ARTICLES

LITTLE THINGS AND BIG CHALLENGES: INFORMATION PRIVACY AND THE INTERNET OF THINGS

HILLARY BRILL* AND SCOTT JONES**

The Internet of Things (IoT), the wireless connection of devices to ourselves, each other, and the Internet, has transformed our lives and our society in unimaginable ways. Today, billions of electronic devices and sensors collect, store, and analyze personal information from how fast we drive, to how fast our hearts beat, to how much and what we watch on TV. Even children provide billions of bits of personal information to the cloud through "smart" toys that capture images, recognize voices, and more. The unprecedented and unbridled new information flow generated from the little things of the IoT is creating big challenges for privacy regulators. Traditional regulators are armed with conventional tools not fully capable of handling the privacy challenges of the IoT.

A critical review of recent Federal Trade Commission (FTC) enforcement decisions sheds light on a recommended path for the future regulation of the IoT. This Article first examines the pervasiveness of the IoT and the data it collects in order to clarify the challenges facing regulators. It also highlights traditional privacy laws, principles, and regulations and explains why those rules do not fit the novel challenges and issues resulting from the IoT. Then it presents an in-depth analysis of four key FTC enforcement decisions to highlight how the FTC has and can regulate the IoT without undermining the innovation and benefits that this technology—and the data it provides—brings to our society.

---

* Glushko-Samuelson Intellectual Property Practitioner-in-Residence, *American University Washington College of Law.*

** Senior Associate, Latham & Watkins LLP.

Specifically, the Article describes how the FTC, faced with the privacy challenge that accompanies the interconnected world of the IoT, has managed to apply traditional standards of "unfairness" and "deceptive practices" to protect private information. The FTC has been flexible and nimble with its interpretations of such standards and, in its most recent IoT case, FTC v. VIZIO*, established a new "tool" in its toolkit for regulating IoT devices: an "unfair tracking" standard. As the de facto data protection authority in the United States, the FTC can use this new tool to work toward standardizing its treatment of IoT privacy issues instead of trying to fit those concerns neatly under the deception authority of section 5 of the FTC Act. However, this new tool also means that the FTC has the opportunity—and responsibility—to provide guidance on how it will wield that authority.*

To assure that innovation is not stifled and that this new rule is fairly applied (whether by the FTC or other agencies that may follow suit), it is imperative that the FTC diligently address concerns about the scope of this new rule and communicate that guidance to businesses, other regulators, and consumers alike. The new FTC administration should, as the primary regulator of information privacy and the IoT, continue the strong practice established by the previous administration, which is to provide guidance to businesses, consumers, and other regulators navigating the big challenges caused by the little things in the IoT.

TABLE OF CONTENTS

INTRODUCTION

The Internet of Things (IoT) is part of our lives in countless ways—some are welcome and intentional, such as trackable fitness devices, home security alert systems, or cars that can be unlocked and started remotely; others are unintentional and may cause concern to consumers, such as connected toys that can listen to our kids, or technologies capable of tracking our whereabouts or our shopping habits without our knowledge. The rapid growth of the IoT has prompted incredible technological advances along with thorny regulatory issues, specifically in the area of information privacy. Traditional regulators of privacy, specifically the Federal Trade Commission (FTC), have stretched to apply traditional tools to regulate unprecedented technological advances and the privacy challenges they bring. An analysis of the latest FTC cases and outcomes reveals an independent agency retooling investigative and enforcement methods and priorities to establish new expectations for how fair information practices and principles will be applied to new technologies.

The FTC, like the technological advances it has stretched to keep pace with, has been increasingly progressive in its recent decision-making terminology. This Article uses recent, seminal FTC cases and outcomes to demonstrate how the FTC has developed a new information privacy framework, most recently expressed as the concept of "unfair tracking," by modifying traditional legal concepts. The FTC has significantly expanded its role as the primary reviewer of information privacy matters raised by the IoT, while attempting to balance a philosophy not to

impede the advance of the technology comprising the IoT. This Article reviews recent FTC efforts to regulate the IoT and provides critical commentary on how the FTC might proceed.

To best understand the genesis of recent FTC actions on IoT data collection, Part I describes what makes up the IoT, how pervasive the IoT has become in our lives and, perhaps most importantly, how it will continue to innovate at a rapid pace. Parts II and III of this Article describe some unprecedented benefits and unprecedented challenges confronting regulators of information privacy in today's IoT age, including how to protect individual privacy rights without undermining innovation and the promise the connected world of the IoT brings.

Part IV provides an in-depth critical review of four key FTC cases attempting to strike this sort of balance: *In re Nomi Technologies, Inc.*,[1] *United States v. InMobi Pte Ltd.*,[2] *In re Turn, Inc.*,[3] and *FTC v. VIZIO*.[4] Initially, the FTC applied its traditional section 5 "deception" jurisprudence in a novel way to advance traditional notions of privacy, but it has recently transitioned to a new paradigm in the form of a cause of action for "unfair tracking," starting with *VIZIO*. However, this Article concludes that this new standard could prove either too anemic or, alternatively, overbroad, without proper shepherding by the FTC. It is only with proactive guidance to supplement its traditional reactive enforcement that the little things of the IoT can overcome the big information privacy challenges the IoT creates.

I. IOT: A BIG CONNECTION OF LITTLE THINGS

The term "Internet of Things" (IoT) has been defined in a variety of ways. In the broadest sense, the phrase "encompasses everything connected to the [I]nternet, but it is increasingly being used to define objects that 'talk' to each other."[5] A simple definition of the IoT is "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)."[6] *Oxford Dictionaries* define it as

1. No. C-4538, 2015 WL 5304114 (F.T.C. Aug. 28, 2015).
2. No. 3:16-cv-3474 (N.D. Cal. June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf.
3. No. 152-3099, 2016 WL 7448417 (F.T.C. Dec. 20, 2016).
4. No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.
5. Matt Burgess, *What Is the Internet of Things? WIRED Explains*, WIRED (Feb. 16, 2017), http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.
6. Jacob Morgan, *A Simple Explanation of "The Internet of Things,"* FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand.

"[t]he interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."[7] Others define the IoT as "the ability of one device to connect to other devices through wireless data infrastructure"[8] or "a system of devices and things that are implanted with sensors, software and electronics to initiate the exchange and collection of data and information."[9]

All of these definitions share a common theme: devices connected to each other and the Internet. However, devices connecting to each other—also known as machine-to-machine communication—is only one relevant part of the IoT. Machine-to-machine communication "use[s] network resources . . . for the purposes of monitoring and control, either of the 'machine' itself, or the surrounding environment," while the "[IoT] is envisioned to be[] where the physical world will merge with the digital world."[10] More simply stated, machine-to-machine communication is the "plumbing of the [IoT]" and is "what provides [t]he [IoT] with the connectivity" it needs to function.[11] Anything that connects to the Internet with an embedded sensor is part of the IoT, so devices within the IoT can be any size—even microscopic. It is in this sense that little things make up the IoT.

The vision for an IoT—connecting devices to the Internet—is not new. "[T]ech[nology] companies and pundits have been discussing the idea for decades . . . ."[12] Indeed, the "first Internet-connected toaster was unveiled at a conference in 1989."[13] Twenty-five years earlier, media theory professor Marshall McLuhan stated, "by means of electric media, we set up a dynamic by which all previous technologies . . . including cities—will be translated into information

---

7. *Internet of Things*, OXFORD DICTIONARIES, https://en.oxforddictionaries.com/definition/Internet_of_things (last visited July 4, 2017).

8. Nikole Davenport, *Smart Washers May Clean Your Clothes, but Hacks Can Clean out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 259, 261 (2016).

9. Vikas Agarwal, *10 Real Life Examples of Internet of Things*, CIR. DIG., http://circuitdigest.com/ten-examples-of-internet-of-things-iot (last visited July 4, 2017).

10. *What Is the Difference Between M2M and IoT?*, TELEFONICA BUS. SOLUTIONS BLOG (May 14, 2013), https://iot.telefonica.com/blog/what-is-the-difference-between-m2m-and-iot.

11. Esther Sanchez Garcia, *Internet of Things: The Big Brother of M2M*, ENNOMOTIVE (Feb. 25, 2016), http://www.ennomotive.com/internet-of-things-the-big-brother-of-m2m.

12. *See, e.g.*, Nicole Kobie, *What Is the Internet of Things?*, GUARDIAN (May 6, 2015, 4:51 AM), https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google.

13. *Id.*

systems."[14] German computer science pioneer Karl Steinbuch said in 1966 that "in a few decades' time, . . . computers will be interwoven into almost every industrial product."[15] In fact, in 1982, Carnegie Mellon students wired a Coca Cola machine to the Internet to avoid having to walk down to the third floor and find it was frustratingly empty.[16] The students were pleased with their solution, but "no one really regarded it as the vanguard of things to come."[17] In 1992, Cambridge University had the first wired web-cam showing employees when the coffee pot was freshly full.[18]

The term "Internet of Things" was not coined until the mid-1990s by Kevin Ashton, a "quirky young [Procter & Gamble] brand manager in the U.K. [who] puzzled over why a shade of brown lipstick kept disappearing from store shelves."[19] Bothered that "one shade of lipstick in his cosmetic line always seemed to be sold out" and not convinced that it was a coincidence, Ashton used "brand-new technology: a tiny 'radio-enabled' chip, later called [radio-frequency identification, or] *RFID*," and attached it to his lipstick.[20] The embedded RFID lipsticks were the beginning of today's "smart packaging," which enables customers to check out at registers in seconds.[21] In 2002, the movie *Minority Report* fictionalized the IoT of the future where Tom Cruise, as the protagonist John Anderton, walks by an advertisement that calls out his name and changes its advertisements accordingly.[22] One year later, Massachusetts Institute

14. MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 57 (1964).

15. Megan Garber, *The Real Reason Apple Wants You to Talk to Your House*, ATLANTIC (June 2, 2014), https://www.theatlantic.com/technology/archive/2014/06/your-home-theres-an-app-for-that/372032.

16. Danny Vink, *The Internet of Things: An Oral History*, POLITICO (June 29, 2015, 5:25 AM), http://www.politico.com/agenda/story/2015/06/history-of-internet-of-things-000104.

17. *Id.*

18. *Id.*

19. Kevin Maney, *Meet Kevin Ashton, Father of the Internet of Things*, NEWSWEEK (Feb. 23, 2015, 12:10 PM), http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html.

20. *Id.*

21. *Id.*

22. MINORITY REPORT (Cruise/Wagner Productions 2002); *see also* Richard Gray, *Minority Report-Style Advertising Billboards to Target Consumers*, TELEGRAPH (Aug. 1, 2010, 9:30 AM), http://www.telegraph.co.uk/technology/news/7920057/Minority-Report-style-advertising-billboards-to-target-consumers.html (describing billboards developed by IBM that use chips to identify an individual passing by and provide an advertisement based on that individual's shopping preferences).

of Technology declared 2013 "The Year of the Internet of Things" because of the growing influence it had on society.[23]

Jargon aside, our lives seamlessly incorporate the IoT into everyday items, such as watches,[24] cars,[25] coffee machines,[26] smartphones,[27] refrigerators,[28] home security systems,[29] and more. In addition to seamless incorporation, the IoT's use rate is also increasing at a lightning-quick pace.[30] Only twelve years ago, scholars Jerry Kang and Dana Cuff envisioned a future where "pervasive computing" would be the norm.[31] They envisioned a world where "the Internet will always be around—in the air and the walls," and where "networks of miniaturized, wirelessly interconnected, sensing, processing, and actuating computing elements kneaded into the physical world" and would "take place without direct human intervention or delay."[32]

We are moving toward this world. Estimates for the growth of IoT are astonishing. In 2010 and 2011, the idea that 50 billion devices

---

23. *2013: The Year of the Internet of Things*, MIT TECH. REV. (Jan. 4, 2013), https://www.technologyreview.com/s/509546/2013-the-year-of-the-internet-of-things.

24. *See* Daniel Joseph, *Apple Watch Will Power the Internet of Things*, GUARDIAN (Sept. 15, 2014, 10:04 AM), https://www.theguardian.com/technology/2014/sep/15/apple-watch-internet-of-things; Andrew Meola, *Internet of Things Devices, Applications & Examples*, BUS. INSIDER (Dec. 19, 2016, 1:44 PM), http://www.businessinsider.com/internet-of-things-devices-applications-examples-2016-8.

25. *See* Andrew Meola, *Automotive Industry Trends: IoT Connected Smart Cars & Vehicles*, BUS. INSIDER (Dec. 20, 2016, 12:12 PM), http://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10.

26. *See* Emily Reynolds, *The Internet of Things Wants to Make Your Coffee Too*, WIRED (Mar. 1, 2016), http://www.wired.co.uk/article/internet-connected-coffee-machine.

27. *See* Ernest Wittmann, *The Internet of Things Is Here, and It Will Revolve Around the Smartphone*, MEMEBURN (Dec. 9, 2015), http://memeburn.com/2015/12/the-internet-of-things-is-here-and-it-will-revolve-around-the-smartphone.

28. *See* India Ashok, *CES 2016: Samsung to Showcase Internet of Things Fridge Called Family Hub*, INT'L BUS. TIMES (Jan. 5, 2016, 12:34 PM), http://www.ibtimes.co.uk/ces-2016-samsung-showcase-internet-things-fridge-called-family-hub-1536010.

29. *See* Gail Dutton, *Home Security 2015: The Internet of Things (IoT) Brings Innovation AND Danger*, FORBES: BRANDVOICE (Apr. 8, 2015, 8:00 AM), http://www.forbes.com/sites/sungardas/2015/04/08/home-security-2015-the-internet-of-things-iot-brings-innovation-and-danger.

30. *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.

31. *See* Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 95–98 (2005) (defining "pervasive computing" as computing stemming from the convergence of the ubiquitous access to information, computers embedded in the physical world, and devices that can "measure the physical world and . . . initiate physical response").

32. *Id.* at 94, 99.

would be connected to the IoT by 2020 took the technology world by storm.[33] That number has since been criticized, but others have claimed similarly gargantuan amounts of interconnectivity. Predictions by technology companies and research firms have ranged from 20.8 billion to 75 billion connected devices by 2020.[34]

While the growth of the IoT is uncertain, the IoT is clearly here to stay, and the number of connected devices is growing at a viral pace.[35] While we may not yet live in the world that Kang and Cuff envisioned, where pervasive computing is seamlessly incorporated into our lives,[36] we are getting closer to it each day and perhaps faster than many may think. As a result, incorporating the little things of the IoT is leading to big regulatory challenges.

A. Visualizing the Internet of Things

The scene in Spielberg's film *Minority Report* where Tom Cruise's character walks by a billboard that instantly calls out his name once seemed science fiction; today, such a feature seems within reach. The IoT of today—and the IoT that the future envisions—is much more robust and pervasive than Spielberg imagined; today's IoT is everywhere. Specifically, the IoT touches four areas: body, home, city, and industry. Describing some trends and examples in each of these categories and the data they collect is helpful to better understand today's privacy challenges.

1. Wired body inside and out

Health, and safety are the biggest drivers of most wearable IoT devices used to monitor the body.[37] In the fitness industry, the most commonly known and well-accepted IoT devices are wearables like

---

33. *See* Amy Nordrum, *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, IEEE SPECTRUM (Aug. 18, 2016, 1:00 PM), http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.

34. *See* Syed Zaeem Hosain, *Reality Check: 50B IoT Devices Connected by 2020—Beyond the Hype and into Reality*, RCR WIRELESS NEWS (June 28, 2016), http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10. In 2010, IBM even predicted one trillion devices connected to the IoT by 2015. *Id.*

35. *See* Rob van der Meulen, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917 (forecasting that the number of connected devices will grow 31% worldwide in 2017 alone).

36. Kang & Cuff, *supra* note 31, at 94.

37. *See* Jessica Twentyman, *Wearable Devices Aim to Reduce Workplace Accidents*, FIN. TIMES (June 1, 2016), https://www.ft.com/content/d0bfea5c-f820-11e5-96db-fc683b5e52db.

Fitbit, Jump, and the Samsung or Apple smartwatches. These devices have sensors that monitor heart rate, steps, sleeping patterns, when you stand, and more. Your smartphones accumulate some of the same data and with it you can use your WiFi and GPS to track how far you walk, where you walk, how many steps you take, and how many stairs you climb, among other things. The information transmitted through Internet connections is accumulated in a manner for the user to keep or share. Other sensors are not wearables, such as the Aria weight scale, which connects with your Fitbit account. If you want to use your smartphone—along with your scale and your wearable—to support nutritional goals, then you can use a phone app like SmartPlate, for example, that tracks the nutritional content of the food you consume.[38]

The pharmaceutical industry has joined the IoT through the introduction of "smart" products that encourage accurate and efficient medication use. For example, prescription bottle services may include a wireless chip to send reminder messages and coordinate refills with doctors.[39] Smart pills are being tested that, once ingested, can communicate when you took the medications, what kind you took, and how effective it was.[40] All of this information can be transferred to your physician.

Aging is another growing market for the IoT, with companies like BodyGuardian—approved by the FDA—offering a sensor system that remotely reads a patient's heart and respiration rates, and activity level. The sensors allow a user's family or physicians to monitor the patient and call for medical attention if necessary.[41] These types of IoT devices provide family members access to their "loved one's daily routine[,] giv[ing them] peace of mind for their safety by alerting [them] to any serious disruptions detected in [the user's] normal schedule."[42] Even babies are connected to the IoT wearable market

38. *See* SMARTPLATE, https://www.getsmartplate.com (last visited July 4, 2017).

39. *See* Nissa Simon, *Technology Puts You in Charge of Your Health*, AARP (Sept. 23, 2013), http://www.aarp.org/health/healthy-living/info-09-2013/health-gadgets.html.

40. *See Proteus Digital Health Announces FDA Clearance of Ingestible Sensor*, PROTEUS DIGITAL HEALTH (July 30, 2012), http://www.proteus.com/press-releases/proteus-digital-health-announces-fda-clearance-of-ingestible-sensor-2.

41. Brian Dolan, *FDA Clears Cardiac Monitor from Preventice, Mayo Clinic*, MOBIHEALTHNEWS (Sept. 11, 2012), http://www.mobihealthnews.com/18407/fda-clears-cardiac-monitor-from-preventice-mayo-clinic.

42. *An Internet of Things*, POSTSCAPES, https://www.postscapes.com/internet-of-things-examples (last visited July 4, 2017).

through products like Rest Device's groundbreaking Mimo onesie.[43] Because Mimo monitors sleeping, breathing, heart rate, and perspiration, Rest Device has developed a set of standards that will be the basis of an alert system if a user's health deteriorates.[44]

2. Connected home

The IoT-connected home includes monitoring systems, smart appliances, and connected entertainment. Today, we can control and monitor our home's exterior and interior through apps and devices integrated with the IoT. For example, to monitor lighting usage or turn on devices when you are inside or outside your house, you can use Belkin's WeMo home automation system, which will even let you turn on your Mr. Coffee smart coffee maker and Crock-Pot slow cooker.[45] Home security systems have upgraded from internal motion detectors and window sensors to devices that include not just a video camera but also sensors for air quality, motion, sound, temperature, and vibration.[46] The Canary system learns what a home's normal conditions are and then sends an alert if something, such as temperature or ambient noise, changes.[47]

Users that are willing to embed a device in their homes' central electric control panel can use Neurio, which recognizes "power signatures" of home appliances.[48] It monitors power use, breaks down activity by device, uses machine learning to interpret that activity, and alerts the user when something important happens, such as an oven being left on for an extended period of time.[49] The ivee Sleek is a voice-activated alarm clock that interacts with another IoT device, the Nest smart home thermostat.[50] You can ask your clock to turn down

43. Danny Chrichton, *With Mimo, MIT Alums Are Disrupting the Baby Nursery, Onesie at a Time*, TECHCRUNCH (Jan. 27, 2015), https://techcrunch.com/2015/01/27/with-mimo-mit-alums-are-disrupting-the-baby-nursery-onesie-at-a-time.

44. *Id.*

45. *See* Robert L. Mitchell, *The Internet of Things at Home: 14 Smart Products that Could Change Your Life*, COMPUTERWORLD (June 30, 2014, 6:30 AM), http://www.computerworld.com/article/2474727/consumerization-of-it/consumerization-150407-the-internet-of-things.html.

46. *Id.*

47. *Id.*

48. Antonio Pasolini, *Neurio Sensor Monitors Multiple Household Appliances to Cut Energy Consumption*, NEW ATLAS (Oct. 16, 2013), http://newatlas.com/neurio-monitor-energy-home/29420.

49. *See id.*; Gillian Shaw, *Vancouver Company Helps You Create a Smart Home*, VANCOUVER SUN (Nov. 25, 2013), http://www.vancouversun.com/touch/story.html?id=9206731.

50. *See ivee Sleek: Wi-Fi Voice-Activated Assistant*, KICKSTARTER, https://www.kickstarter.com/

the heat and then ask it to connect with your Staples Connected Home and SmartThings home monitoring and control systems to turn off your alarm.[51] Other systems, such as Lowe's Iris, allow you to turn on your sprinkler system and monitor your water usage remotely.[52]

IoT-connected appliances also include the newest version of "smart coffee" makers, such as the Firebox Coffee Maker, which allows you to use your phone to automatically make a cup of coffee when the weather drops to a certain temperature or when your GPS places you in a certain location.[53] The Samsung Smart Hub refrigerator allows you to use your phone to see what you need at the store.[54] At home, you can use your fridge to play your favorite tunes and connect with your family calendars.[55] Further, if you want your wine decanted with the precise amount of oxygen and at a certain time, you can use the iSommelier Smart Decanter.[56]

Connected entertainment is another part of the smart home. With the SmartV mobile application, you can use your smartphone to control thirty-two devices in addition to receiving other benefits, such as monitoring the "health" of your viewing habits and alerting kids if they are too close to the TV.[57] Amazon's Alexa and the new Google Home are "smart speakers" that will tell you the weather and the latest news, play music, and control other smart home devices

---

projects/ivee/ivee-sleek-wi-fi-voice-activated-assistant (last visited July 4, 2017) (describing ivee Sleek as an alarm clock that "answers questions, obeys commands, and controls other internet-connected devices").

51. Megan Wollerton, *Ivee Sleek Voice-Activated Home Assistant Joins Forces with Lowe's Iris and Staples Connect*, CNET (Jan. 9, 2014, 4:06 PM), https://www.cnet.com/news/ivee-sleek-voice-activated-home-assistant-joins-forces-with-lowes-iris-and-staples-connect.

52. *See Customize Your Iris Experience*, IRIS BY LOWES, https://www.irisbylowes.com/solutions (last visited July 4, 2017).

53. *See Smarter Coffee*, FIREBOX, https://www.firebox.com/Smarter-Coffee/p6991 (last visited July 4, 2017).

54. *See Family Hub Refrigerator*, SAMSUNG, http://www.samsung.com/us/explore/family-hub-refrigerator (last visited July 4, 2017) (stating that "[t]he Family Hub is a revolutionary new refrigerator with a Wifi enabled touchscreen that lets you manage your groceries, connect with your family and entertain like never before").

55. *Id.*

56. *See iSommelier Pro Smart Decanter (Black)*, WINE ENTHUSIAST, http://www.wineenthusiast.com/isommelier-pro-smart-decanter-(black).asp (last visited July 4, 2017) (describing the decanter as "the first smart decanter using a revolutionary technology that reinvents the decanting experience to enhance the flavors and aromas of the wine in just a few minutes").

57. *See iiMote*, SMARTV, http://smartv.hk/iiMote.html (last visited July 4, 2017); *Life Can Be Fun & Healthy*, SMARTV, http://smartv.hk/hc/dsl.html (last visited July 4, 2017) (promoting SmartV as a technology that will provide users with "better time management[and a] healthier life style").

connected to your television or other app-based entertainment sources, such as iHeartRadio, Spotify, or Audible, heating, air conditioning, lights and more.[58] Both Amazon and Google are working on turning these smart speakers into home phones.[59]

3. Connected purchasing

Smartphones offer integrated purchasing that mimics an in-store experience and gives consumers the convenience of purchasing coffee or a burrito while at their desks or in a cab. Grocery store delivery services merely connect users to a list of goods through smartphones and tablets; however, IoT devices, like Amazon Dash, enable users to push a button and an automatic shipment of the particular product will be on its way. Amazon Dash unrolled its connected purchasing button for select items like Tide washing detergent, Glad trash bags, or Colgate toothpaste.[60] While users currently need one button for each item they would like to buy, experts foresee that consumers will soon be able to design custom buttons based on their own purchasing habits.[61] Amazon's smart speaker, Alexa, also accommodates voice-enabled purchases. When you make a purchase request, Alexa "talks" you through several purchase options, including Amazon choices for highly rated, well-priced products that are immediately available to be shipped quickly

58. *See* Ry Crist, *Amazon Alexa: Device Compatibility, How-tos and Much More*, CNET (Apr. 8, 2016, 11:21 AM), https://www.cnet.com/how-to/amazon-alexa-device-compatibility-how-tos-and-much-more; Andrew Gebhart, *Google Home vs. Amazon Echo, Round 2: Google Strikes Back*, CNET (Mar. 18, 2017, 2:49 PM), https://www.cnet.com/news/google-home-vs-amazon-echo.

59. Ryan Knutson & Laura Stevens, *Amazon and Google Consider Turning Smart Speakers into Home Phones*, WALL ST. J. (Feb. 15, 2017, 9:46 AM), https://www.wsj.com/articles/amazon-google-dial-up-plans-to-turn-smart-speakers-into-home-phones-1487154781.

60. *See* Samantha Murphy, *Amazon Dash Is Here: Push Button, Get Stuff*, MASHABLE (July 30, 2015), http://mashable.com/2015/07/30/amazon-dash-button-launch; Barbara Thau, *Retailers Are Spending Billions on the "Internet of Things," but Will It Pay off?*, FORBES (Nov. 18, 2016, 10:30 AM), http://www.forbes.com/sites/barbarathau/2016/11/18/retailers-are-spending-billions-on-the-internet-of-things-but-will-it-pay-off ("Amazon Dash addresses a longtime shopper pain point: Buying everyday essentials that pose a particular inconvenience when they run out. 'Customers never want to reach for a new trash bag and find out the box is empty.'" (quoting Brandi Pitts, Reynolds Consumer Products head of ecommerce)).

61. Kellen Beck, *Amazon's Customizable Dash Button Sold out in Less than a Day*, MASHABLE (May 13, 2016), http://mashable.com/2016/05/13/amazon-dash-custom.

with their Prime Service.[62] Alexa will then give you delivery information and the total price.[63]

Additionally, RFIDs are IoT sensors that have been around for years and are used to help manage inventory by tracking the location of merchandise throughout the supply chain and replacing the process of employees scanning items manually.[64] This technology has dropped in price from one dollar in 2003 to ten cents today, and more retailers are embracing the benefits it provides, including "cycl[ing] inventory at a rate of 12,000 to 18,000 items per hour versus previous manual counts that average about 250 times per hour."[65] Stores are also using IoT to create interactive and connected experiences. For example, Sephora has Beauty Boards that show uploaded photos of customers using their products, and shoppers can click on which ones they want to buy.[66] Similarly, at a wine store, shoppers can enter taste preferences into an app, and bottles with those preferences will light up on a digital shelf.[67]

4. Connected cities and environmental protection

Many advances in IoT-connected cities revolve around environmental monitoring and analysis of data to prevent waste. For example, smart trashcans, like Big Belly Trash, use real-time data collection and alerts to trigger bin collection. Through data analysis, cities can ultimately reduce the number of pick-ups required and lessen fuel and other wasted resources.[68] Mobile apps like the popular Waze program help ease traffic, and real-time parking space apps, such as Streetline's ParkSight, can help save energy and resources needed for managing traffic.[69] Crowd-sourced IoT efforts,

---

62. *About Placing Orders with Alexa*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201807210 (last visited July 4, 2017).

63. *See id.*

64. Thau, *supra* note 60.

65. *Id.* (quoting Melanie Nuce, vice president of GS1 US).

66. Chanel Parks, *3 Reasons Why We're Loving Sephora's Beauty Board*, HUFFINGTON POST (Mar. 13, 2014, 4:02 PM), http://www.huffingtonpost.com/2014/03/13/sephora-beauty-board_n_4956441.html.

67. Thau, *supra* note 60.

68. *Bigbelly Smart Waste & Recycling Systems Captured over 112 Million Gallons of Public Space Waste Last Year*, BIGBELLY (Feb. 7, 2017, 8:05 AM), http://bigbelly.com/bigbelly-smart-waste-recycling-systems-captured-over-112-million-gallons-of-public-space-waste-last-year; *Labor and Vehicle Efficiency*, BIGBELLY, http://bigbelly.com/benefits/optimization (last visited July 4, 2017).

69. *See* Matthew Shaer, *Google Scoops up Waze in a Deal Reportedly Worth $1.1 Billion*, CHRISTIAN SCI. MONITOR (June 11, 2013), http://www.csmonitor.com/Technology/

such as that promoted by AirCasting, rely on users to connect a device to their phones to record, map, and share environmental data, such as sound level, temperature, humidity, carbon monoxide and more with their communities via the CrowdMap.[70] Echelon's technology allows cities to adjust the level of outdoor lighting depending on the time of day, weather, and season, enabling cities to reduce streetlight energy cost by thirty percent.[71] SenseNET, built by the Canadian start-up Awesense, uses battery-powered sensors to measure electrical power line usage and identify meter-tampering issues, installation issues, or malfunctions.[72]

To track water movement, the University of California at Berkeley created a floating sensor network that uses motorized drifters, embedded with cell communication and location devices, to determine water temperature, flow, and salt levels.[73] To stop illegal deforestation in Brazil, devices are attached to trees that alert authorities when those trees have been logged in the nearby area.[74] To protect cattle in Kenya, conservationists are attaching smart

---

2013/0611/Google-scoops-up-Waze-in-a-deal-reportedly-worth-1.1-billion (describing Waze as an application for crowd-sourcing traffic information that allows users to warn others of traffic jams and suggest better routes); *Streetline Announces Smart Parking Project with Montreal*, PRNEWSWIRE (Mar. 18, 2014, 12:45 PM), http://www.prnewswire.com/news-releases/streetline-announces-smart-parking-project-with-montreal-250809681.html (explaining that a network of ultra-low power sensors built into the pavement detects the presence of cars and reports parking availability and traffic congestion metrics).

70. *About AirCasting*, AIRCASTING, http://aircasting.org/about (last visited July 4, 2017) (describing Aircasting as "a platform for recording, mapping, and sharing health and environmental data using your smartphone" and indicating that "[e]ach AirCasting session lets you capture real-world measurements, annotate the data to tell your story, and share it via the CrowdMap").

71. MOOR INSIGHTS & STRATEGY, ECHELON'S EFFICIENT CONNECTED LIGHTING SOLUTIONS 5 (2015), http://www.moorinsightsstrategy.com/wp-content/uploads/2015/06/Echelons-Efficient-Connected-Lighting-Solutions-by-Moor-Insights-Strategy.pdf (describing the adaptive and predictive controls and software that is built into intelligent lighting); *see also* ECHELON, SHINING A LIGHT ON ENERGY SAVINGS, http://www.echelon.com/assets/blt1f1c055db1151a7c/Outdoor-Lighting-Wired-Solution-Brochure.pdf (last visited July 4, 2017).

72. *See* James Grundvig, *Detecting Power Theft by Sensors and the Cloud: Awesense Smart System for the Grid*, HUFFINGTON POST (Apr. 15, 2013, 12:44 PM), http://www.huffingtonpost.com/james-grundvig/detecting-power-theft-by-_b_3078082.html.

73. U.C. BERKELEY, FLOATING SENSOR NETWORK, http://float.berkeley.edu/fsn/?q=webfm_send/213 (last visited July 4, 2017).

74. *See* Zafar Anjum, *How Internet Devices Are Working to Save the Rainforest*, PCWORLD (June 16, 2013, 2:00 PM), http://www.pcworld.com/article/2042086/how-internet-devices-are-working-to-save-the-rainforest.html (describing the use and benefits of machine-to-machine learning to preserve rainforests).

collars to lions that can track and communicate their location to herders and conservationists.[75]

Simply put, this non-scientific survey of IoT devices reveals that the IoT already affects many parts of our lives. It is not a world of the future but the world we live in today. This amazing connected world and the promises it brings and provides also comes with challenges for regulators because these devices only work when information is collected. Regulators striving to uphold fair information practices must now set policy guidelines and enforcement priorities within a quick moving, rapidly growing, Internet-connected world handling new and sensitive data sets: from heart rate and body temperature, to the content playing on our devices, to how the world is managing pollution. Regulators have a daunting task to keep pace with the innovation of the IoT and to protect security and privacy of the information it collects.

II. THE PROMISES AND CHALLENGES OF THE INTERNET OF THINGS

The IoT has already begun to impact our lives, and its possibilities are endless. Describing the hypotheticals for the future of IoT invokes a world filled with magic from autonomous cars that drive us to work, to refrigerators that order food for us and connect with drones that deliver it. The cost for this "magic" is the private information we are sharing about ourselves—from our purchasing habits, to our whereabouts and even our bodily fluids. When that private information is collected from or about consumers, regulators of fair information practices are faced with difficult questions: Are consumers aware of what is collected and how they are being profiled? Is that information augmented or monetized in potentially surprising or unfair ways? What happens if the data falls into unauthorized hands, e.g., through sloppy practices or malicious hacks? Addressing and balancing these fundamental consumer protection considerations has caused the primary data protection "regulator" in the United States, the FTC, to apply longstanding doctrines in surprising ways, with far reaching consequences, for IoT sellers and consumers alike.

---

75. *See Species Research: Protecting, Monitoring & Researching the Wildlife of Kuku*, MASSAI WILDERNESS CONSERVATION TR., http://maasaiwilderness.org/programs/species-research (last visited July 4, 2017).

A. Untraditional Rules for a Traditional Problem

At the beginning of the Internet age, fair information practices were (in hindsight) fairly straightforward. The collection of personal information was obvious and in plain view. Purchasers completed online order forms with payment and address details, which were used by sellers in non-surprising ways: order fulfillment and customer service, for example. Consumers provided their home or email address for a sweepstakes giveaway. Individuals could opt out of marketing messages and simply get on a do-not-call or do-not-email list.

These early online data collection, use, and sharing practices at first presented new challenges for the FTC. For example, in a 2002 case, the FTC settled charges against Eli Lilly that alleged the unauthorized disclosure of sensitive personal information collected through its website, Prozac.com.[76] In that matter, a Lilly employee was alleged to have sent a bulk email message that included the email addresses of all recipients in the "To:" line, unintentionally revealing to each recipient the email addresses of hundreds of subscribers.[77] The FTC settled the case on allegations of deception, arguing that Lilly's claim that it took measures to protect the privacy and confidentiality of sensitive personal information were deceptive because Lilly failed to maintain internal measures (including training or oversight) to prevent such disclosures.[78] Shortly thereafter, the rules of the road were widely communicated and adopted: post and adhere to an online privacy policy that states what is collected; how it is shared, used, and secured; and what choices consumers have regarding their personally identifying/able information.[79]

Today, ideas of what privacy means are different than even those from a generation ago.[80] For example, previous rules grounded in traditional ideas of privacy were simpler and easier to implement. Today, those rules do not necessarily apply because our idea of privacy is no longer concrete. As the boundaries and definitions of privacy are challenged, it

76. *Eli Lilly & Co.*, 133 F.T.C. 763, 763 (2002).

77. *Id.* at 767.

78. *Id.*

79. *See id.* at 784–87.

80. *See* Phil Pitchford, *The Changing Face of Privacy*, U.C. RIVERSIDE (2013), http://magazine.ucr.edu/85 (explaining how our ideas of privacy have changed in that "we share intimate photos on Facebook" and allow ourselves to be "filmed by security cameras to feel safer"); Laurence Scott, *How Airbnb Kills Our Ideas of Privacy*, DAILY BEAST (Aug. 28, 2016, 12:01 AM), http://www.thedailybeast.com/articles/2016/08/28/how-airbnb-kills-our-ideas-of-privacy.html ("We are required to accumulate an online history of consistent, amiable personhood, so that we can be recognized wherever we crop up in digital space.").

creates uncertainty for businesses and consumers that are part of the economy of the IoT. This uncertainty creates challenges for regulators, like the FTC, that need to protect users without unnecessarily stifling innovation. Our traditional modes of governing privacy may not be well-suited for meeting these new challenges.

While traditional data collection practices and compliance expectations certainly still exist, they no longer present the same range of enforcement or policy challenges to regulators and businesses. Much of what the IoT does is enable rich learning about the world through the tracking of activity (personal or not) and analysis of that tracking information. This tracking may occur across time (how many steps you take in a day) or across devices (what YouTube videos should be recommended to you on your iPad based on those you watched on your iPhone). So-called "tracking" provides for valuable individualized recommendations (geolocation tracking may help you find the closest gas station or emergency room) or informs aggregate analysis that creates overwhelming human value (traffic trends or aggregate health data about a flu outbreak). The information collected through new abilities to "track" with the IoT is one of the recent challenges that the FTC has addressed.[81]

B. Machine-to-Machine Communication and the Privacy Challenges of Aggregating Data from Multiple Sources

The next noteworthy step in the growth of the IoT is the capacity for devices to communicate this "tracking" information with each other, even autonomously. Devices are increasingly gathering information not for the immediate, obvious use by that device but instead for *another device*; for example, the Nest thermostat connects to Amazon Echo, and the SmartPlate connects to your Fitbit.

The aggregation of data from multiple IoT sources creates both fantastic opportunities for consumer value and potentially outsized privacy concerns.[82] As the IoT becomes more integrated, it may also be easier for unauthorized parties to obtain a more comprehensive and complete dataset of an individual.[83] For example, right now, if you wanted to piece together a digital profile of someone, you would

---

81. *See infra* Part IV.

82. *See* FED. TRADE COMM'N, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT 5–7 (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 (attempting to balance the pros and cons of IoT).

83. *Id.* at 9.

have to pull from several data sources. As data aggregators continue to pull more information from more devices, personal control over one's information wanes and the security and privacy risks for an individual's personal information grows.[84] Untraditional data collection creates a great challenge for regulators that may lack the appropriate tools to handle these issues.

Industry is eliminating the human review of this information and is incorporating innovative machine learning, artificial intelligence, and sophisticated algorithms into the processing and collecting of data from interconnected IoT devices.[85] Devices are collecting data from each other but are also now shutting out humans. For example, a recent Super Bowl ad showed H&R Block incorporating IBM Watson, an artificial intelligence device, into its tax tool.[86] A question arises whether human involvement diminishes privacy concerns—for example, that humans are subject to certain regulatory controls that may not work to regulate artificial intelligence. On the other hand, could human involvement increase privacy concerns—for example, are individuals more comfortable with a computer knowing their sensitive information than another person?

C. Children and "Smart" Toys

IoT privacy concerns are challenging enough for adults to navigate. The issue may be even more difficult for parents whose children are using IoT devices and toys and are not aware of the privacy information aggregated by toymakers and manufacturers.[87] Parents are increasingly choosing "connected toys" that are integrated into the IoT to provide interactive learning and

84. *Id.*

85. *See* Brandon Rohrer, *An Adaptive Learning Algorithm for the Internet of Things*, DATA SCI. & ROBOTS BLOG (Mar. 30, 2016), https://brohrer.github.io/adaptive_reinforcement_learning_iot.html (describing the application of a model-based reinforcement learning algorithm to IoT); Mika Tanskanen, *Applying Machine Learning to IoT Data*, SAS, https://www.sas.com/en_us/insights/articles/big-data/machine-learning-brings-concrete-aspect-to-iot.html (last visited July 4, 2017) (discussing the symbiotic development of machine learning and IoT).

86. *See* Jonathan Vanian, *H&R Block Is Enlisting IBM's Watson to Help with Your Taxes*, FORTUNE (Feb. 1, 2017), http://fortune.com/2017/02/01/hr-block-ibm-watson-taxes.

87. *See, e.g.*, Complaint & Request for Investigation, Injunction, & Other Relief at 18–19, *In re Genesis Toys & Nuance Commc'ns* (F.T.C. 2016) (submitted by the Electronic Privacy Information Center) [hereinafter EPIC Complaint], https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf (alleging violations of the Children's Online Privacy Protection Act because Genesis failed to properly notify parents of information collection practices and material changes to its privacy policy).

entertainment for their children.[88] These "smart toys" raise new issues concerning the amount of information that the companies are collecting as well as how to protect and keep that information secure.[89] Ninety percent of connected toys collect information about children, and seventy percent of those devices transmit that information through unencrypted networks, leaving children's personal information open to potential cyber attacks.[90]

In fact, the personal information of six million children, plus four million parents, has already been exposed through just one hack.[91] VTech collected personal information via its connected tablets for kids.[92] Such information included names, gender, birthdates, and photographs.[93] VTech's data information was breached, leaving personal information available to the hackers.[94] The VTech breach not only alerted legislators to the issue of children's privacy and IoT devices but also resulted in an official congressional investigation that documented serious security flaws in two other connected toys.[95] The Fisher-Price Smart Toy Bear, which is a WiFi-connected stuffed animal that "listens" and "remembers" what your child says, had an unsecured server vulnerable to potential attackers.[96] The information that the bear collects includes parents' email addresses and login passwords; children's first names, birthdates, and gender; WiFi

88. *See* FUTURE OF PRIVACY FORUM, FAMILY ONLINE SAFETY INST., KIDS & THE CONNECTED HOME: PRIVACY IN THE AGE OF CONNECTED DOLLS, TALKING DINOSAURS, AND BATTLING ROBOTS 1 (2016), https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf.

89. *Id.*

90. *Id.* at 15.

91. BILL NELSON, S. COMM. ON COM., SCI, & TRANSP., 114TH CONG., CHILDREN'S CONNECTED TOYS: DATA SECURITY & PRIVACY CONCERNS 1 (2016) [hereinafter SENATE REPORT] (mentioning that of the total records exposed, 2.8 million children and 2.2 million parents were in the United States).

92. *Data Breach on VTech Learning Lodge (Update)*, VTECH (Nov. 30, 2015), https://www.vtech.com/en/press_release/2015/data-breach-on-vtech-learning-lodge-update; Daniel Victor, *Security Breach at Toy Maker VTech Includes Data on Children*, N.Y. TIMES (Nov. 30, 2015), https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html.

93. *FAQ About Cyber Attack on VTech Learning Lodge*, VTECH (Dec. 16, 2016, 11:30 AM), https://www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge.

94. *Id.*

95. SENATE REPORT, *supra* note 91, at 1.

96. *Researchers Discover a Not-so-Smart Flaw in Smart Toy Bear*, TRENDMICRO (Feb. 4, 2016), https://www.trendmicro.com/vinfo/us/security/news/Internet-of-things/researchers-discover-flaw-in-smart-toy-bear.

password; and mobile device information in addition to the children's images and audio saved locally on the toy.[97] Additionally, the information collected by the hereO watch—a GPS watch for children that allows parents to track their child's location—was also vulnerable to attack.[98] Investigators discovered that a hacker could access every family member's real-time location, including that of the child wearing the watch, plus the child's historical location data.[99]

According to Rapid7, the research company that identified the privacy security flaw in the Fisher-Price Smart Toy Bear, "most companies making connected devices—not just toys—aren't paying close enough attention to security."[100] These connected toys are a "potential landmine."[101] For example, today's IoT Barbie is a network-enabled, cloud-powered, AI-driven doll with a necklace that records the child's conversations and uses WiFi to transmit it back to a server for processing before Hello Barbie responds.[102] Mattel and ToyTalk's failure to employ proper encryption standards left the personal utterances of children exposed to hackers, despite the software company's privacy policy stating that the company would not share the information for any reason other than to improve its speech recognition capabilities and similar research and development projects.[103] The IoT Barbie is just one type of connected doll that collects personally identifiable information and

97. SENATE REPORT, *supra* note 91, at 12.

98. Mark Stanislav, *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy & hereO GPS Platform Vulnerabilities (FIXED)*, RAPID7 (Feb. 2, 2016), https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform.

99. SENATE REPORT, *supra* note 91, at 14.

100. Laura Hautala, *Playtime Is Over: Can Smart Toys Ever Be Safe?*, CNET (Feb. 26, 2016, 5:30 AM), https://www.cnet.com/news/internet-of-things-connected-smart-toys-rsa-security-conference.

101. Dan Goodin, *Internet-Connected Hello Barbie Doll Gets Bitten by Nasty POODLE Crypto Bug*, ARS TECHNICA (Dec. 4, 2015, 12:57 PM), https://arstechnica.com/security/2015/12/internet-connected-hello-barbie-doll-gets-bitten-by-nasty-poodle-crypto-bug.

102. *Id.*

103. *Id.*; Whitney Meers, *Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns*, HUFFINGTON POST (Nov. 30, 2015, 4:45 PM), http://www.huffingtonpost.com/entry/hello-barbie-security-concerns_us_565c4921e4b072e9d1c24d22; *see also Hello Barbie/Barbie Hello Dreamhouse Privacy Policy*, TOYTALK, https://www.toytalk.com/hellobarbie/privacy (last updated Apr. 11, 2017) ("We do not use voice recordings or their content, including any personal information that may be captured therein, to contact children or to advertise to them.").

may be retaining it for an indefinite period of time.[104] Consumer groups are identifying other types of smart dolls and raising privacy and security concerns to the FTC.[105]

Connected toys raise serious information privacy and security issues that challenge regulators to protect personal information while undermining the potential benefits these toys can bring. Not all connected toys are talking dolls and plush bears. Technology inherent in the IoT can be used for interactive learning and could revolutionize our education industry. The new toys created by the IoT have put regulators in a tough spot. Regulators will want to look at the future growth of the IoT, current privacy and security challenges of the IoT, and yesterday's regulatory tools to ensure privacy protections for the IoT.

D. IoT Challenges and Early Regulatory Response

In the face of these new technological advances, the FTC for the past few years has moved to fill a perceived vacuum in privacy and security protections for consumers in the IoT, beginning with its first workshop in November 2013.[106] The workshop—and ensuing reports and enforcement cases—confirm that the IoT era presents unique problems and requires novel expansions of consumer protection doctrines, even where devices are only handling data points that are traditionally viewed as "anonymous," such as IP addresses.

From a privacy standpoint, applying historical notions of "fair information practices"[107] to the IoT becomes increasingly difficult to

---

104. EPIC Complaint, *supra* note 87, at 5–6 (describing security and data privacy risks with information collected by the Cayla and i-Que toys, which are dolls with a companion app that captures the child's communications).

105. *See* Grant Gross, *Privacy Groups Urge Investigation of "Internet of Toys"*, CIO (Dec. 5, 2016, 9:05 PM), http://www.cio.com/article/3147335/internet-of-things/privacy-groups-urge-investigation-of-internet-of-toys.html (describing how privacy groups in the United States and seven European countries will ask consumer protection agencies to investigate the maker of Internet toys Cayla and i-Que intelligence robots because the groups are "worried about the lack of consumer and data protection for children in the rapidly emerging internet of things" (quoting Jeffrey Chester, Center for Digital Democracy executive director)).

106. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD i (2015) [hereinafter FTC IOT REPORT], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

107. Since the late 1990s, the FTC has espoused basic fair information practice principles, focusing on notice and awareness, choice and consent, access and participation, integrity and security, and enforcement and redress. *See* FED. TRADE

regulate in a predictable and fair manner as the sources, richness, and uses of data expand.[108] The federal government's regulation of information privacy is grounded historically in an analog, and only recently digital, world.[109] Additionally, regulatory systems can be slow to adapt to change. The tools our regulators possess to protect privacy interests have unsurprisingly failed to catch up to the challenges the IoT presents. Additionally, today's regulators are confronted with the challenge of protecting information privacy without unreasonably inhibiting the innovations that the IoT promises for our society.

The remainder of this Article will review recent FTC settlements that illustrate how the FTC has been creative in taking traditional consumer protection concepts and molding those rules into new tools that work for today's untraditional, magical world of the IoT. Part III describes information privacy in detail, how it has been traditionally regulated, and how the FTC is best situated to serve as the primary regulator of information privacy and the IoT. Part IV analyzes the recent FTC decisions and explains new trends regarding the use of "deceptive" practices and "unfairness" when regulating the IoT. Finally, Part V sets forth predictions of how the FTC under the new administration will handle the IoT, and it provides suggestions for how the FTC should be both proactive and reactive when regulating the IoT.

III. REGULATION OF INFORMATION PRIVACY IN THE UNITED STATES

A. Information Privacy

The right to privacy has been widely examined, but over time it has generally come to embody several concepts, among them rights of "personhood, intimacy, secrecy, limited access to the self, and control over information."[110] With respect to the IoT, control over

---

COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7–11 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

108. *See generally* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (demonstrating the effect of an increasingly digital society on fair information practices).

109. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 9–10 (1973) (describing the growing use of computers to process personal data and the lack of protections for the data).

110. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 45 (5th ed. 2015).

information, or "informational privacy," by the user is most relevant.[111] The Stanford Encyclopedia of Philosophy defines informational privacy as a right "to have direct or indirect control over access to (1) information about oneself, (2) situations in which others could acquire information about oneself, and (3) technology that can be used to generate, process or disseminate information about oneself."[112]

The concept of informational privacy is by no means new, and the just outcome that it seeks for individuals—personal control over information—is at the heart of the IoT privacy discussion.[113] However, the advent of the Internet, emergence of the IoT, and advances in data processing have created a wealth of information that will test our ability to offer personal control over data in a meaningful way.

B. The Sectoral Approach to Privacy Regulation in the United States

In the United States, the sources of privacy regulations are "sectoral" in nature.[114] There is no comprehensive federal privacy law addressing data protection. Instead, certain laws govern certain types of data, and certain agencies regulate certain entities that collect and process that data.[115] For example, health data is protected under the

---

111. Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* 3 (2014) (demanding that despite the growth of IoT in the European Union (EU), "users must remain in complete control of their personal data throughout the product lifecycle"); CROSS-DEVICE TRACKING, *supra* note 82, at 16 (noting that "it is important that consumers are informed and able to control tracking that occurs across their devices"); *see also* PEW RESEARCH CTR., THE INTERNET OF THINGS WILL THRIVE BY 2025, at 9 (2014), http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf (stating that the growth of the IoT raises "substantial concerns" about consumers' ability to control their own information).

112. *Privacy and Information Technology*, STAN. ENCYCLOPEDIA PHIL. (Nov. 20, 2014), https://plato.stanford.edu/entries/it-privacy.

113. *See* Shawn A. Johnson, *A Law and Economics Approach to Privacy Policy Misstatements: Considering the Need for a Cost-Benefits Analysis in the FTC's Deception Framework*, 18 COLUM. SCI. & TECH L. REV. 79, 83 (2016) (summarizing the historical development of the concept of privacy).

114. *Id.*

115. *See generally* Chris Hoofnagle, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: United States of America*, EUR. COMMISSION 11–14 (2010) (listing and describing American sectoral privacy laws); Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada, and Europe*, 29 CONN. J. INT'L L. 257, 289 (2014) (discussing the sectoral development of privacy in the United States).

Health Insurance Portability and Accountability Act[116] (HIPAA) and the Health Information Technology for Economic and Clinical Health Act[117] (HITECH); multiple laws govern financial data including the Fair Credit Reporting Act[118] (FCRA) and the Gramm-Leach-Bliley Act[119] (GLBA); and the Children's Online Privacy Protection Act[120] (COPPA) regulates the privacy of data relating to children.

Various federal agencies oversee privacy in connection with the industries they regulate. For example, the Federal Communications Commission (FCC) regulates privacy relating to the Do Not Call List[121] and cable subscriber privacy.[122] The United States Department of Health and Human Services (HHS) Office of Civil Rights (OCR)

---

116. Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPPA] (codified as amended in scattered sections of 26, 29, and 42 U.S.C.); *see also Summary of the HIPAA Privacy Rule*, DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last updated July 26, 2013) (discussing the statutory background, obligations, and scope of HIPAA).

117. Pub. L. No. 111-5, § 13,001, 123 Stat. 115, 226 (2009) [hereinafter HITECH] (codified as amended in scattered sections of 42 U.S.C.); *see also HHS Strengthens HIPPA Enforcement*, DEP'T OF HEALTH & HUM. SERVS. (Oct. 30, 2009), https://wayback.archive-it.org/3926/20131018161347/http://www.hhs.gov/news/press/2009pres/10/20091030a.html (explaining how the HITECH Act expands enforcement actions under HIPAA).

118. 15 U.S.C. § 1681 (2012) [hereinafter FCRA]; *see also* FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT 1 (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf (describing the FCRA as the law that "governs the collection, assembly, and use of consumer report information").

119. Pub. L. 106-102, 113 Stat. 1338 (1999) [hereinafter GLBA] (codified in scattered sections of 12 and 15 U.S.C.); *see also How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N (July 2002), https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (outlining the privacy requirements of GLBA).

120. 15 U.S.C. §§ 6501–6506 [hereinafter COPPA]; *see also* FED. TRADE COMM'N, PROTECTING CHILDREN'S PRIVACY UNDER COPPA: A SURVEY ON COMPLIANCE 1 (2002) (stating that COPPA directed the FTC "to set forth limited rules governing the online collection of personal information from children 12 and under").

121. *See Stop Unwanted Calls, Texts and Faxes*, FCC, https://www.fcc.gov/consumers/guides/stop-unwanted-calls-texts-and-faxes (last updated June 21, 2017).

122. *Cable Companies' Record Retention and Cable Subscriber Privacy*, FCC, https://www.fcc.gov/consumers/guides/cable-companies-record-retention-and-cable-subscriber-privacy (last updated June 13, 2017); *see also Protecting Your Privacy: Phone and Cable Records*, FCC, https://www.fcc.gov/consumers/guides/protecting-your-privacy (last updated Oct. 25, 2016).

helps to ensure the privacy and security of health information.[123] For a more obscure example, consider that the National Highway Transportation Safety Administration (NHTSA) has recently begun reviewing the information privacy implications of autonomous (self-driving) vehicles and vehicle-to-vehicle communications.[124]

Complicating matters even further, states also regulate information privacy explicitly in some cases but more commonly through the exercise of consumer protection powers.[125] States may have their own legislation regulating certain types of information. For example, more than a decade ago, California passed the California Online Privacy Protection Act[126] (CalOPPA). Nearly every state now has its own data security or breach notification laws that to some extent mandate reasonable security practices and set rules for when and how companies must notify individuals when their personal information has been compromised.[127]

C. Role of the Federal Trade Commission

Unlike sector-oriented federal agencies, such as the Department of Defense, HHS, FCC, NHTSA, or the FDA, when it comes to matters of information privacy, the FTC has statutory authority over a relatively broad—and overlapping—set of actors and activities.[128]

---

123. *Office for Civil Rights: About Us*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/ocr/about-us (last updated Sept. 6, 2015).

124. *See* NHTSA, FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY 6 (2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

125. *See, e.g.*, Missouri Merchandising Practices Act, MO. REV. STAT. § 407.020 (2016) (allowing local prosecutors or the state's Attorney General to press charges against people who knowingly use deceptive business practices in a consumer transaction); NAT'L CONSUMER LAW CTR., CONSUMER PROTECTION IN THE STATES, APPENDIX B: STATE-BY-STATE SUMMARIES OF STATE UDAP STATUTES (2009), https://www.nclc.org/images/pdf/udap/analysis-state-summaries.pdf (analyzing each state's consumer protection laws through their adoption of the Uniform Deceptive Trade Practices Act); *see also* PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org (last visited July 4, 2017) (educating consumers about their privacy rights).

126. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2017); *see also California Online Privacy Protection Act (CalOPPA)*, CONSUMER FED'N CAL., https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3 (last updated July 29, 2015).

127. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS. (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (listing the statutes for the forty-seven states that maintain state data breach notification laws).

128. *See* Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, AM. B. ASS'N, http://www.americanbar.org/groups/young

Pursuant to section 5 of the FTC Act,[129] the FTC may assert privacy-related claims for "unfair or deceptive acts or practices *in or affecting commerce*."[130] This means that the FTC's jurisdiction is nationwide and extends to companies irrespective of industry (except where an industry is carved out for exclusive oversight by other regulators).[131] Consequently, the FTC's jurisdiction closely intersects with[132] and overlaps[133] other sectoral regulations and regulatory authorities within the United States.

The FTC has used this authority to establish the broadest and most impactful jurisprudence in the area of information privacy, contending in guidance and through enforcement actions that consumers are entitled to "fair information practices," such as notice, choice, access, accuracy, data minimization, security, and accountability.[134] In their article "The FTC and the New Common Law of Privacy," Daniel Solove and Woodrow Hartzog detail how the FTC came to be the "de facto" data protection authority for the United States,[135] tracing that path from its role as overseer of certain

---

_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html (last visited July 4, 2017); *see also* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2014 PRIVACY AND DATA SECURITY UPDATE 1 (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

129. Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41–58 (2012).

130. *Id.* § 45(a)(1) (emphasis added). *But see* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 610–12 (D.N.J. 2014) (challenging the notion that the FTC has authority to regulate this area through enforcement actions, an argument the court rejected), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

131. These are statutory exceptions to the FTC's jurisdiction over commercial activities, including with respect to banks, airlines, insurance, and the common carrier activities of telecommunications services providers. § 45(a)(2). The FTC also does not have jurisdiction over most nonprofit organizations. *See infra* Section V.B (discussing the FTC's venture into offering comments and guidance to industry-specific regulators); *see, e.g.*, *Sharing Consumer Health Information? Look to HIPAA and the FTC Act*, FED. TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act (providing guidance for companies that may be subject to both HIPAA and the FTC Act).

132. *See infra* notes 262–63 and accompanying text (discussing guidance provided by the FTC to other regulators like the FCC and NHTSA).

133. Some FTC enforcement actions are joint settlements with state attorneys general. Indeed, the VIZIO resolution discussed in Section IV.D, *infra*, was a joint resolution with the New Jersey Division of Consumer Affairs.

134. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

135. *Id.* at 600–06; *see also* Steven Hetcher, *The* De Facto *Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 131 (2000) ("[T]he FTC is fairly viewed as a nascent, *de facto* federal privacy commission."); James Taylor & Jill

privacy statutes in the mid-to-late 1990s through the FTC's engagement with the early Internet privacy policies in the 2000s.[136]

Because of its broad, nationwide authority over activities in interstate commerce, the FTC is uniquely situated to address the privacy concerns inherent to the IoT.[137] However, while it has broad subject-matter jurisdiction under section 5—compared to the Consumer Financial Protection Bureau, for example—the FTC has a relatively circumscribed set of tools to set policy or carry out law enforcement functions. The FTC is limited to Magnuson-Moss rulemaking authority under section 5,[138] which effectively leaves the FTC with just two means to advance an information privacy agenda: namely, enforcement of violations of section 5 and informal guidance, including guidance published in the Code of Federal Regulations but lacking the formal nature of rulemaking. The sections below set forth the enforcement authority of the FTC for privacy actions, specifically the use of the "unfairness standard" and "deceptive" practices standard. The use of FTC guidance and its importance when regulating the IoT will be discussed in greater detail in section five.

D. The FTC's Section 5 Enforcement Authority

The FTC Act empowers the FTC to bring enforcement actions when companies engage in "*unfair* or *deceptive* acts or practices in or

---

Westmoreland, *Recent FTC Enforcement Actions Involving Endorsements, Privacy and Data Security*, M/E INSIGHTS, Winter/Spring 2011, at 28, 28–29 ("The FTC continues to be the most active regulatory agency when it comes to privacy and data collection."); *FTC Issues Final Commission Report on Protecting Consumer Privacy*, INFOLAWGROUP (Mar. 26, 2012), http://www.infolawgroup.com/2012/03/articles/privacy-law/ftc-issues-final-commission-report-on-protecting-consumer-privacy ("The FTC has a front and center role in data privacy and enforcement.").

136. Solove & Hartzog, *supra* note 134, at 600.

137. *See* Christin S. McMeley, *Protecting Consumer Privacy and Information in the Age of the Internet of Things*, ANTITRUST, Fall 2014, at 71, 71 (describing the FTC's ability to adapt its procedures and principles to meet the challenges of new technologies across varies sectors); *see also A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (summarizing the statutes underlying the FTC's broad investigative, enforcement, and litigation authority).

138. *See* 15 U.S.C. § 57a (2012). This requires the FTC to navigate several procedural steps in the rulemaking process. *See, e.g.*, Jeffrey S. Lubbers, *It's Time to Remove the "Mossified" Procedures for FTC Rulemaking*, 83 GEO. WASH. L. REV. 1979, 1982–85 (2015); *see also* Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended in scattered sections of 15 U.S.C.).

affecting commerce."[139] When the FTC brings an enforcement action against a company, it prepares a complaint concerning the alleged conduct, and that complaint serves either as the basis for a settlement or the initiation of litigation either administratively or in federal court. If there is a settlement or a successful prosecution by the FTC, the resulting order typically contains certain common provisions binding the defendant: injunctive relief against continued violations, compliance and reporting obligations, recordkeeping requirements, employee acknowledgment of the order, and, in some cases, equitable monetary relief (e.g., disgorgement). The FTC is generally limited to equitable monetary relief, except where it has been given explicit statutory authorization to bring civil penalties.[140] Importantly, these orders often have a twenty-year term, and violation of the order can lead to civil penalties of up to $40,000 per violation.[141]

Solove and Hartzog argue that the FTC's enforcement actions have come to operate as a de facto common law of informational privacy,[142] and this "common law" is properly read to apply to the IoT equally. Enforcement actions by the FTC must be understood to apply universally, and the principles established through enforcement actions are expected to be followed.[143]

The FTC enforcement common law is rooted in longstanding FTC guidance on what constitutes deception and unfairness under section 5.[144] A brief review of this guidance is merited because it is essential for understanding some of the biggest hurdles for addressing IoT challenges using the FTC "common law."

1. The FTC's unfairness standard

The FTC may bring an enforcement action if it views a company's practices as being unfair.[145] The FTC Act explains that "unfair" acts or practices "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers

139. *See* 15 U.S.C. § 45(a)(1) (emphasis added).
140. *See, e.g.*, COPPA, 15 U.S.C. §§ 6501–6505.
141. *See generally FTC Raises Civil Penalty Maximums to Adjust for Inflation*, FED. TRADE COMMMISSION (June 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/ftc-raises-civil-penalty-maximums-adjust-inflation (detailing the final amendments to Commission Rule 1.98, which raised the civil penalty dollar amounts).
142. Solove & Hartzog, *supra* note 134, at 606–25.
143. *See id.*
144. *See id.* at 627–43.
145. 15 U.S.C. § 45(a)(1).

themselves and not outweighed by countervailing benefits to consumers or to competition."[146]

The FTC Policy Statement on Unfairness spends considerable time covering the "substantial injury" prong.[147] In order for a practice to be "unfair," it must "cause[] or [be] likely to cause substantial injury to consumers."[148] The injury cannot be trivial or merely speculative.[149] Consequently, most cases brought under the unfairness doctrine involve allegations of monetary harm.[150] Of course, practices that impose substantial health or safety risks on consumers have also been subject to scrutiny under the unfairness standard.[151]

It is difficult to find room for "privacy harms" in the FTC Policy Statement on Unfairness—for example, emotional harm caused by unauthorized access to or disclosure of private information is not likely connected to tangible harm. Indeed, the FTC Policy Statement on Unfairness expressly states that emotional impact and subjective harms are generally insufficient to support a claim of substantial injury.[152]

It is for this reason that until recently, the FTC has only alleged unfairness in instances involving the unauthorized disclosure of (1) directly-identifiable personal information (2) that is clearly "sensitive." For example, the FTC has brought enforcement actions against a company for posting illicit photographs of individuals, along with their

---

146. *Id.* § 45(n).

147. *See FTC Policy Statement on Unfairness*, FED. TRADE COMMISSION (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (highlighting that "unjustified consumer injury" is the focus of the FTC Act).

148. 15 U.S.C. § 45(n).

149. *FTC Policy Statement on Unfairness*, *supra* note 147.

150. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 622–23 (D.N.J. 2014) (accepting that allegations of financial injury resulting from fraud are sufficient to plead a substantial injury), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *see also* Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985) (explaining that most substantial injury cases would include monetary harm); Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1236–38 (2017) (arguing for the adoption of section 5's unfairness doctrine in requiring companies whose cybersecurity has been breached to notify interested parties).

151. *See generally FTC Policy Statement on Unfairness*, *supra* note 147.

152. *See id.* (stating that emotional harm, such as "harassing late-night telephone calls" and "high-pressure sales tactics," can serve as the basis for substantial injury "[i]n an extreme case . . . where tangible injury could be clearly demonstrated" based on subjective or emotional harm); *see also Am. Fin. Servs. Ass'n*, 767 F.2d at 972–74 (explaining that threats of seizure of secured assets can serve as the basis for substantial injury, and such an injury "is not limited to psychological harm" because "[t]he consumer may default on other debts or agree to enter refinancing agreements" or "forego assertion of valid defenses").

names and contact information, without consent;[153] where a company collected and transmitted usernames, passwords, financial account information and other sensitive personal information without consent;[154] and where the FTC has alleged that sensitive health information was not adequately protected from unauthorized disclosure.[155]

A practice is not unfair, however, if it is "reasonably avoidable."[156] A consumer can reasonably avoid a substantial injury where "they have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end."[157] This is the basis for most notice and consent forms: if a practice causes or is likely to cause substantial injury, then the company should provide appropriate notice and sufficient consent obtained prior to engaging in the practice. Otherwise, a data practice may be vulnerable to liability under the "unfairness" doctrine.

2. The FTC's deception standard

The FTC may also bring an enforcement action if a company engages in deceptive acts or practices.[158] In 1983, the FTC published the FTC Policy Statement on Deception, which explained that deceptive acts or practices involve a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[159] In other words, a practice is deceptive within the meaning of section 5 "(1) if it is likely to mislead consumers acting reasonably under the circumstances (2) in a way that is material."[160] Whether a misrepresentation is likely to mislead is based on the "net impression that it is likely to make on the

153. *See In re* Craig Brittain, No. C-4564, 2015 WL 9702431, at *4–5 (F.T.C. Dec. 28, 2015).

154. *See In re* UPROMISE, Inc., No. C-4351, 2012 WL 1225058, at *3–4 (F.T.C. Mar. 27, 2012).

155. *See In re* LabMD, Inc., No. 9357, 2015 WL 4967222, at *2–3 (F.T.C. Aug. 10, 2015).

156. 15 U.S.C. § 45(n) (2012).

157. Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1365 (11th Cir. 1988) (citation omitted).

158. 15 U.S.C. § 45(a)(1).

159. FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION 2 (1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

160. FTC v. Cyberspace.com LLC, 453 F.3d 1196, 1199 (9th Cir. 2006); *see also* FTC v. Tashman, 318 F.3d 1273, 1277 (11th Cir. 2003) ("To establish liability under section 5 of the FTCA, the FTC must establish that (1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances; and (3) the representation was material.").

general populace."[161] The FTC's analysis requires "'common sense,' and . . . a section 5 violation is not determined by fine print, technicalities, and legalese."[162]

In approaching the issue of materiality, the FTC Policy Statement on Deception explained that a "'material' misrepresentation or practice is one which is likely to affect a consumer's choice of or conduct regarding a product. In other words, it is information that is important to consumers."[163] The guidance goes on to state that "the Commission presumes that express claims are material . . . [w]here the seller knew, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false."[164] The FTC Policy Statement on Deception also recognizes that claims or omissions that "significantly involve health, safety, or other areas with which the reasonable consumer would be concerned" are presumptively material.[165]

Most disclosures about company privacy practices are, of course, not made in traditional marketing and advertising materials presented to consumers but instead appear in a company's privacy policy presumably published on the Internet. However, while the posting of privacy policies is widely accepted practice and generally expected, apart from state laws and COPPA, it is generally *not required* under rule or regulation.[166] However, if a privacy policy is *voluntarily* posted, the FTC may review it for accuracy under its deception guidelines.[167]

Indeed, FTC enforcement actions on privacy have generally focused on allegations of deceptive privacy policies as opposed to allegations of unfairness, and this is where we begin our discussion of recent FTC cases below.

---

161. FTC v. EMA Nationwide, Inc., 767 F.3d 611, 631 (6th Cir. 2014) (quoting Nat'l Bakers Servs., Inc. v. FTC, 329 F.2d 365, 367 (7th Cir. 1964)).

162. FTC v. AMG Servs., Inc., 29 F. Supp. 3d 1338, 1365 (D. Nev. 2014) (quoting FTC v. Commerce Planet, Inc., 878 F. Supp. 2d 1048, 1063 (C.D. Cal. 2012)).

163. *FTC Policy Statement on Deception*, *supra* note 159.

164. *Id.*

165. *Id.*

166. *See* Johnson, *supra* note 113, at 101.

167. The FTC has settled a number of complaints where an alleged omission or false statement in a privacy notice was the jurisdictional hook or basis for negotiating the stipulated relief in the consent decree. *See, e.g.*, Complaint at 2–3, Nomi Techs., Inc., No. C-4538, 2015 WL 5304114 (F.T.C. Aug. 28, 2015), https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (reviewing Nomi Technology's deceptive statements within its published privacy policies).

IV. RECENT FTC GUIDANCE, ENFORCEMENT, AND THE CHALLENGE OF THE INTERNET OF THINGS

The FTC has pursued numerous policy initiatives aimed at enhancing consumer privacy that inform its enforcement work. Of note here, the FTC has hosted workshops and issued reports recommending best practices aimed at (1) improving privacy in the mobile ecosystem (February 2013);[168] (2) increasing transparency within the data broker industry (May 2014);[169] (3) maximizing the benefits of big data while mitigating its risks, particularly for low-income and underserved consumers (January 2016);[170] and (4) highlighting the privacy and security implications of the IoT (January 2015),[171] among other areas.

The FTC's 2015 IoT Report, in particular, contained important guidance for businesses venturing into the IoT market. The Report encouraged "data minimization."[172] A company should "collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect," and "[i]f a company determines that none of these options work, it can seek consumers' consent."[173] In short, consent is not required where the data collected is de-identified and not particularly sensitive.[174]

In addition, the FTC reiterated its view "that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer."[175] On the other hand, "[n]otice and choice is particularly important when sensitive data is collected"[176] as well as for data collections that are unexpected.[177]

---

168. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

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

170. *See* FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

171. *See* FTC IOT REPORT, *supra* note 106.

172. *Id.* at 33.

173. *Id.* at 38–39.

174. Indeed, the FTC IoT Report explicitly stated that "[c]ompanies can use . . . de-identified data without having to offer consumers choices." *Id.* at 43.

175. *Id.* at 40.

176. *Id.* at 39.

Enforcement is the lynchpin of the FTC's approach to privacy protection, however, and three recent FTC cases reveal how the FTC has flexibly used its section 5 "deception" authority to regulate information privacy issues that are fundamental to the IoT—specifically, so-called consumer "tracking."[178]

However, the first FTC enforcement action regarding IoT devices—*VIZIO*, which ended in a stipulated order in February 2017[179]—has potentially upended the need for creative application of the FTC's deception authority, creating a new theory of liability under its "unfairness" authority in section 5. *VIZIO* creates several new rules of the road, including a new "unfair tracking" standard and "consent and choice" rules that are applied to a new category of "sensitive" information.[180] Until the FTC is fully staffed with new Commissioners and leaders, it may be premature to assess the long-term impact of this case except to say that all entities that engage in highly specific profiling and tracking practices—even on a basis that was formerly considered "anonymous"—should reevaluate whether and how they provide detailed notice and secure individual consent from consumers' use of a particular IoT device.

A. Nomi Technologies, Inc.

The FTC's 2015 settlement with Nomi signaled a new era in the FTC's supervision of the IoT. The Complaint alleges that in January 2013, Nomi began marketing its "Listen" technology to help retail stores learn more about customer traffic.[181] Nomi deployed sensors at participating retail stores and, in other instances, used the stores' WiFi routers to collect the unique media access control ("MAC") addresses being broadcast by the mobile devices of customers.[182] In addition to these device identifiers, Nomi collected other information, such as WiFi signal strength—to determine a device's

177. *Id.* at 43.

178. *See* Complaint at 3, United States v. InMobi Pte Ltd., No. 3:16-cv-3474 (N.D. Cal. June 22, 2016) [hereinafter *InMobi* Complaint]; Complaint at 1, *In re* Nomi Techs., Inc., No. C-4538, 2015 WL 5304114 (Aug. 28, 2015) [hereinafter *Nomi* Complaint]; Complaint ¶¶ 3, 5, Turn, Inc., No. 152-3099, 2016 WL 7448417 (F.T.C. Dec. 20, 2016) [hereinafter *Turn* Complaint].

179. *See* FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

180. *See infra* Section IV.D (explaining why *VIZIO* was a groundbreaking application of the FTC's unfairness authority).

181. *Nomi* Complaint, *supra* note 178, at 1–2.

182. *Id.* at 1.

proximity to the sensor or router—and the date and time that the MAC address was collected—to track customers' activity over time.[183] Neither Nomi nor its retail clients were alleged to have paired any of this tracking data with known shoppers.[184]

Instead, Nomi collected and analyzed this data to provide aggregate analytics to the participating retail store clients.[185] Retail stores could learn from this data the percentage of individuals passing by that actually entered the store, how long customers spent at their store on average, the rate of repeat customers, and how many customers visited multiple locations of the same retail chain.[186] Again, Nomi was never alleged to have used the data to re-target marketing to customers' devices nor to have attempted to identify the individual customers.

Nomi (and its retail clients) did not publish notices on the premises of participating retail stores explaining its data collection practices.[187] Customers were not specifically made aware of Nomi's tracking practices in the context of their visits to, or other interactions with, retailers.[188] Customers were not alerted to the presence of tracking technology at all and had no means to encounter the Nomi brand.[189] However, Nomi did have an online privacy policy, through which a hypothetical consumer might have read that she could opt-out of the data collection either online or at the retail stores where the data collection was enabled.[190] The online privacy policy was not required to be seen or consented to by a shopper, and a shopper would have to know on their own which retailers used the technology and where to find the policy.[191]

The concern that Nomi's business practices presented was that its technology tracked devices across retail locations and over time without the customer (device owner) receiving notice or providing consent. Some may describe it as *unfair* that devices could be tracked

183. *Id.* at 1–2.

184. Taking further precautions, Nomi "hashed" the MAC addresses from the mobile devices before storing them on servers. *Id.* at 2. Hashing obscures the MAC address but provides the same unique identifier each time the address is run through the hash function and therefore is potentially reidentifiable to a particular device by anyone with access to the hash algorithm. *Id.*

185. *Id.*

186. *Id.* at 1–2.

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.* at 2–3.

191. *Id.* at 2.

without notice and consent. However, the FTC settled the case with Nomi on *deception* grounds.[192] The FTC alleged that Nomi's privacy policy was deceptive because (1) the privacy policy stated that customers could opt-out at retail stores, even though retail stores implemented no separate mechanism for opting out,[193] and (2) by claiming that customers could opt-out at retail stores, the privacy policy *implied* that Nomi would provide a notice at each retail store where they were collecting data so that customers would know to opt out.[194]

Simply put, as noted by the dissenting Commissioners, if Nomi as a technology provider leveraging smartphone technology on behalf of its business customers had not *voluntarily* posted a privacy policy, then there would have been no grounds to allege deception. There was no affirmative source of law requiring that Nomi publish a privacy statement addressing end user data at all. However, because Nomi had a privacy policy—a public pledge as the FTC has characterized it—with which it technically was not in compliance, Nomi was liable for deception under section 5.[195] For FTC Commissioner Maureen Ohlhausen, who vigorously dissented, the decision to file a Complaint merely incentivized a business-to-business vendor to abstain from providing any voluntary opt-out or public privacy disclosure at all.[196] Indeed, Nomi did not respond to the settlement by posting opt-out notices at retail stores, but instead, it merely deleted any reference of opt-outs from its privacy policy.[197]

In *Nomi*, the FTC applied its deception authority in a controversial way to address a concerning (to some) practice in the IoT—where users were not directly identifiable but their activities were nevertheless being tracked. *Nomi* made sense as a deception case because this sort of retail tracking likely did not otherwise satisfy the requirement of "substantial injury" to support a finding of unfairness.[198] The highly specific data Nomi collected was perhaps not deemed "sensitive" because it was not directly personally-

192. *See, e.g.*, Decision and Order at 2, *In re* Nomi Techs., Inc., No. C-4538, 2015 WL 5304114 (F.T.C. Aug. 28, 2015) (ordering Nomi not to "misrepresent in any manner" customers' notice and choices).

193. *Nomi* Complaint, *supra* note 178, at 3.

194. *Id.*

195. *Id.*

196. *Nomi*, 2015 WL 5304114 (Ohlhausen, dissenting).

197. Johnson, *supra* note 113, at 105.

198. *See id.* at 98 ("Despite the fact that the FTC considers precise geolocation date to be sensitive personal information, the risk of concrete harm does not arise in the case of Nomi's tracking practices." (citation omitted)).

identifiable data.[199] However, the case—certainly in hindsight—was a strong signal that certain members of the Commission were troubled by highly specific and potentially surprising profiling and tracking. Notice and choice were lacking in this case, except in a privacy policy that almost certainly none of the data subjects read or saw (and which contained the "false" promise of store-specific opt-outs).

B. United States v. InMobi PTE, Ltd.

The FTC used its deception authority in *InMobi* to police a similar issue of end user tracking. As in *Nomi*, the FTC's case against InMobi challenged a defective privacy control under claims of deception rather than unfairness.[200] InMobi, according to the Complaint, marketed a software development kit ("SDK") that could be integrated into mobile applications to enable the delivery of advertisements (for example, banner ads) within the mobile app environment.[201] A developer looking to monetize a new app could incorporate this SDK into its app to deliver ads to app users.[202]

The InMobi SDK enabled ads to target consumers based on geolocation data.[203] Unless disabled, the InMobi SDK would access the device's geolocation application programming interface ("Geolocation API") and use that data to target ads delivered through the InMobi SDK.[204] Consistent with requirements by both Android and iOS, after installing apps with the InMobi SDK embedded, device users were prompted to grant the app access to the Geolocation API.[205] By disabling the Geolocation API, neither the Android nor iOS device would make geolocation data available to the InMobi SDK.[206]

However, the InMobi SDK also collected data about the WiFi networks to which the devices were connected.[207] For users who did not disable the Geolocation API, InMobi simultaneously collected both latitude and longitude through the Geolocation API *and* details about the WiFi network to which each device was connected at that moment.[208] With these two data sets, InMobi was able to populate a database that

199. *Id.*
200. *InMobi* Complaint, *supra* note 178, at 13–14.
201. *Id.* at 3.
202. *Id.*
203. *Id.* at 3–4.
204. *Id.* at 4.
205. *Id.* at 5.
206. *Id.*
207. *Id.*
208. *Id.* at 6.

mapped each WiFi network to the latitude and longitude that the Geolocation API delivered.[209] Consequently, the locations of app users *who had disabled access* to the Geolocation API could nevertheless be pinpointed by merely looking up the location of the WiFi network they were using.[210] InMobi targeted ads to users based on the location they derived through this WiFi network lookup process.[211]

As with Nomi, the concern InMobi's practices presented was that InMobi tracked geolocation without the device owner's actual notice or consent—indeed, some would argue, in contravention of the express intentions of the user.[212] The FTC alleged that InMobi's practices were deceptive because they were allegedly false as compared to certain representations made *not* to app end users but to the app developers who incorporated the InMobi SDK.[213] The Complaint alleged that InMobi's SDK integration guide and product marketing materials suggested that it was the Geolocation API feature alone that enabled geo-targeting.[214]

Like in *Nomi*, the FTC applied its deception authority flexibly to address the alleged tracking of highly specific consumer activities on their connected devices without notice and consent. But unlike *Nomi*, the FTC did not look to consumer disclosures; instead, InMobi was principally found liable for having made deceptive representations to its business partners (app developers), *not to consumers*.

C. Turn, Inc.

For the third time, the FTC used its deception authority to address a matter of "tracking" in *Turn, Inc.* The case involved a similar issue in which a defective control was challenged under the FTC's deception authority and not unfairness.[215] Turn, Inc. ("Turn") offers a digital marketing platform ("DMP") designed to allow advertisers to target consumers across devices.[216] The digital advertising ecosystem Turn relied on used various identifiers and techniques to try to connect user activity across the Internet and across devices to inform (personalize) the advertising delivered to particular users.[217]

---

209. *Id.*
210. *Id.*
211. *Id.*
212. *See id.* at 8.
213. *Id.* at 9.
214. *Id.*
215. *Turn* Complaint, *supra* note 178, ¶¶ 16–19.
216. *Id.* ¶ 3.
217. *Id.* ¶ 5.

Many will be familiar with two types of identifiers Turn used to track digital activity across devices: cookies and device advertising identifiers. Cookies, as the *Turn* Complaint describes, are unique text files stored in a browser that allow a company like Turn to identify the user accessing a website.[218] Device advertising identifiers, including Google's advertising ID and Apple's "Identifier for Advertisers" (IDFA), allow companies like Turn to recognize a device that accesses a website.[219]

Internet users looking to control their information privacy by preventing efforts to track their activity across devices can generally do so by deleting their cookies and resetting their device advertising identifiers.[220] But Turn also collected another type of identifier called a Unique Identifier Header ("UIHD") from those using the Verizon Wireless network.[221] This UIHD encoded web traffic by Verizon Wireless network users and, like InMobi, which allegedly mapped WiFi network data to location data, Turn allegedly mapped its UIHD data to device advertising identifiers and cookies.[222] As a result, if a user of the Verizon Wireless network attempted to stop efforts to track cross-device activity by deleting cookies and resetting device advertising identifiers, Turn could easily read the UIHD on later device activity and know which cookies to replace in the user's browsers and connect the reset device advertising identifier to the existing profile.[223]

Again, the FTC attacked Turn's practice on deception grounds and not grounds of unfairness. According to the Complaint, Turn voluntarily posted privacy guidelines, which stated, in pertinent part, that users could opt-out of tracking by opting out of accepting cookies.[224] The Complaint alleged that this was deceptive because doing so would not ultimately disable tracking for those using the Verizon Wireless network.[225] The enforcement action was settled, and Turn entered into a consent order with the FTC.[226]

---

218. *Id.*
219. *Id.* ¶ 6.
220. *Id.* ¶ 7.
221. *Id.* ¶ 8.
222. *Id.* ¶¶ 9–10.
223. *Id.*
224. *Id.* ¶¶ 11–14.
225. *Id.* ¶¶ 16–20.
226. Agreement Containing Consent Order, Turn Inc., No. 152-3099, 2016 WL 7448417 (F.T.C. Dec. 20, 2016).

D. Federal Trade Commission v. VIZIO, Inc.

Previous seminal FTC cases concerning highly specific tracking of users via mobile devices looked to deceptive grounds as a basis to effectively impose notice and choice principles in those new use cases. On February 6, 2017, however, acting jointly with the New Jersey Attorney General, the FTC filed its first true IoT privacy enforcement case against Smart TV manufacturer VIZIO, Inc.[227] The case applied the FTC's section 5 unfairness authority to an IoT "tracking" case for the first time and attempted to plead a new cause of action called "unfair tracking."[228] The case resulted in a Stipulated Order in which VIZIO agreed to a new set of notice-and-choice ground rules for the collection and use of information relating to television viewing content.[229]

The Ccomplaint alleged that VIZIO offered a feature called "Smart Interactivity" that used embedded "automated content recognition" (ACR) software in VIZIO Smart TVs.[230] ACR software can automatically detect the content appearing on a television.[231] VIZIO allegedly collected information about what was showing on VIZIO TVs ("viewing data") and shared it with authorized data partners who used the viewing data to carry out familiar use services: (1) the generation of summary reports and analytics about device (television) usage and (2) ad retargeting.[232] According to the Complaint, neither process required associating viewing data with directly personally-identifiable information, such as name or contact information.[233] Instead, the Complaint alleges that VIZIO paired viewing data with device IP addresses, and that IP addresses were sometimes used to (1) enhance data with demographic information to allow for richer analysis and (2) match TVs to other devices for ad retargeting and other analytical purposes.[234]

As alleged, VIZIO generally provided notice to consumers in the form of an online privacy policy[235] and at least two on-screen pop-up notifications, the first of which alerted users that the privacy policy had

---

227. Complaint at 1–2, 4, F.T.C. v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) [hereinafter *VIZIO* complaint]. One of the authors of this piece, Scott Jones, represented VIZIO, Inc. in the matter.

228. *Id.* ¶ 35.

229. Stipulated Order at 4, *VIZIO*, No. 2:17-cv-00758.

230. *Id.* ¶¶ 9, 22.

231. *Id.* ¶ 14.

232. *Id.* ¶ 16.

233. *Id.* ¶ 17.

234. *Id.* ¶¶ 16–17.

235. *Id.* ¶ 20.

changed and the second of which described the collection of viewing data and pairing with IP address.[236] In addition, the Complaint alleged that the televisions were equipped with a choice mechanism by design: the settings menu on VIZIO TVs included an option to turn off viewing data collection by turning off the "Smart Interactivity" feature.[237]

Count 1 of the Complaint alleged a cause of action pled for the first time: "unfair tracking."[238] This allegation was unprecedented for several reasons. First, the count provided the full weight of the FTC's enforcement authority behind a concept it had only previously endorsed in informal speeches and a letter to the FCC: that an IP address could be treated as personally-identifiable or that, at the very least, the data associated with IP addresses is still in need of privacy protections even if it was not directly personally-identifiable.[239] Indeed, the Complaint specifically acknowledged that VIZIO's contracts with licenses prohibited the re-identification of viewing data; yet, this precaution was not sufficient to foreclose allegations of "unfairness."[240]

Second, the "unfair tracking" count created a new category of sensitive data: "viewing data."[241] The count states that consumers "would not expect" viewing data to be collected from their televisions,[242] and Commissioner Ohlhausen noted in her concurring statement that there may be policy reasons for treating viewing data as sensitive as evidenced by the Cable Privacy Act, which protected viewing data in other contexts.[243]

Taken together, the FTC alleged that VIZIO's collection and sharing of viewing data without sufficient notice and consent "caused or is likely to cause substantial injury" as is required to sustain a

---

236. *See* Exhibits A and B, *VIZIO, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017).

237. *VIZIO* Complaint, *supra* note 227, ¶¶ 20–22.

238. *Id.* ¶ 35.

239. *See, e.g.*, FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 20–25 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf [hereinafter SELF-REGULATORY PRINCIPLES] (asserting that in certain instances, the line between directly personally-identifiable data and data associated with an IP address or device identifiers is blurred such that privacy protections are prudent both for the former and the latter).

240. *VIZIO* Complaint, *supra* note 227, ¶¶ 17, 31–35.

241. *Id.* ¶¶ 32–34.

242. *Id.* ¶ 32.

243. Concurring Statement of Acting Chairman Maureen K. Ohlhausen, FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) [hereinafter Concurring Statement], https://www.ftc.gov/system/files/documents/public_statements/1070773/vizio_concurring_statement_of_chairman_ohlhausen_2-6-17.pdf.

section 5 claim for unfairness.[244] However, Commissioner Ohlhausen pointed out that the FTC must actually "determine whether the practice causes substantial injury" and explained that "[t]his case demonstrates the need for the FTC to examine more rigorously what constitutes 'substantial injury' in the context of information about consumers."[245] The link between viewing data and "substantial" injury is not apparent on the face of the Complaint.

The relief set forth in *VIZIO* was perhaps just as important as the new count for "unfair tracking." Section II of the Order established a new set of notice-and-choice ground rules for the collection of television viewing data:

First, prior to collection, notice must be provided.[246] That notice must appear "separate and apart" from a privacy policy or terms of use, and it must be "prominent(),"which means, among other things, unavoidable.[247]

Second, the notice must contain certain substantive elements, including a description of the types of viewing data that will be collected, what will be shared with third parties, and the purposes for sharing that data.[248]

Third, when the notice is provided, true "opt-in" consent must be collected from the consumer before viewing collection may be enabled.[249]

If a data collection practice is subject to this standard, the practical effects are clear. It is no longer sufficient to obtain opt-in consent through passive or even active assent to a privacy policy or terms of service. Before engaging in data collection, companies must comprehensively describe sharing and use under this new set of notice and choice ground rules. The company must provide notice to a consumer in a manner that the consumer cannot avoid, and the consumer must provide true opt-in consent ("I agree" or "Accept") upon receipt of the notice.[250]

The FTC in *VIZIO* established new unprecedented regulations of the IoT. The *VIZIO* case established a new count of "unfair tracking" and a new set of notice and choice rules. This settlement shows that the FTC is prepared to flexibly interpret the unfairness standard and willing to establish new standards and develop new tools to regulate

244. *VIZIO* Complaint, *supra* note 227, ¶ 33.
245. Concurring Statement, *supra* note 243.
246. Stipulated Order at 4, *VIZIO*, No. 2:17-cv-00758.
247. *Id.*
248. *Id.*
249. *Id.*
250. *Id.*

the IoT. These new rules of the road will require guidance for companies to follow moving forward.

V. GUIDING THE FUTURE OF THE INTERNET OF THINGS

Part IV's review of recent FTC enforcement cases reveals that the FTC initially looked to traditional concepts of deceptiveness to address issues concerning "tracking." But in its seminal IoT matter, the FTC adopted an unprecedented theory of "unfair tracking" that provides a new tool the FTC may use to address future IoT privacy cases. Unfair tracking was applied in *VIZIO* to newly defined sensitive "viewing data."[251] Now, robust notice and opt-in consent requirements apply to the collection of this data. The future implications of the recent *VIZIO* case have yet to unfold, but companies that capture and use viewing data will likely need to reevaluate their data practices to ensure they comply with the FTC's new rules of the road or will otherwise face potential enforcement action. It is important now for the FTC to provide future guidance for these new rules to ensure companies can continue to innovate while respecting the privacy issues at the heart of the FTC's recent enforcements.

Where the FTC of the Obama Administration was first to forge its way to regulate the IoT, the framework it produced is now for a new Commission, once in place under the Trump Administration, to apply. Within this new framework, the greatest tool in the new administration's FTC toolkit is now *proactive* guidance to industry, fellow regulators, and consumers about how it interprets and applies the "unfair tracking" standard to the intertwined web of the IoT.

A. Guidance to the IoT Business Community

Recent FTC cases and outcomes have created a new rubric for understanding how the FTC may expect companies to respect fair information practices within the IoT. And with new rules of the road, guidance and clarity with respect to applying these rules can help businesses move forward with technological advances that can provide both benefit and privacy protection to the consumers. The most salient issue now is whether the FTC means to expand the definition of "sensitive" data any further.

The notice and consent obligations established in the *VIZIO* Order apply at least to the collection of viewing data because the FTC described that data as sensitive in the Complaint.[252] Consequently,

---

251. *VIZIO* Complaint, *supra* note 227, ¶ 32.
252. *Id.* ¶ 33.

companies participating in the viewing data ecosystem (manufacturers, app developers, analytics companies, advertisers, and content providers that consume this data or the results of it) are now on notice of the then-constituted FTC's view that their practices must be permissioned through notice-and-consent standards outlined in Section II of the *VIZIO* Order.[253]

But the extent to which the "unfair tracking" standard will be applied to other data collected through the IoT is unclear. The benefits that the IoT delivers to customers often require "tracking" to some extent, such as tracking activity on a particular device across time, tracking a consumer's activity across devices at the same time, or both. Without boundaries having been established about what data is "sensitive," IoT companies must assess the risk that, if every new instance of "tracking" is not accompanied with the same notice and choice now required of Smart TV manufacturers, FTC enforcement may be forthcoming. This risk may create unnecessary drag on an industry with otherwise enormous potential to create consumer value. Others may take a different view and welcome a new framework for regulating a central IoT practice: the use of device identifiers, like IP addresses, to conduct individualized data tracking for aggregate analysis and personalized experiences and targeting.[254]

Regardless, additional instruction from the FTC is warranted, especially concerning what constitutes "sensitive" data, the "tracking" of which may cause "substantial injury" sufficient to support a section 5 unfairness claim. The FTC's Acting Chair, Maureen Ohlhausen, acknowledged in her concurrence in *VIZIO* that the FTC has "long defined sensitive information to include financial information, health information, social security numbers, information about children, and precise geolocation information."[255] And, to its credit, the FTC has been proactive in communicating these categories of sensitive information to the public.[256]

---

253. *See* FTC v. Wyndham Worldwide Corp, 799 F.3d 236, 257 (3d Cir. 2015) (noting that FTC enforcement decisions and consent decrees can provide fair notice to a party about FTC rules), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

254. *See* Tanya Dua, *How Smart TV Maker Vizio's Privacy Settlement Hurts Programmatic TV Advertisers*, DIGIDAY PULSE (Feb. 9, 2017), http://digiday.com/marketing/smart-tv-maker-vizios-recent-privacy-settlement-hurts-marketers-large; Andy Meek, *What Role Should the Government Play in Developing the Internet of Things?*, GUARDIAN (Oct. 14, 2015, 6:04 AM), https://www.theguardian.com/technology/2015/oct/14/government-regulation-internet-of-things.

255. Concurring Statement, *supra* note 243.

256. *See Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones & Your Privacy: Hearing Before the S. Comm. on the Judiciary Subcomm. for Priv., Tech., & the L.*,

None of these reports previewed the sensitivity of viewing data, however,[257] and to Acting Chair Ohlhausen, the expansion of "sensitive" data to include viewing data demonstrates "the need for the FTC to examine more rigorously what constitutes 'substantial injury' in the context of information about consumers."[258] Acting Chair Ohlhausen took an important step by calling for a dialogue on the subject in the coming period.

It is unclear what the result of those deliberations will be. The *VIZIO* Complaint included an allegation that viewing data is "sensitive" based in part on congressional intent and references the privacy protections established under the Cable Privacy Act.[259] Perhaps the FTC will conclude that absent expressions of congressional intent, the traditional categories of "sensitive" data will remain unchanged, and the expansion of the unfairness doctrine will stop there. Or perhaps the FTC will tie sensitivity to the locus of data collection (e.g., a place of worship or the home) or the ability to make sensitive inferences from the collected data (e.g., inferences about religious, political, or sexual preference), or the obviousness of the data collection to the consumer.

Whatever the result of those deliberations may be, it is important that they occur sooner rather than later because a ubiquitous, pervasive, fully-embedded IoT is not far away.[260] And while many will debate what the substantive rules should be, few would take the view that those substantive ground rules should await discovery through the enforcement process. The unavoidable delay between conduct and enforcement makes real-time guidance more important than ever. Indeed, by the time the *VIZIO* settlement was announced,

---

112th Cong. 1, 7–11 (2010) (statement of Jessica Rich, Deputy Dir. of the Bureau of Consumer Prot., FTC) (outlining FTC engagement with the public through privacy roundtables and note and comment rulemaking).

257. *See, e.g.*, CROSS-DEVICE TRACKING, *supra* note 82, at ii (recommending "heightened protections for sensitive information, including health, financial, and children's information"); FTC IOT REPORT, *supra* note 106 (describing privacy risks, including "the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information"); SELF-REGULATORY PRINCIPLES, *supra* note 239 (citing the risk of unauthorized access to or use of "sensitive data regarding health, finances, or children").

258. Concurring Statement, *supra* note 243.

259. *See VIZIO* Complaint, *supra* note 227, ¶ 23; *see also* 47 U.S.C. § 551 (2012) (governing the privacy of personally identifiable information collected by cable operators).

260. *See* Louis Columbus, *Roundup of Internet of Things Forecasts and Market Estimates, 2015*, FORBES (Dec. 27, 2015, 3:39 PM), http://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015.

numerous major Smart TV manufacturers were already engaged in automated content recognition.[261] If IoT tracking causes or is likely to cause "substantial injury" to consumers under the unfairness standard, regulators necessarily must ensure that companies are aware of that view before their technologies are put on the market.

B. Guidance to Other Regulators

Of course, as the FTC continues to wrestle with the challenging notice-and-choice issues that the ever-innovating IoT presents, it is equally important that the FTC continue to bring along other agencies and regulatory authorities with sectoral oversight to limit conflicting regulatory regimes. This has been an FTC priority over the past few years, and the FTC's efforts to make use of opportunities to synchronize their views with other agencies on matters of privacy and cybersecurity are commendable. For example, the FTC provided valuable commentary to the FCC on its proposed privacy rulemaking;[262] the FTC's Bureau of Consumer Protection offered comments on the NHTSA's Automated Vehicle Policy;[263] and the FTC has recently offered comments to the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) regarding the disclosure of security vulnerabilities.[264]

Additionally, FTC staff "participates in NTIA's multi-stakeholder group that is considering guidelines for facial recognition and the

---

261. *See, e.g.*, *Fall Technology Series: Smart TV*, FED. TRADE COMMISSION (DEC. 7, 2016, 1:00 PM), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv (discussing addressable TVs and automated content recognition at an FTC-sponsored conference in December 2016, shortly before the announcement of the *VIZIO* decision).

262. *See FTC Staff Provides Comment on FCC's Proposed Privacy Rulemaking*, FED. TRADE COMMISSION (May 27, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-staff-provides-comment-fccs-proposed-privacy-rulemaking (using FTC experience to suggest improvements to the FCC's proposed rulemaking regarding privacy protections by broadband Internet access service providers).

263. *FTC's Bureau of Consumer Protection Director Comments on NHTSA's Federal Automated Vehicle Policy*, FED. TRADE COMMISSION (Nov. 22, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftcs-bureau-consumer-protection-director-comments-nhtsas-federal (commending NHTSA's proposed industry guidelines that protect the private data of consumers).

264. *FTC Provides Comment to NTIA on Multistakeholder Initiative to Improve Cybersecurity Vulnerability Disclosure*, FED. TRADE COMMISSION (Feb. 16, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/ftc-provides-comment-ntia-multistakeholder-initiative-improve (outlining public comments submitted by the FTC to the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) on a proposed model disclosure policy created by an NTIA-led multistakeholder process).

Department of Energy's multi-stakeholder effort to develop guidelines for smart meters."[265] As the FTC noted, even without legislation, these efforts can result in "best practices for companies developing connected devices, which can significantly benefit consumers."[266] The FTC of the previous administration promised "to continue to participate in multistakeholder groups to develop guidelines related to the IoT."[267] For the IoT industry to succeed, the Trump Administration needs to continue to work with regulators and stakeholders and uphold the previous administration's promise to develop best practices and guidelines.

This practice must continue, and indeed, it must expand, especially as the FTC develops its views on the treatment of IP addresses and device identifiers and the sensitivity of data associated with those data elements. Other industry regulators may be too compartmentalized to appropriately weigh the balance of consumer interests that the FTC has long been entrusted with measuring, and the very nature of the IoT demands a comprehensive appreciation of what it means in the IoT to collect, share, and use data, both in terms of risk and benefit.

C. Guidance to the Consumer Marketplace

There is also an increasing role for consumer education of the IoT, especially if, through future deliberation, consumer "surprise" remains an essential element of the unfairness doctrine. The sophistication of the technologies (both hardware and software) that make up the IoT promises to bring enormous value to consumers. The "unfair tracking" count in the *VIZIO* Complaint included language stating that the connected device at issue (Smart TVs) was "a medium that consumers would not expect to be used for tracking."[268] In later describing the settlement, the FTC expressed concern for transparency and consent with respect to data collections consumers would not "expect" to occur.[269] If consumer surprise (or expectation) is the predicate for notice and consent, ensuring consumers' general awareness of how the IoT works will be

265. *See* FTC IOT REPORT, *supra* note 106, at 53.
266. *Id.*
267. *Id.*
268. *VIZIO* Complaint, *supra* note 227, ¶ 327.
269. *See* Lesley Fair, *What Vizio Was Doing Behind the TV Screen*, FED. TRADE COMMISSION (Feb. 6, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen (detailing VIZIO's consumer data tracking, the FTC's concerns for consumer privacy that these practices raised, and suggesting practices for other companies operating in the IoT).

important, lest all future innovation needlessly require cumbersome disclosures and consent. Worse, if surprise is to play a key component of the doctrine of unfairness, then the most innovative technologies will also face the hardest "sell." It is incumbent that the community of regulators (as well as businesses) help educate consumers on the basic functionality of the IoT in order to prevent unwarranted "surprise" caused by lack of education.

At its root, this education may be as simple as helping consumers distinguish between deterministic and probabilistic tracking, which are fundamentals of delivering on the promises of big data and personalized experiences.[270] Many IoT products and services simply cannot function without these "tracking" mechanisms, and the industry should educate consumers about them so they can gauge the privacy impact of new IoT innovations in an informed way.

Additionally, and in particular with respect to children and connected toys, parents need further education on what toy manufacturers are actually doing with the information pertaining to their children. Parents are not necessarily familiar with how "smart" toys perform the functions they perform, such as by "listening" or keeping photos or sound recordings of their children. Many of these background mechanics are necessary to provide the desired functionality, but parents lacking in knowledge about how these features work are ill-informed to make privacy decisions. There are substantial legal constructs in place to protect children's data,[271] and increased guidance on how to protect children using new "smart toys" or being recorded by home assistant devices like Siri, Amazon's Alexa, or Google Home is needed.[272]

The FTC supports guidance for consumers and in its recent report, "Internet of Things: Privacy & Security in a Connected World," states that "[c]onsumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available

---

270. *See Deterministic vs. Probabilistic Data Tracking: Which Is More Effective?*, APPLIFT (Sept. 24, 2015), http://www.applift.com/blog/deterministic-data (defining deterministic tracking as the analysis of data that is known to be true, such as an individual entering his physical address into a website before purchasing, and probabilistic tracking as tracking data that involves unknowns, such as weather forecasting).

271. *See, e.g.*, COPPA, 15 U.S.C. §§ 6501–6506 (2012) (regulating the collection and use of personal information by operators of websites or online services for users younger than thirteen).

272. *See* Mark Harris, *Virtual Assistants Such as Amazon's Echo Break US Child Privacy Law, Experts Say*, GUARDIAN (May 26, 2016, 7:00 AM), https://www.theguardian.com/technology/2016/may/26/amazon-echo-virtual-assistant-child-privacy-law.

privacy settings."[273] In the past, the FTC said it was dedicated to developing new consumer "materials" in this area,[274] and the Trump Administration should continue providing such guidance to consumers.

CONCLUSION

Faced with the privacy challenge that accompanies the interconnected world of the IoT, the FTC has managed to use traditional privacy regulation standards, such as "unfairness" and "deceptive practices," to protect private information. The FTC has been flexible and nimble with its interpretations of such standards and, in its most recent IoT case, *VIZIO*, established a new "tool" in its toolkit for regulating IoT devices: a new "unfair tracking" standard.[275] As the de facto data protection authority in the United States, this new tool provides the FTC the ability to standardize its treatment of IoT privacy issues instead of trying to fit those concerns less neatly under the deception authority of section 5 of the FTC Act. However, this new tool also means that the FTC has the opportunity, and responsibility, to be proactive about wielding it.

To assure that innovation is not stifled and that this new rule is evenly applied across industries (whether regulated by the FTC or other agencies), it is imperative that the FTC diligently address concerns about the scope of this new rule and communicate that guidance to businesses, other regulators, and consumers alike. The new FTC administration should, as the primary regulator of information privacy and the IoT, continue the strong practice established by the previous administration, which is to provide guidance to businesses, consumers, and other regulators navigating the big challenges caused by the little things in the IoT.

---

273. *See* FTC IOT REPORT, *supra* note 106, at 53.
274. *Id.*
275. *VIZIO* Complaint, *supra* note 227, ¶¶ 31–35.