Lee Rainie, *The State of Privacy in Post-Snowden America*, Pew Res. Ctr.: FactTank (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

by business practices that often leave consumers in the lurch.[45] As IoT products may not have patch support[46] or the same life expectancy as other connected products,[47] and these limitations are not always communicated clearly to consumers.[48]

Such concerns have real-life consequences that can affect consumer demand for IoT.[49] In 2015, almost half of American consumers reported that they were less likely to use certain online services because of privacy concerns,[50] and there is evidence that those same worries are slowing the pace of IoT adoption.[51] Consumers are repeatedly saying that data security is a top barrier to purchasing connected devices.[52] 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 consumers prefer on their IoT lightbulbs? But with billions of devices connected to the internet, there is a tremendous risk of abuse, impacting more than just the individual consumer.[53] For example, denial-of-service attacks have been launched from IoT devices, like routers and internet-connected video cameras.[54] These attacks, whereby attackers attempt "to prevent legitimate users from accessing information or services" through "targeting [a consumer's] computer and its network connection, or the computers and network of the sites [she is] trying to use,"[55] have the potential to disable not just

45. Hamid R. Nemati, *Preface*, *in* Security and Privacy Assurance in Advancing Technologies xxvii (Hamid R. Nemati ed., 2010).

46. "A patch is a software update . . . inserted (or patched) into the code of an executable program." *Patch*, Techopedia, https://www.techopedia.com/definition/24537/patch (last visted Apr. 1, 2018). Patches may fix software bugs or "[a]ddress new security vulnerabilities [or] software stability issues." *Id.* In online enviornments, "[p]atches have become extremely important as a methodology for updating programs or new system security threats which appear regularly." *Id.*

47. *See* Internet of Things: Privacy & Security in a Connected World, *supra* note 25, at 31. IoT devices can include "cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day," *id.* at 1, but are generally not considered to include desktop or laptop computers, smartphones, or tablets, even though they can be connected to the internet. *Id.* at 5.

48. *Id.* at 13–14.

49. Accenture, Igniting Growth in Consumer Technology 2, 7 (2016), https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf.

50. Goldberg, *supra* note 42.

51. In a 2016 global consumer survey, forty-seven percent of participants "cited 'privacy risk/security concerns' as a barrier" of adopting the IoT. Accenture, *supra* note 49, at 7.

52. *See, e.g.*, *id.* at 6–7; Nemati, *supra note* 45, at xxv–xxvii.

53. *See* Internet of Things: Privacy & Security in a Connected World, *supra* note 25, at 1, 10–13.

54. Brian Krebs, *KrebsOnSecurity Hit with Record DDoS*, KrebsOnSecurity, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (last updated Sept. 22, 2016, 8:33 AM).

55. Mindi McDowell, *Understanding Denial-of-Service Attacks*, U.S. Computer Emergency Readiness Team (last modified Feb. 6, 2013), https://www.us-cert.gov/ncas/tips/ST04-015.

websites but also critical infrastructure.[56] Insecure devices connected to the internet can be exploited in a matter of minutes.[57]

Insecure IoT devices are especially vulnerable to ransomware attacks,[58] which can hold hostage not only data, but refrigerators,[59] cars,[60] or factories as well.[61] Helping consumers mitigate IoT ransomware attacks is something policy makers, enforcers, and entire industries are just beginning to grapple with.[62]

Sometimes, the most harmful attacks go unnoticed or do not immediately seem harmful to an individual consumer.[63] What can a homeowner do if her router is used in a denial-of-service attack? Will she even know beyond noticing a degradation in quality of her connection? Or might the inconvenience of fixing the security breach outweigh the harm she perceives?

For all these reasons, the FTC is active in this field and has taken enforcement actions against hardware producers whose security flaws put hundreds of thousands of customers at risk.[64] Two prominent actions include those against router manufacturers

---

56. Joseph Carson, *The Risks of Critical Infrastructure and IoT from DDOS Attacks That Could Bring the Internet to a Standstill*, Thycotic: Lockdown (Nov. 1, 2016), https://thycotic.com/company/blog/2016/11/01/the-risks-of-critical-infrastructure-and-iot-from-ddos-attacks-that-could-bring-the-internet-to-a-standstill/.

57. Danny Palmer, *IoT Devices Can Be Hacked in Minutes, Warn Researchers*, ZDNet (Oct. 25, 2016, 9:00 AM), http://www.zdnet.com/article/iot-devices-can-be-hacked-in-minuteswarn-researchers/.

58. A ransomware attack is malicious software "that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom." Kim Zetter, *What Is Ransomware? A Guide to the Global Cyberattack's Scary Method*, Wired (May 14, 2017, 1:00 PM), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.

59. Kaveh Waddell, *The Extortionist in the Fridge*, Atlantic (Jan. 6, 2016), https://www.theatlantic.com/technology/archive/2016/01/the-extortionist-in-the-fridge/422742/.

60. Jeff Plungis, *Your Car Could Be the Next Ransomware Target*, Consumer Rep. (June 1, 2017), https://www.consumerreports.org/hacking/your-car-could-be-the-next-ransomware-target/.

61. Byron Kaye, *Chocolate Factory Becomes Australia's First Victim of Latest Cyber Attack*, Reuters (June 27, 2017, 9:41 PM), https://www.reuters.com/article/us-cyber-attack-australia/chocolate-factory-becomes-australias-first-victim-of-latest-cyber-attack-idUSKBN19J06G (examining the ransomware attack of a Cadbury chocolate factory); Dustin Volz & Eric Auchard, *More Disruptions Feared from Cyber Attack; Microsoft Slams Government Secrecy*, Reuters (May 12, 2017, 10:38 AM), http://www.reuters.com/article/us-britain-security-hospitals-idUSKBN18820S (discussing widespread ransomware attacks that affected operations at car factories).

62. *See* Internet of Things: Privacy & Security in a Connected World, *supra* note 25, at 47–50.

63. *See* Nicole Perlroth, *A Cyberattack "the World Isn't Ready for,"* N.Y. Times (June 22, 2017), https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html.

64. *See, e.g.*, *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Risk*, Fed. Trade Commission (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put; *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of its Computer Routers and Cameras*, Fed. Trade Commission (Jan. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

D-Link[65] and ASUS.[66] Both were alleged to have had inadequate security practices.[67] The FTC has also held companies accountable for making deceptive claims about their security practices, including bringing an action against TRENDnet, an electronics company that allegedly misrepresented the security of its video cameras.[68] These and other FTC security cases have alleged security failures such as hard-coding login credentials;[69] failing to assess command injection vulnerabilities;[70] exposing a private key;[71] transmitting or storing login credentials and sensitive information in clear text;[72] and failing to perform security testing or reviews of software.[73]

The FTC also launched the "Start with Security" Initiative in 2015.[74] Companies are encouraged to think about consumer privacy and security before it ever gets to the point of a data breach or FTC enforcement.[75] The initiative asks IoT companies to take ten simple steps to secure consumer data:

1. Start with security—build products with security in mind;
2. Control access to data sensibly, and think about whether companies really need to collect and keep all of the data;
3. Require secure passwords and authentication;
4. Store sensitive personal information securely and protect it during transmission;
5. Segment networks and monitor who is trying to get in and out;
6. Secure remote access to networks;
7. Apply sound security practices when developing new products;

65. Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. D-Link Corp., No. 3:17-cv-00039, 2017 WL 65168 (N. D. Cal. Jan. 5, 2017) [hereinafter D-Link Complaint].

66. ASUSTeK Computer Inc., No. 142-3156, 2016 WL 4128217 (F.T.C. July 18, 2016).

67. *ASUSTeK*, 2016 WL 4128217, at *6; D-Link Complaint, *supra* note 65, at 5.

68. TRENDnet, Inc., No. 122-3090, 2014 WL 556262, at *2 (F.T.C. Jan. 16, 2014).

69. *See* D-Link Complaint, *supra* note 65, at 5.

70. *See* Life is good, Inc., No. C-4218, File No. 072-3046 at *1 (F.T.C. Apr. 18, 2008); Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 6, United States v. RockYou Inc., No. 312-cv-01487 (N.D. Cal. Mar. 26, 2012) [hereinafter RockYou, Inc. Complaint].

71. *See* D-Link Complaint, *supra* note 65, at 5.

72. *See TRENDnet, Inc.*, 2014 WL 556262, at *2; Compete, Inc., No. C-4384, File No. 102-3155, at 5 (F.T.C. Feb. 20, 2013); Upromise, Inc., No. C-4351, File No. 102-3116, 2012 WL 1225058, at *2–3 (F.T.C. Mar. 27, 2012); RockYou, Inc. Complaint, *supra* note 70, at 5–6.

73. *See ASUSTeK*, 2016 WL 4128217, at *6; Credit Karma, Inc., No. C-4480, File No. 132-3091, 2014 WL 4252397, at *3–4 (F.T.C. Aug. 13, 2014); Fandango, LLC, No. C-4481, File No. 132-3089, 2014 WL 4252396, at *2–3 (F.T.C. Aug. 13, 2014).

74. Fair, *supra* note 18.

75. *See* Start with Security, *supra* note 24, at 1.

8. Ensure service providers implement reasonable security measures;
9. Put procedures in place to train employees and to keep security current and address vulnerabilities that may arise; and
10. Secure paper, physical media, and devices.[76]

These steps may sound straightforward, but time and again, cases arise in which even these basic principles were not followed. It lies with the FTC to help educate businesses about good, common-sense privacy practices and to foster a positive security culture for IoT devices.[77]

The FTC is also using new tools, like competitions, to stimulate innovations aimed at helping consumers.[78] In January 2017, the FTC launched the IoT Home Inspector Challenge, offering a $25,000 prize to a contestant who developed the best new tool to address security vulnerabilities caused by outdated software in IoT devices.[79]

The FTC also has suggestions for best practices for IoT consumers.[80] Through decades of computer use, many home users understand the basics of digital hygiene, like keeping a current anti-virus program,[81] refraining from opening suspicious links, and not downloading unknown files.[82] But what proactive measures should consumers take when their computer is inside a bagel toaster or a children's toy? A consumer may be justified in treating that device the same way she treats any other appliance or toy: plug it in and forget about it. But it is critical that consumers understand the

76. *Id.* at *passim*.

77. *See id.* at 1.

78. *See, e.g.*, *FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices*, Fed. Trade Commission (Jan. 4, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security [hereinafter *Challenge to Combat Security Vulnerabilities*]; *FTC Announces New Robocall Contests to Combat Illegal Automated Calls*, Fed. Trade Commission (Mar. 4, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-announces-new-robocall-contests-combat-illegal-automated; *FTC Publishes Official Rules for Zapping Rachel Robocall Contest*, Fed. Trade Commission (July 18, 2014), https://www.ftc.gov/news-events/press-releases/2014/07/ftc-publishes-official-rules-zapping-rachel-robocall-contest.

79. *Challenge to Combat Security Vulnerabilities, supra* note 78. The winning entry, announced on July 26, 2017, is a proposal for a mobile application named "IoT Watchdog." Ari Lazarus, *The Winner of the IoT Home Inspector Challenge Is…*, Fed. Trade Commission: Consumer Info., https://www.consumer.ftc.gov/blog/winner-iot-home-inspector-challenge (last modified July 27, 2017). Developed by Steve Castle, IoT Watchdog would "scan a person's Wi-Fi and Bluetooth networks to gather a list of IoT devices . . . , flag devices with out-of-date software and other common vulnerabilities, and then give instructions on how to update that device's software and fix other vulnerabilities." *Id.*

80. *See Online Security*, Fed. Trade Commission, https://www.consumer.ftc.gov/topics/online-security (last visited Apr. 1, 2018).

81. *See* Tami Abdollah, *5 Ways to Become a Smaller Target for Ransomware Hackers*, U.S. News (Apr. 5, 2016, 8:58 PM), https://www.usnews.com/news/business/articles/2016-04-05/5-ways-to-become-a-smaller-target-for-ransomware-hackers; Paul Norris, *Back to Basics: Tips to Improve Your Security Hygiene*, Tripwire: St. of Security (July 17, 2017), https://www.tripwire.com/state-of-security/security-awareness/back-to-basics-tips-to-improve-your-security-hygiene/.

82. *See* George Loukas, Cyber-Physical Attacks 200–01 (2015).

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 find it attractive to opt for a less expensive, albeit less secure, device.[83] But decisions about cost and security are optimally made bearing in mind all 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.[84] Consumers must be informed about the expected lifetime of a device, any available software support, and how to receive applicable security updates.[85]

Moreover, consumers must be warned if internet-connected devices are "bricked"—that is, no longer supported with relevant software updates.[86] Early termination of support for a connected device is especially worrisome as IoT becomes more central to consumers' day-to-day lives. For example, a consumer might buy an analog thermostat expecting it to last ten or more years, and she might understandably have the same expectation for the lifecycle of the thermostat's IoT equivalent. Manufacturers must either make clear to consumers how long to expect their devices will be supported or conform to reasonable consumer expectations.

The FTC has done much to bolster consumer confidence and ensure industry compliance with best practices.[87] This work alone is not enough, though, as the rapid spread of connected devices into the most far-flung and intimate aspects of daily life means that the FTC by itself cannot provide all the needed tools to maintain a fair and open market.

There are many areas for improvement with IoT devices, and there is a need across industries to find effective solutions for security and privacy.[88] The FTC must work with expert regulators, like the Federal Communications Commission, Food

83. Bruce Schneier, *Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations.*, Wash. Post: PostEverything (Nov. 3, 2016), https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/?utm_term=.906af876adff.

84. *See* Cross-Device Tracking, *supra* note 26, at 11–12.

85. *See* Internet of Things: Privacy & Security in a Connected World, *supra* note 25, at 31–32.

86. *See* Jessica Rich, *What Happens When the Sun Sets on a Smart Product?*, Fed. Trade Commission: Bus. Blog (July 13, 2016, 1:25PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product; Lee Matthews, *A Malware Outbreak Is Bricking Insecure IoT Devices*, Forbes (Apr. 10, 2017, 12:30 PM), https://www.forbes.com/sites/leemathews/2017/04/10/a-malware-outbreak-is-bricking-insecure-iot-devices/#7b8bd44729a3 (detailing a malware attack that interrupts a device's connectivity, limits its processing power, and scrambles and wipes storage, rendering the device useless). Bricking causes an electronic device to become completely nonfunctional. *Brick*, Dictionary.com, http://www.dictionary.com/browse/brick?s=t (last visited Apr. 1, 2018).

87. *See generally* Internet of Things: Privacy & Security in a Connected World, *supra* note 25 (discussing an FTC workshop at which representatives from government and industry, academics, and consumer advocates discussed issues arising out of the IoT and how to confront those issues); Start with Security, *supra* note 24 (drawing on previous FTC cases to recommend best practices for businesses to secure consumer information).

88. *See* Lucero, *supra* note 4, at 8–9.

and Drug Administration, Federal Aviation Administration, and National Highway Traffic Safety Administration, and with industry and consumer groups to develop a sustainable model for integrating secure IoT into our lives. The surest way to set clear industry-wide standards is through the passage of comprehensive data security and privacy legislation.[89]

The creation, storage, and use of all the data generated by our hyperconnectivity can lead to overt challenges, like discrimination. For instance, if the underlying data fed into algorithms is biased, inaccurate, incomplete, or not representative of certain populations, big data analysis can lead to inaccurate predictions that may perpetuate biases.[90] It can also lead to more subtle challenges: the data we create can feed algorithms that affect consumer choice, implicating laws and public policy along the way.[91] As the machines running algorithms get smarter, this technology raises questions regarding the roles of human beings in decision-making.[92] Which choices do we want to keep making ourselves, and which ones are we comfortable essentially automating or turning over to artifical intelligence?

The FTC has evolved to keep pace with a changing marketplace before—and it can continue to do so. It should build on frameworks—like privacy by design and security by design—that have evolved from its privacy and data security cases by convening a conversation with industry about data governance and, ultimately, ethics by design.[93] The basic requirements should include (1) transparency; (2) choice; (3) explainability; (4) testing; (5) data quality; (6) compliance; and (7) remediation or mitigation when necessary.

Rapidly expanding IoT-enabled connectivity has tremendous potential and pitfalls. Expanding and adapting consumer protection and the FTC will help foster trust and adoption of new technologies.

---

89. Internet of Things: Privacy & Security in a Connected World, *supra* note 25, at 49–52.

90. Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? 28–29 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

91. *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 252 (2013).

92. *See id.* at 252.

93. Fed. Trade Comm'n, Careful Connections: Building Security in the Internet of Things 1 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf; Edith Ramirez, Comm'r, Fed. Trade Comm'n, Remarks at the Privacy by Design Conference: Privacy by Design and the New Privacy Framework of the U.S. Federal Trade Commission 2 (June 13, 2012) (transcript available at https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf).