Fordham Law Review

Volume 86 | Issue 5 Article 10

2018

Tell the Smart House to Mind its Own Business!: Maintaining Privacy and Security in the Era of Smart Devices

Kathryn McMahon
Fordham University School of Law

Tell the Smart House to Mind its Own Business!: Maintaining Privacy and Security in the Era of Smart Devices

Erratum

TELL THE SMART HOUSE TO MIND ITS OWN BUSINESS!: MAINTAINING PRIVACY AND SECURITY IN THE ERA OF SMART DEVICES

*Kathryn McMahon**

Consumers want convenience. That convenience often comes in the form of everyday smart devices that connect to the internet and assist with daily tasks. With the advancement of technology and the "Internet of Things" in recent years, convenience is at our fingertips more than ever before. Not only do consumers want convenience, they want to trust that their product is performing the task that they purchased it for and not exposing them to danger or risk. However, due to the increasing capabilities and capacities of smart devices, consumers are less likely to realize the implications of what they are agreeing to when they purchase and begin using these products.

This Note will focus on the risks associated with smart devices, using smart home devices as an illustration. These devices have the ability to collect intimate details about the layout of the home and about those who live within it. The mere collection of this personal data opens consumers up to the risk of having their private information shared with unintended recipients whether the information is being sold to a third party or accessible to a hacker. Thus, to adequately protect consumers, it is imperative that they can fully consent to their data being collected, retained, and potentially distributed.

This Note examines the law that is currently in place to protect consumers who use smart devices and argues that a void ultimately leaves consumers vulnerable. Current data privacy protection in the United States centers on the self-regulatory regime of "notice and choice." This Note highlights how the self-regulatory notice-and-choice model fails to ensure sufficient protection for consumers who use smart devices and discusses the need for greater privacy protection in the era of the emerging Internet of Things. Ultimately, this Note proposes a state-level resolution and calls upon an exemplar state to experiment with privacy protection laws to determine the best way to regulate the Internet of Things.

---

* J.D. Candidate, 2019, Fordham University School of Law; B.A., 2012, College of the Holy Cross. I would like to thank Professor Joel Reidenberg for guiding me and lending his expertise throughout this process. I also would like to thank my family and friends for their constant love, support, and encouragement.

INTRODUCTION

"Can you play dollhouse with me and get me a dollhouse?" asked six-year-old Brooke to Amazon's voice-activated Echo Dot, "Alexa."[1] Brooke also discussed her love of sugar cookies with Alexa.[2] A few days later, both a dollhouse and a four-pound box of sugar cookies totaling $160 arrived at Brooke's doorstep.[3] At first her parents were confused about the items' origin, but they soon realized that Brooke's discussion with Alexa, whether

1. Jennifer Earl, *6-Year-Old Orders $160 Dollhouse, 4 Pounds of Cookies with Amazon's Echo Dot*, CBS NEWS (Jan. 5, 2017, 5:41 PM), https://www.cbsnews.com/news/6-year-old-brooke-neitzel-orders-dollhouse-cookies-with-amazon-echo-dot-alexa/ [http://perma.cc/DV8J-YC2D].
2. *Id.*
3. *Id.*

she had intended to place the order or not, had resulted in the seamless delivery of some of her favorite things to her home.[4] Brooke's experience and so many others like it show the immense capabilities of smart devices today. Smart devices have changed the way we function on a daily basis. The capabilities of these devices can make our lives easier and more efficient.[5] We now can ask a device to turn on our lights, play music, vacuum our floors, and even lock our homes remotely.[6]

Although this modern convenience is appealing, these technologies expose consumers to risks they never imagined. Take the negative consequences of data collection as an example. In early 2017, a television manufacturing company settled a lawsuit with the Federal Trade Commission (FTC) and the New Jersey Attorney General's Office for $2.2 million for installing software that could collect user viewing data in eleven million consumers' televisions without their consent or knowledge.[7] The complaint alleged that Vizio was monitoring its users' "second by second" viewing information and assisting in combining that data with certain demographic information including sex, age, marital status, education level, household size, and income level.[8] The complaint further stated that Vizio then sold that information to third-party companies for targeted advertising.[9] According to Kevin Moriarty, an attorney with the FTC's Division of Privacy and Identity Protection, "Before a company pulls up a chair next to you and starts taking careful notes on everything you watch (and then shares it with its partners), it should ask if that's O.K. with you."[10]

But why does this matter? In today's fast-paced society, should we not be jumping at the opportunity to have a vacuum cleaner do our cleaning without us, have Alexa remind us of our dentist appointment, or have our lights turn themselves off even if it means giving up some of our privacy? While it is true that the prevalence of smart devices—particularly within the home—has the potential to make daily life easier, these devices are also gathering and storing vast amounts of information about our homes and our habits within

4. *Id.*

5. *See, e.g.*, Camryn Rabideau, *10 Gadgets That Will Prevent Everyday Problems and Make Your Life Easier*, USA TODAY (Sept. 22, 2017, 1:24 PM), https://www.usatoday.com/story/tech/reviewedcom/2017/09/22/10-gadgets-that-will-prevent-everyday-problems-and-make-your-life-easier/105879344/ [https://perma.cc/Z8H2-KSCP].

6. *See* Christian de Looper, *The 12 Best Smart Home Devices You Need to Live Like the Jetsons*, BUS. INSIDER (Dec. 7, 2017, 12:15 PM), http://www.businessinsider.com/best-smart-home [https://perma.cc/K2EU-TKKP].

7. Press Release, FTC, VIZIO to Pay $2.2 Million to FTC, State of N.J. to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it [http://perma.cc/D6GQ-R9PN].

8. Complaint paras. 17, 32, FTC v. Vizio, Inc., No. 2:17-cv-00758, 2017 WL 7000553 (D.N.J. 2017); Press Release, FTC, *supra* note 7.

9. Complaint, *supra* note 8, para. 16(c); Press Release, FTC, *supra* note 7.

10. Hayley Tsukayama, *These Smart TVs Were Apparently Spying on Their Owners*, WASH. POST (Feb. 6, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/02/06/these-smart-tvs-were-apparently-spying-on-their-owners [https://perma.cc/XTG5-6BZQ].

our homes.[11] How this data is stored, used, and shared is critical for users to understand because it can have negative consequences for them.[12]

The fact that smart-device companies have access to and control over users' personal data has sparked concern among privacy advocates and scholars.[13] This is due, in part, to the ability of powerful technology companies, which have broad user bases and vast amounts of knowledge about their users, to use data in a manipulative way.[14] Furthermore, smart-device users are likely unaware of the many different ways that smart devices can collect personal data.

For example, recent news stories have drawn attention to the ability of the Roomba, a smart vacuum, to create a map of the home while cleaning to develop a clear path and avoid bumping into stationary objects.[15] This information could be sold to companies such as Amazon, Apple, Facebook, or Google.[16] The Roomba not only knows the floor plan of the user's home but also knows the room in which the user's child sleeps (the one where it consistently bumps into toys on the floor) and the room that is missing certain furniture.[17] Thus, if the data was sold to third parties, the purchasers would gain access to information about the consumer, his home, and his lifestyle that the purchasers did not originally have access to, which would enable them to use that information to their advantage.[18]

For instance, with access to the map data, large technology companies could develop income estimates on each user or determine how many people lived in the home, which would create countless new ways to target the user through advertising.[19] In fact, an increasingly large part of some companies' business models is simply to sell data to advertisers.[20] In addition, the mere

---

11. For example, a Canadian vibrator company that connected to the internet via a smartphone app was found to be using the app to collect data regarding the use of the device, including temperature and intensity settings and how frequently it was used. Jeff John Roberts, *Sex Toy Maker Pays $3.75 Million to Settle 'Smart' Vibrator Lawsuit*, FORTUNE (Mar. 10, 2017), http://fortune.com/2017/03/10/sex-toy-maker-settlement-smart-vibrator-lawsuit/ [https://perma.cc/C2LZ-SEJ7]. Ultimately the company agreed to settle for about $3.75 million to resolve the privacy claims against it. *Id.*

12. *See infra* Part I.A.3.

13. *See, e.g.*, Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 90–91 (2014).

14. *See* Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 AM. U. L. REV. 1183, 1200–01 (2017) (explaining that as the Internet of Things becomes more integrated, data aggregators can pull more information from more devices, which makes it easier to piece together a digital profile of someone).

15. *See, e.g.*, Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html [https://perma.cc/VZC6-A3PS].

16. *Id.*

17. *Id.*

18. *See id.*

19. *See* Bryan Clark, *iRobot Wants to Sell Your Floor Plan Data to Amazon, Apple or Facebook*, NEXT WEB (July 24, 2017, 7:50 PM), https://thenextweb.com/insider/2017/07/25/irobot-wants-to-sell-your-floor-plan-data-to-amazon-apple-or-facebook/ [http://perma.cc/8VBR-SQGY].

20. *See, e.g.*, Ron Hirson, *Uber: The Big Data Company*, FORBES (Mar. 23, 2015, 9:15 AM), https://www.forbes.com/sites/ronhirson/2015/03/23/uber-the-big-data-

collection of data exposes consumers to the potential of the device being hacked and having detailed maps of their homes accessible to anyone who can break through the product's privacy protections.[21] The capacities of these devices raise privacy and security concerns in an area that is generally accepted as being the most sacred and private place for an individual: the home.

Because these devices have the potential to gather, retain, and share a significant amount of detailed personal information about users, it is imperative that users are fully aware of company policies related to user data so that they can choose to accept or reject the terms.[22] While average consumers may be aware that their devices are connected to the internet, they are likely unaware of the type and amount of information that their devices are collecting.[23] The language in companies' policies permitting devices to gather information is often vague, ambiguous, buried deep in the policy, or altogether missing, which leaves consumers completely unaware of what they consented to.[24] A study of 1900 Internet of Things ("IoT")[25] consumers found that 81 percent believed that device manufacturers had not provided any details about how their personal information was used.[26]

This Note's purpose is to investigate and evaluate consumer protection currently in place for smart devices. Due to the increasing ubiquity of smart devices in the home, and their evolving ability to collect personal information, this Note examines the effectiveness of the current notice-and-choice[27] approach to privacy law in the United States. Part I of this Note provides an overview of smart devices prevalent in homes today. This Part discusses the IoT, the capabilities of smart devices, and the current notice-and-choice approach to consumer privacy law in the United States. This Part also examines current IoT privacy policies to evaluate whether users are given true "notice" regarding how and why their information is collected, which enables them to make an informed "choice" about whether they want to use the product.

---

company/#1c62f37b18c7 [http://perma.cc/5YGZ-HZ6R] (discussing how Uber uses vast quantities of user data it collects about people, including where they live, where they work, and when they travel, to generate revenue by selling the data to others).

21. *See* Thomas Fox-Brewster, *Time to Update Your Vacuum Cleaner—Hack Turns LG Robot Hoover into a Spy*, FORBES (Oct. 26, 2017, 9:00 AM), https://www.forbes.com/sites/thomasbrewster/2017/10/26/lg-hom-bot-robot-hoover-hacked-into-surveillance-device [http://perma.cc/6U25-QUEQ] (explaining how a design malfunction in another robotic vacuum cleaner brand exposed the device to hackers and potential spies).

22. *See* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 41–42 (2015) (discussing the United States' approach to internet privacy relying on "notice and choice").

23. *See id.* at 83.

24. *See* Peppet, *supra* note 13, at 140–47.

25. *See infra* Part I.A.

26. PONEMON INST., PRIVACY AND SECURITY IN A CONNECTED LIFE: A STUDY OF U.S. CONSUMERS 7 (2015), http://www.trendmicro.de/media/report/ponemon-privacy-and-security-in-a-connected-life-us-consumers-report-en.pdf [http://perma.cc/V933-A6N3].

27. *See infra* Part I.C.

Part II explores the current law that protects consumers who purchase and use smart devices within the home.[28] This Part discusses current laws that may protect consumers whose privacy is violated due to inadequate "notice and choice." Although consumers often unknowingly agree to the privacy policies of smart devices as soon as they begin to use them, this Note argues that, as technological advances create increasingly pervasive smart devices, consumers will require greater protections to ensure that they can make the informed choices necessary for adequate consent. Part III proposes a resolution by arguing that consumer protection statutes should be implemented at the state level initially in order to determine the best way to regulate the IoT. These statutes should mandate explicit requirements for smart-device companies to include in their privacy policies to give consumers an adequate understanding of how their data is being used, thus enabling them to make truly informed choices about whether to use a particular device.

I. SETTING THE SCENE: PRIVACY AND SECURITY IN THE ERA OF THE IOT

In 1999, Kevin Ashton, executive director of Auto-ID Labs at MIT, became the first person to describe the IoT. He explained that the future of the internet would be in devices that could collect data without human assistance to maximize efficiency, cut costs, and reduce waste.[29] Today, less than twenty years later, the IoT has become a reality. By 2020 there will be an estimated twenty-one billion connected devices worldwide,[30] an increase of nearly 250 percent from 2017.[31] With this sharp increase in an entirely new market comes many legal questions related to consumer privacy and security.

This Part provides an overview of the IoT and legal concerns that arise from it. Part I.A describes the IoT. Part I.B introduces the Roomba robotic vacuum cleaner, which this Note uses as an illustration because of its unique capability to collect personal data. Part I.C explains the history and standards of the notice-and-choice approach to privacy law in the United States. Finally, Part I.D expresses the importance of privacy policies for the notice-

28. Fourth Amendment privacy protection within the home is beyond this Note's scope. This Note instead focuses on consumer protection.

29. Keith D. Foote, *A Brief History of the Internet of Things*, DATAVERSITY (Aug. 16, 2016), http://www.dataversity.net/brief-history-internet-things/ [http://perma.cc/BB3P-VXBL] ("The problem is, people have limited time, attention, and accuracy. All of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best.").

30. Julia Boorstin, *An Internet of Things That Will Number Ten Billions*, CNBC (Feb. 1, 2016, 10:52 AM), https://www.cnbc.com/2016/02/01/an-internet-of-things-that-will-number-ten-billions.html [http://perma.cc/7Y8E-R3YS].

31. *See* Press Release, Gartner, Inc., Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent from 2016 (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917 [http://perma.cc/EF72-SQ9P].

and-choice approach to be effective and examines common shortcomings of privacy policies for smart devices.

A. The IoT

This Part provides an overview of the IoT. Part I.A.1 discusses smart devices and highlights the different types of smart devices that are available, the benefits of using them, and why the smart device market is growing. Part I.A.2 then explains how smart devices work and how they fit into the IoT. Next, Part I.A.3 discusses the overarching risks associated with smart devices.

1. The Technology

Smart devices are everyday objects that have embedded sensors allowing the devices to collect and send data about the individuals who use the device and their surroundings to a sensor system.[32] For consumers, smart devices are available in numerous contexts. For health and fitness, Fitbits and similar devices are wearable technology that can track health, fitness, and eating habits. Smart devices in the home include smart vacuum cleaners that can automatically sweep at scheduled intervals, smart refrigerators that can detect and notify a user when they are about to run out of a product, smart thermostats that can control the temperature of the home based on the weather and the time of day, and smart lights that can self-adjust based on occupancy and available sunlight. Smart home devices are also available in the form of voice-activated assistants such as the Amazon Echo and Google Home, both of which can set reminders for users, answer user questions, and control other smart devices. While all smart devices share the characteristic of communicating data about their users to sensor systems,[33] this Note uses smart home devices as an illustration. Smart home devices are uniquely positioned to gather highly personal and intimate data about consumers and their habits implicating numerous privacy and security concerns.

Despite these concerns, it is undoubtedly true that smart devices present significant benefits to consumers who use them.[34] First, the devices are

32. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 554 (2017); Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, HUM. RTS., 2016, at 14, 14 . There is no formal definition for a smart device. Some argue that they encompass virtual things, in addition to physical things such as people. *See, e.g.*, Guido Noto La Diega & Ian Walden, *Contracting for the 'Internet of Things': Looking into the Nest*, EUR. J.L. & TECH., Sept. 2016, at 1, 2. In this Note, however, a smart device will refer to everyday objects with embedded sensors used to collect and communicate data.

33. *See, e.g.*, Ferguson, *supra* note 32, at 554; Williams, *supra* note 32, at 14.

34. *See infra* text accompanying notes 35–40. In fact, a recent study of smart home-device owners found that 26 percent bought their first device in order to "increase overall convenience, improve their quality of life, or help them be more productive." PWC, SMART HOME, SEAMLESS LIFE: UNLOCKING A CULTURE OF CONVENIENCE 7 (2017), https://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-consumer-intelligence-series-iot-connected-home.pdf [http://perma.cc/7TQ3-XD55]. Yet, to reap the benefits of smart devices, consumers make a trade-off of their privacy. *See infra* Part I.A.3.a.

convenient.[35] Users can remotely access their devices or preprogram them to work without any further interaction.[36] Smart home devices also enable energy efficiency.[37] Products such as smart lights and smart thermostats can automatically adjust based on current needs within the home.[38] In addition, certain smart home devices can promote security through video monitoring, motion detection, smart locks, and smart doorbells.[39] Finally, users of smart devices gain insights about their habits within the home by tracking information such as how often their lights are left on, the types of food they keep in their refrigerator, and what times of day they watch television, which can ultimately help them change unwanted habits.[40]

The conveniences of smart devices coupled with the fact that "new efficiencies have pushed down the cost of sensors and new innovations have improved the communication capacities of low-power devices" has resulted in substantial growth in consumer smart devices.[41] One information-technology analyst firm estimates that there are currently 8.4 billion connected devices in use worldwide, up 31 percent from 2016.[42] By 2020, the firm predicts that there will be over 20.4 billion connected devices.[43] Furthermore, the number of smart home devices delivered worldwide increased 64 percent between 2015 and 2016.[44] Thus, as the availability and interconnectivity of these devices grow, they will become more prevalent among average homeowners looking to modernize and maximize efficiency.[45] As these devices become commonplace in homes, it is critically important that users understand how the devices work and their associated risks.

---

35. *See The Advantages of a Smart House*, SFGATE, http://homeguides.sfgate.com/advantages-smart-house-8670.html [http://perma.cc/8K5L-RBH3] (last visited Mar. 15, 2018).

36. *See id.*

37. *See 6 Benefits of Smart Home Technology*, AM. FAM. INS., https://www.amfam.com/resources/articles/at-home/six-benefits-of-smart-home-technology [http://perma.cc/T5VV-GA4Y] (last visited Mar. 15, 2018).

38. *See id.*

39. *See id.*

40. *See The 7 Greatest Advantages of Smart Home Automation*, BLUE SPEED AV BLOG (June 14, 2016), http://www.bluespeedav.com/blog/item/7-greatest-advantages-of-smart-home-automation [http://perma.cc/7JLT-KFZ8].

41. Ferguson, *supra* note 32, at 556.

42. *See* Press Release, Gartner, Inc., *supra* note 31.

43. *See id.* Thus, in our lifetime, we may see

> a future that includes "smart" refrigerators that sense when you are out of milk; smart clocks that alert your smart coffee machine that it's time to start the morning brew; smart cars that automatically notify your smart thermostat that you are almost home; smart sheets that track your restlessness; smart glucose monitors that send signals directly to your doctor; smart light switches, ovens, security systems, toothbrushes, and toilets.

Williams, *supra* note 32, at 14.

44. Diana Olick, *Why 2017 Will Finally Be the Year of the Smart Home: Consumers Figure It Out*, CNBC (Jan. 4, 2017, 8:03 AM), https://www.cnbc.com/2017/01/04/why-2017-will-finally-be-the-year-of-the-smart-home-consumers-figure-it-out.html [http://perma.cc/BRU9-FKME].

45. *See id.*

2. Internet Connection

The convenience and efficiency promised by smart devices is the result of their internet connectivity. Smart devices function through embedded sensors that are connected to the internet, which enable them to collect and transmit data without human interaction.[46] In addition to the sensor technology, the devices also rely on existing wireless networking systems such as Wi-Fi, Bluetooth, and GPS.[47]

As more devices have the ability to communicate through internet connectivity, society is transitioning into a world full of smart devices, known as the IoT.[48] The FTC has defined the IoT as "an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people."[49] Similarly, legal analysts describe the IoT as "the network of everyday physical objects that surround us and are increasingly being embedded with technology to enable those objects to collect and transmit data about their use and surroundings."[50] As the IoT grows, and smart devices make their way into homes, many believe that this technology will operate quietly in the background as it seamlessly integrates into our everyday lives.[51]

3. Data Collection, Device Functionality, and Risks for Consumers

As consumers purchase smart devices and connect them with one another, increasing amounts of data about the consumer become available.[52] Smart-device companies consider data collection to be necessary for the effectiveness and proper functionality of the device.[53] For example, as

---

46. *See* Williams, *supra* note 32, at 14.

47. *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, RICH. J.L. & TECH., Winter 2015, at 1, 8–9.

48. *See* Peter M. Lefkowitz, *Making Sense of the Internet of Things*, 59 BOS. B.J. 23, 23 (2015).

49. FTC, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 1 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [http://perma.cc/83MA-ED9N].

50. Amy Collins et al., *The Internet of Things Part 1: Brave New World*, MORRISON FOERSTER: SOCIALLY AWARE (Apr. 2, 2014), https://www.sociallyawareblog.com/2014/04/02/the-internet-of-things-part-1-brave-new-world-2/ [http://perma.cc/ESQ7-PSKA].

51. *See* Thierer, *supra* note 47, at 9.

52. *See* Brill & Jones, *supra* note 14, at 1199.

53. *See, e.g.*, *Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_467C686A137847768F44B619694D3F7C [http://perma.cc/TG64-SC8T] (last visited Mar. 15, 2018) ("You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you."); *Privacy Policy*, IROBOT, http://www.irobot.com/Legal/Privacy-Policy.aspx [http://perma.cc/L8B3-NRU4] (last visited Mar. 15, 2018) ("We use this information to collect and analyze statistics and usage data, diagnose and fix technology problems, enhance device performance, and improve user experience.").

Amazon's Alexa becomes more familiar with the user's voice, it can respond to requests more accurately and consistently.[54] Similarly, a device such as the Nest Thermostat becomes more effective when it is familiar with the user's heating and cooling preferences.[55] While data collection may be important to the device's functionality, it also presents privacy and security concerns. Part I.A.3.a outlines data privacy concerns while Part I.A.3.b discusses data security concerns.

a. Data Privacy

The constant collection of a vast amount of consumer data has led to a growing market for such information.[56] The sensors on smart devices can collect information about a user's lifestyle, habits, and preferences, which, once analyzed, has the potential to provide useful information to third parties.[57]

For large technology companies, much of the data collected by smart devices has become incredibly valuable because the information garnered from the data paints a detailed picture of the consumer.[58] Many powerful technology companies are investing in IoT not only to sell products but also to gather data from those products.[59] Having insight about a consumer's daily habits could give companies a competitive advantage through specific and targeted advertising.[60] Furthermore, as smart devices become more integrated with one another through the IoT, data profiles on consumers will become more comprehensive.[61] Thus, as data aggregation occurs, and companies pull increasing amounts of information from users' devices, "personal control over one's information wanes and the security and privacy risks for an individual's personal information grows."[62]

Not only does the detailed and personal information expose consumers to targeted advertising and marketing, it also could result in unfair forms of

54. *See* Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/ [https://perma.cc/LT9D-TRJM] (explaining that voice-activated assistants must always be listening to what you say so they can differentiate your regular conversations from their wake words, and so they can immediately respond when their wake words (i.e., "Alexa") are called).

55. *See What Is Auto-Schedule and How Does It Learn?*, NEST, https://nest.com/support/article/How-does-Auto-Schedule-learn [https://perma.cc/99JA-C8YS] (last visited Mar. 15, 2018) (discussing how the Nest Thermostat learns your preferences over time and remembers them so the user does not have to manually change the temperature each day).

56. *See* Ferguson, *supra* note 32, at 559.

57. *See* Peppet, *supra* note 13, at 90.

58. *See id.* ("Sensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through 'Big Data' analytics, these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities.").

59. *See* Ferguson, *supra* note 32, at 555.

60. *See id.* at 559.

61. *See* Brill & Jones, *supra* note 14, at 1199.

62. *Id.*

discrimination.[63] Professor Scott Peppet suggests that potential employers could turn to their "commercial partners"[64] to gather information about employees.[65] With access to an individual's electric utility data, for instance, a potential employer could learn how often the individual is at home, when the individual sleeps, or whether the individual is energy conscious—information that could lead to inferences about a candidate and that could result in hidden forms of discrimination.[66] Lack of sleep "has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear."[67] Thus, a candidate whose sensor reveals that she does not sleep enough may be less likely to get a position.[68]

Data could also be used in a similar way by insurance providers, creditors, and others seeking to gain information about users to make decisions about them.[69] In the worst-case scenario, usage of this data could result in forms of illegal discrimination against protected classes.[70] In short, this data provides incredibly detailed and nuanced information about users that, when shared with outside parties or unintended recipients, could result in unfair consequences or outcomes.

b. Data Security

The ability of smart devices to collect data not only implicates privacy concerns but also security concerns.[71] These risks are intertwined with one another because the improper use of data can cause both privacy and security harms.[72] For many, security is more important than privacy.[73] While the security risks posed by IoT devices are not novel and include risks that existed with traditional computers, the FTC expressed in its 2015 report that the risks are exacerbated by IoT devices.[74] These risks include "(1) enabling

63. *See* Peppet, *supra* note 13, at 118.

64. In this context, a "commercial partner[]" refers to a company (such as an electric utility company or an auto insurance company—any company that may have data on the potential employee) that has a business relationship with the potential employer. *See id.* at 120.

65. *Id.*

66. *See id.* at 118. Peppet further suggests that data brokers who accumulate and track information about individuals through their internet usage may soon incorporate Internet of Things data. *Id.* at 120.

67. *See id.* at 119.

68. *See id.*

69. *Id.* at 118.

70. *See id.*

71. *See* FTC, *supra* note 49, at 10–14 (detailing the different types of security risks posed by the IoT).

72. Part II of this Note discusses the legal framework to address privacy harms rather than security harms. However, due to the pervasive nature of smart devices, this Note argues that consumers must be aware of the risks (both privacy and security) associated with the devices in order to adequately consent. Accordingly, when addressing the risks of the IoT, this Note discusses both privacy and security.

73. *See* Lefkowitz, *supra* note 48, at 24.

74. FTC, *supra* note 49, at 10.

unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks."[75]

The first risk, enabling unauthorized access and misuse of personal information, derives from hackers who are able to access and abuse personal information collected and transmitted from a device.[76] This is similar to the traditional idea of a computer hack, in which a fraudster is able to access a user's information on his computer and exploit it.[77] In the case of the smart home, smart televisions similarly allow consumers to make purchases, surf the internet, or share photos.[78] If a security breach occurs, hackers could access all of this information and use it themselves.[79] Furthermore, in a home with multiple smart devices always collecting and sharing personal data, the risk of exposure to a hacker who can access and exploit a user's data increases.[80]

The risk of facilitating attacks on other systems, such as a denial-of-service attack, poses another concern.[81] As users become more dependent upon their devices, the implications of this concern increase. A denial-of-service attack could result in a situation in which a hacker gains access to a smart home's devices such as smart locks, light bulbs or refrigerator.[82] Hackers could "threaten to spoil dinner, cut the lights, or lock a homeowner out (or in!) unless they get paid."[83] For a user with multiple devices, the ability of a hacker to gain control of all the devices and deny service until something is done in return could pose serious problems.[84]

The third risk, creating safety risks, is arguably the most important type of security concern.[85] This type of risk relates to devices that are hacked and ultimately used in a way not originally intended, which could endanger consumers.[86] For instance, researchers recently reported that they were able to hack an LG app that controlled a robotic vacuum cleaner, the "Hom-Bot hoover," which enabled them to use the video feed to spy on anything in the

75. *Id.*
76. *Id.* at 10–11.
77. *Id.*
78. *Id.* at 11.
79. *Id.*
80. *See id.*
81. *Id.* at 11–12. This type of attack is one in which a hacker gains control of a user's device and refuses to give control back until certain conditions are met.
82. *See* Kaveh Waddell, *The Extortionist in the Fridge*, ATLANTIC (Jan. 6, 2016), https://www.theatlantic.com/technology/archive/2016/01/the-extortionist-in-the-fridge/422742/ [http://perma.cc/X9T5-U2EA]; *see also* Stuart Madnick, *Security Surprises Arising from the Internet of Things*, FORBES (May 8, 2017, 10:01 AM), https://www.forbes.com/sites/ciocentral/2017/05/08/security-surprises-arising-from-the-internet-of-things-iot/#76b31a522495 [http://perma.cc/ZC44-GMFY] (discussing the hypothetical situation in which an internet-enabled coffee maker is held to ransom and the owner receives a message stating that he will not be able to have his coffee unless he pays the hacker five dollars).
83. Waddell, *supra* note 82.
84. *See* FTC, *supra* note 49, at 12.
85. *Id.* at 10.
86. *See id.* at 12.

device's vicinity.[87] They expressed that this hack could compromise other devices such as dishwashers, refrigerators, ovens, washing machines, and anything else controlled by the LG app.[88] The ability to hack into a video camera and see what the residents are doing in the privacy of their home poses significant security risks. Examples of similar security risks include a hacker directing a smart car drive off of a bridge[89] or the forcing of a smart insulin pump to no longer deliver medicine.[90] These security risks further demonstrate that while smart devices and the IoT have the capabilities to make daily life easier and more efficient, there are significant risks.

Victims of an IoT hack or security violation may pursue legal remedies.[91] The Computer Fraud and Abuse Act (CFAA),[92] for instance, is an antihacking statute that Congress has essentially expanded to apply to any device with a microchip that has some relationship to interstate commerce.[93] While this statute could be useful for punishing hackers of IoT devices, it has limitations. The CFAA sentencing structure distinguishes punishments based on harms.[94] In certain situations, such as when the crime harms people or computers,[95] the maximum penalty increases.[96] These increased penalties, however, do not apply when a hacker causes a social harm, such as spending the account owner's funds after hacking an Amazon account or updating an account owner's social media information to be false or embarrassing.[97] In situations in which an increased penalty does not apply, there is only a one-year maximum sentence.[98] In these situations, it is unlikely that a potential hacker would be deterred by the threat of the one-year maximum penalty imposed by CFAA.[99] In addition, not only are IoT devices generally easier to hack, but it is also more challenging to identify the hacker than it is for

87. *See* Fox-Brewster, *supra* note 21.

88. *Id.* ("[T]he hack goes to show just how an entire home can be exposed to hackers with a simple weakness in a mobile application.").

89. *See* Madnick, *supra* note 82.

90. *See* FTC, *supra* note 49, at 12.

91. The remainder of this Part provides a broad overview of security laws that could apply to IoT devices, while Part II provides a more in-depth analysis of laws related to privacy.

92. 18 U.S.C. § 1030 (2012).

93. *See id.* § 1030(e)(1), (e)(2)(B); *see also* Matthew Ashton, Note, *Debugging the Real World: Robust Criminal Prosecution in the Internet of Things*, 59 ARIZ. L. REV. 805, 813 (2017) (examining existing criminal statutes applied to the IoT).

94. *See generally* 18 U.S.C. § 1030.

95. *See* Ashton, *supra* note 93, at 816–17.

96. *See* 18 U.S.C § 1030(a)(7), (c)(3) (allowing for punishment of up to five years when a hacker uses an internet-connected device as a tool for ransom); *id.* § 1030(c)(4)(A) (allowing for punishment of up to five years for different types of computer-related harms that result in the loss of more than $5000, the modification of a medical treatment, physical injury, a threat to public health or safety, damage to a government computer, or damage to ten or more computers); *id.* § 1030(c)(4)(E) (allowing for punishment up to twenty years when a hacker attempts to cause or recklessly causes bodily injury); *id.* § 1030(c)(4)(F) (allowing for punishment up to a life sentence when a hacker attempts to cause or recklessly causes death).

97. *See* Ashton, *supra* note 93, at 817.

98. *See generally* 18 U.S.C. § 1030. Under the CFAA, criminals who cause a social harm by hacking an Amazon account or a social media profile would technically be subject to the same one-year maximum sentence as those who share Netflix passwords with one another. *See* Ashton, *supra* note 93, at 817.

99. *See* Ashton, *supra* note 93, at 819.

traditional internet hacks.[100] Thus, a potential hacker who weighs the likelihood of getting caught against the low sentence for causing a social harm.[101]

States also have data-security and data-breach notification laws that could be applicable to IoT devices.[102] These statutes cover "personal information," which most of the statutes define to include an individual's first and last name, plus another piece of information such as a social security number, bank account information, or driver's license number.[103] Thus, a security breach that involved the theft of records containing users' names and their sensor data, or just their sensor data, would not trigger the data-breach notification laws in the majority of states.[104]

Furthermore, the FTC's authority to regulate a smart-device security breach is also limited.[105] While it may regulate privacy and security under its authority to police "unfair" or "deceptive" practices, its authority to do so under these two prongs is quite limited.[106] For the FTC to take action under the deception prong, it would require the company to make clear and unequivocal statements about their security-related promises to the public.[107] For the unfairness prong, the FTC must show that a company injured consumers in a way that violates public policy,[108] which is possible under only a small set of circumstances.[109] In short, while some laws may be applicable to data-security breaches for IoT devices, the laws have limited application and do not sufficiently address all the potential security concerns that arise with IoT devices.

B. The Modern Smart Home

The smart-home market is rapidly growing.[110] A recent study found that the smart-home market is likely to grow at a compounded annual growth rate

100. *See id.*
101. *See id.*
102. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Feb. 6, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [http://perma.cc/WWS6-RXKN] (listing forty-eight states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, all of which have data-breach notification laws). The purpose of these laws is to require private or government entities to inform individuals when a security breach occurs involving personally identifiable information. *Id.*
103. *See* Peppet, *supra* note 13, at 137–38.
104. *See id.*
105. *See id.* at 136–37.
106. *See infra* Part II.C.
107. *See* Peppet, *supra* note 13, at 136–37.
108. *Id.* at 137.
109. *E.g.*, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014) (denying Wyndham's motion to dismiss, which challenged the FTC's authority to bring a claim under the unfairness prong in the context of data security), *aff'd*, 799 F.3d 236 (3d Cir. 2015). For a more detailed discussion of how the FTC has used its authority to police "unfair" or "deceptive" acts, see *infra* Part II.C.
110. *See* Trefis Team, *Why Smart Home Devices Are a Strong Growth Opportunity for Best Buy*, FORBES (July 5, 2017, 3:24 PM), https://www.forbes.com/sites/greatspeculations/2017/

of 14.5 percent between 2017 and 2022 and reach $53.45 billion by 2022.[111] Smart home control devices like the Amazon Echo and the Google Home can connect with other appliances such as lights, thermostats, refrigerators, televisions, and even vacuum cleaners to maximize efficiency within the home.[112] This Part discusses a specific smart home device, the Roomba robotic vacuum cleaner, detailing the device's history, how it works, the information that it collects, and the potential legal questions that arise if data from the device were shared with third parties. The Roomba is used as an illustration throughout this Note to demonstrate current legal issues implicated by smart home devices.

The Roomba was released by iRobot in 2002.[113] Several different models with advanced capabilities have come out since the original model.[114] In 2015, the new Roomba 980 combined intelligent visual navigation, cloud-connected application control, and increased cleaning power.[115] With this technology, the Roomba began creating maps of users' homes.[116] The Roomba uses simultaneous localization and mapping (SLAM) technology to map a user's home.[117] In addition, iRobot recently launched two new versions, the Roomba 690 and the Roomba 890, which extended Wi-Fi connectivity to the entire Roomba line.[118] These newer Roomba models can connect with smart assistants such as Amazon's Alexa so that users can control them with voice commands.[119]

By using SLAM, the newer models collect data about the home, including a map of the layout of the home, what area requires the most cleaning, and what area usually has toys on the floor.[120] Similar to other smart devices,[121] iRobot's privacy policy focuses on the fact that enabling the technology of the product will allow the device to function more effectively, which draws

---

07/05/why-smart-home-devices-are-a-strong-growth-opportunity-for-best-buy/#643505944984 [http://perma.cc/FJ5S-DEWY].

111. *Id.* Due to the increased demand for smart home devices, Best Buy announced that it will make space in 700 stores to showcase how the Amazon Echo and Google Home can interact with other smart devices. *Id.*

112. *See id.*

113. *History*, IROBOT, http://www.irobot.com/About-iRobot/Company-Information/History.aspx [http://perma.cc/9NVW-J2PF] (last visited Mar. 15, 2018).

114. *See id.*

115. *Id.*

116. Joshua A.T. Fairfield, *The 'Internet of Things' Is Sending Us Back to the Middle Ages*, CONVERSATION (Sept. 5, 2017, 8:39 PM), https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435 [http://perma.cc/U3XW-XL5T].

117. Rhett Jones, *Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder*, GIZMODO (July 24, 2017, 2:05 PM), http://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829 [https://perma.cc/WN6U-VTJ5]. The use of SLAM technology makes the product superior to others on the market. *Id.*

118. *History*, *supra* note 113.

119. Aliya Ram, *Vacuums That Pick Up Data as Well as Dirt Renew Privacy Concerns*, FIN. TIMES (Aug. 15, 2017), https://www.ft.com/content/d8630420-776c-11e7-a3e8-60495fe6ca71 [https://perma.cc/2FNZ-GX33].

120. *See* Jones, *supra* note 117.

121. *See supra* note 53 and accompanying text.

attention away from privacy concerns.[122] Although this data collection may enable the Roomba to function more effectively, the prospect of the data being sold or shared raises important legal questions.[123] Not only would it expose consumers to targeted advertising[124] based on items that their homes have or do not have,[125] it could also enable companies to determine the owner's income level by paying attention to the size of the home and the amount of furniture within the home.[126] One staff attorney at the Electronic Frontier Foundation noted that this information, coupled with other data, "is going to be able to reveal a ton of information about what people's lifestyles are like, [and] what people's daily patterns are like."[127]

Furthermore, consider a current homeowner with a Roomba who consents to having his data shared. Suppose that user moves and a new owner moves into the home. A legal question could arise regarding how the previous owner's consent affects the new owner and whether the data about the home can be retained.[128] In addition, new legal questions may arise if that data were shared with law enforcement or insurance companies.[129] Consideration of these legal questions requires an understanding of how the United States addresses issues of consumer data privacy. The next Part discusses the current approach to consumer data privacy in the United States.

C. "Notice and Choice"

Consumer privacy laws in the United States come from multiple sources—state-law privacy torts, federal statutes, and administrative rules—and are thus described as "sectoral."[130] The FTC plays a critical role in regulating the collection of consumer data.[131] In 1914, Congress created the FTC through the Federal Trade Commission Act (FCTA) to protect consumers and promote competition.[132] Section 5 of the FTCA gives the FTC the statutory authority to file complaints against any business that is found to have unfair practices related to the management of consumer data.[133]

---

122. *See* Jones, *supra* note 117. "We collect personal information in order to provide you with a personalized, useful and efficient experience." *Privacy Policy*, *supra* note 53.

123. *See supra* notes 56–70 and accompanying text.

124. *See supra* notes 58–62 and accompanying text.

125. *See* Astor, *supra* note 15.

126. *See id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. *See, e.g.*, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 790–91 (Erwin Chemerinsky et. al. eds., 5th ed. 2014); Amanda Grannis, Note, *You Didn't Even Notice! Elements of Effective Online Privacy Policies*, 42 FORDHAM URB. L.J. 1109, 1113 (2015).

131. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014) ("The FTC reigns over more territory than any other agency that deals with privacy."); Grannis, *supra* note 130, at 1113.

132. *See Our History*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/our-history [http://perma.cc/MRS8-8AS5] (last visited Mar. 15, 2018).

133. 15 U.S.C. § 45(b) (2012). This is determined by whether the business "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers

In the early age of the internet, the FTC addressed online consumer privacy issues by promoting a policy of self-regulation.[134] In 2000, after a few years of studying online privacy issues and promoting the "Fair Information Practice Principles" (FIPPs) of "notice," "choice," "access," and "security," the FTC provided further clarification about the policy of self-regulation in a report to Congress.[135] In the report, the FTC discussed its finding that in a survey of website privacy policies, only 20 percent of policies complied at least in part with the FIPPs.[136] The FTC further noted that the principles of "access" and "security" had implementation issues, which makes compliance with the principles particularly challenging.[137] Therefore, the FTC focused on the principles of "notice," the "most fundamental" principle,[138] and "choice" separately, and it found that only 41 percent of policies complied with the standards.[139] While recognizing the continued need for industry self-regulation, the FTC expressed that adequate protection of consumer privacy online would require Congress to enact legislation.[140]

Because Congress declined to enact comprehensive legislation, self-regulation remains the primary mechanism for addressing issues of consumer privacy today.[141] Furthermore, the principles of notice and choice have been promulgated as critical components to the model.[142] Notice requires that consumers be given "clear and conspicuous notice of an entity's information practices before any personal information is collected from them."[143] Choice entails "giving consumers options as to how any personal information collected from them may be used . . . beyond those necessary to complete a contemplated transaction."[144] This would include using consumer information for marketing additional products or transferring or selling consumer data to third parties.[145]

---

themselves and not outweighed by countervailing benefits to consumers or to competition." *Id.* § 45(n).

134. FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 41 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [http://perma.cc/N8AT-B3N5] ("The [i]nternet is a rapidly changing marketplace. Effective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy.").

135. *See generally* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [http://perma.cc/7QM4-Z3HT].

136. *Id.* at 12.

137. *Id.* at 18.

138. *Id.* at 14.

139. *Id.* at 35.

140. *Id.* at 36 ("Ongoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumers' privacy on the [i]nternet.").

141. *See* Reidenberg et al., *supra* note 22, at 43.

142. *See id.* at 43–44.

143. FTC, *supra* note 135, at 14.

144. *Id.* at 15.

145. *Id.*

The idea of the current regulatory regime is that as long as companies provide accurate information to consumers, and consumers make an informed choice to accept or reject the service, self-regulation works.[146] Accordingly, privacy policies are critically important for this model to be effective.[147] For a consumer to be given adequate notice regarding his data, privacy policies must include information regarding who is collecting the data, how the data is being used, who may potentially receive the data, whether collection of the data is necessary for the device to function, and the steps taken by a company to maintain the confidentiality of the data.[148] Without this detailed and thorough explanation of how their data is being used, consumers are unable to make an informed choice, and thus the self-regulatory model breaks down.[149] The next Part discusses some of the current weaknesses with smart-device privacy policies.

D. Shortcomings of Modern Privacy Policies

Under the current notice-and-choice model, privacy policies are the most important source of information for consumers who are attempting to learn how companies will use their data.[150] For the model to be effective, it is critical for consumers to understand the policy to which they are agreeing. Despite this important principle, privacy policies are consistently "verbose, difficult to understand, take too long to read, and may be the least-read items on most websites even as users express growing concerns about information collection practices."[151] These problems exist with smart devices' privacy policies as well.[152] Thus, with ineffective privacy policies, the notice-and-choice model fails to work.

Consumers have become more hesitant to buy smart home devices due to security and privacy concerns.[153] A recent study found that consumers are uncomfortable being "watched, listened to, or tracked by devices they place in their homes."[154] The study further found that 40 percent of consumers felt that they were not informed about the risks of the device.[155] These findings highlight the conundrum faced by consumers surrounded by the rapidly growing IoT. While consumers may be excited about the prospect of using smart devices and reaping the benefits that they offer, consumers also feel that they are not receiving the requisite notice that enables them to make informed choices about the devices. Thus, some consumers may be

146. *See* Reidenberg et al., *supra* note 22, at 41.
147. *See id.*
148. *See id.*
149. *See id.*
150. *See id.*; *see also supra* Part I.C.
151. Reidenberg et al., *supra* note 22, at 41.
152. *See infra* Parts I.D.1–4.
153. *See* Caroline Cakebread, *Consumers Are Holding Off on Buying Smart-Home Gadgets Thanks to Security and Privacy Fears*, BUS. INSIDER (Nov. 15, 2017, 3:20 PM), http://www.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11 [https://perma.cc/JAM2-363J].
154. *Id.*
155. *Id.*

refraining from the smart market entirely, while others may be entering the market unaware of how the devices collect, use, and share data.

Failure to provide adequate notice to consumers in the form of privacy policies results in uninformed choices. When this occurs, the self-regulatory model fails. This Part highlights common problems with smart-device privacy policies and uses iRobot's privacy policy for the Roomba to illustrate these common problems. Specifically, this Part addresses the difficulty of finding smart-device privacy policies, the vague and unclear language common within privacy policies, the time constraints of reading privacy policies, and, finally, the glaring omissions from privacy policies.

1. Location of Smart-Device Privacy Policies

As one privacy scholar noted, notice and choice for IoT devices is inherently complicated because the device's physical features do not facilitate consent.[156] The devices—generally small, screenless, and lacking an input mechanism—make it challenging to confront a user with a privacy policy and to obtain consent.[157] If the device cannot display the privacy policy, the company is left with the choice of placing the policy in the box with the device, on the company's website, or within a connected mobile application.[158] This scholar studied twenty IoT devices and their privacy policies to learn more about their commonalities and found that none of the devices included privacy- or security-related information in the box.[159] Nor did any of the device boxes contain information pointing the user to the privacy policy's location.[160] Thus, by not having a privacy policy in the box and not mentioning where to locate the policy, a consumer could be entirely unaware of the existence of any privacy policy.[161]

The study also found that the overwhelming majority of IoT manufacturers preferred to provide the policy on their websites.[162] For many of these devices, it was unclear whether the privacy policy on the website applied to use of the website or the sensor device.[163] While some of the policies stated that they applied to the use of both the website and the device, others

156. Peppet, *supra* note 13, at 140–41. Upon purchasing a device called a "Breathometer," the consumer was provided with the device and a user manual, but had to go online and search for the privacy policy, which was buried deep in the product's website. *Id.* at 89–90.

157. *Id.* at 140.

158. *Id.* at 141.

159. *Id.*

160. *Id.*

161. *See id.*

162. *Id.*

163. *Id.* at 142. Peppet examined iHealth, a company that manufactured health devices such as a health and sleep monitor, which works through an app. *Id.* at 141–42. According to Peppet, the policy on the iHealth website, only applied to the use of the website and not to the use of the monitor or the app. *Id.* at 142. When installing the app, a user encountered a software license agreement, which stated that the app may upload personal information and that the use of personal data is outlined in the privacy policy. *Id.* Despite this, the user was never told where the device's privacy policy could be located. *Id.* Thus, "even an interested consumer seeking privacy information about iHealth products and sensor data [was] led in an unending circle of confusion." *Id.*

indicated that the privacy policy applied only to the website and that the user would need to go elsewhere to read the device's privacy policy.[164] Some websites included separate policies, one for the use of the website and one for use of the device; while this makes it clear to the consumer what policy applies to his or her data, it takes significant time and energy to sift through all the information.[165] In short, because most companies do not include privacy policies for smart devices in the box, users must independently seek them out to give fully informed consent.[166] Even once the user locates the policy, he may be unclear about whether the policy applies to the device.[167]

The findings of this study are consistent with the case of the Roomba. The device lacks an input mechanism and thus cannot display a privacy policy. Upon opening the box, there is no indication that the device is subject to a privacy policy. To find the privacy policy, the user must go to the iRobot website and scroll to the bottom of the page. Furthermore, while the language of the privacy policy indicates that it applies to the device itself—"[t]his [p]olicy applies to [iRobot] websites and Service, including www.iRobot.com (the "Web Site"), as well as to consumer devices you register with [iRobot] Service and to the online applications ("Apps") which provide support for those consumer devices"[168]—this information is not immediately apparent, and it takes time for the consumer to locate.

2. Language in Smart-Device Privacy Policies

A study investigating users' understanding of privacy policies found that 52 percent of users incorrectly believe that "[w]hen a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."[169] In the age of smart devices, this is a concerning statistic due to the ability of the devices to collect highly personal data.[170] Even for a user who is able to locate a privacy policy and is willing to read it, understanding it can be incredibly difficult.[171] Research has shown that high levels of education are often required to understand the verbose and legalistic nature of most privacy policies.[172] Yet, even for a highly educated user who can read the policy, a true understanding may be challenging due to the policy's ambiguity or obscurity.[173] One study found that the language of privacy policies framed the data-collection practices in a positive light and

164. *Id.*
165. *See id.* at 143.
166. *See id.* at 141.
167. *See id.* at 142–43.
168. *Privacy Policy*, *supra* note 53.
169. Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ [http://perma.cc/3ND3-TFAY].
170. *See supra* text accompanying notes 124–27.
171. *See* Grannis, *supra* note 130, at 1149.
172. *See* Reidenberg et al., *supra* note 22, at 46.
173. *See* Grannis, *supra* note 130, at 1149.

neglected to acknowledge their potential invasiveness.[174] Similarly, the iRobot privacy policy opens with the statement that the purpose of collecting "personal information" is to "provide you with a personalized, useful and efficient experience."[175]

In addition, the study found that "modal" verbs and adverbs such as "may" and "might" were common. These words downplayed how often companies collected data, which resulted in individual interpretation of how that data was appropriated.[176] In the case of the iRobot privacy policy, the modal verb "may" was used more than forty times and granted the service the ability to share a user's information in specific instances[177] and to collect and store identification numbers unique to the device.[178] In addition, the policy "reserve[d] the right" to de-identify a user's personal data, to retain that information for their own records, and to modify the policy "from time to time," but it failed to specify when and why that would occur.[179] Thus, in the case of the Roomba, the frequent use of modal verbs leads to lack of clarity around how individual data will be used.

Furthermore, Scott Peppet's analysis noted that the language of many policies was unclear about whether the data collected counted as "personal information," which led to more confusion about whether the data could be shared or sold to third parties.[180] The policies often referred to the collection of "personal information" but failed to provide a definition.[181] For some companies, this personal information constituted "personally identifiable information," which is traditionally defined as an individual's name, address, email address, or telephone number.[182] Thus, the majority of information collected by sensor devices would not be protected by this definition.[183] Some policies include language that would lead a consumer to believe the information collected by the device does constitute personal information such as "data that can be reasonably linked to a specific individual or household."[184] When policies fail to clarify what specifically constitutes personal information, or information that is considered nonpersonal information, consumers are left wondering how their data will be used.[185]

For iRobot, personal information is defined as "information about you or associated with you."[186] The policy fails to specify whether information

174. *See* Irene Pollach, *What's Wrong with Online Privacy Policies?*, COMM. ACM, Sept. 2007, at 103, 106.
175. *Privacy Policy*, *supra* note 53.
176. *See* Pollach, *supra* note 174, at 106–07.
177. *Privacy Policy*, *supra* note 53 ("We may share your personal information in the instances described below.").
178. *Id.* ("[W]e may receive or collect and store a unique identification numbers [sic] associated with your device or our mobile application.").
179. *Id.*
180. *See* Peppet, *supra* note 13, at 143.
181. *Id.* at 143–44.
182. *Id.* at 143.
183. *Id.*
184. *Id.* at 144.
185. *See id.*
186. *Privacy Policy*, *supra* note 53.

collected by the device constitutes "personal information," and thus it lacks clarity about how that information can be used.[187] In addition, while the circumstances enumerated in the privacy policy already give the company a significant amount of freedom to share the data,[188] confusion recently arose concerning the chief executive's expressed interest in selling the data to other companies in the coming years.[189] While iRobot has since denied that it plans to sell user data and rather plans only to share it with consumer consent,[190] this situation has raised concerns about what "consent" actually means. It is clear that there are already numerous circumstances in which consent is not required.[191] In short, the language of the iRobot privacy policy is consistent with the findings of previous analyses in that it is unclear as to what and how consumers' information is being used. This lack of clarity highlights the ways that smart-device privacy polices fail to provide adequate notice and thus exposes the limitations on self-regulation.

3. Time Constraints for Reading Privacy Policies

The majority of consumers fail to pay significant attention to privacy policies, despite the fact that they are expected to self-regulate the privacy agreements that they are entering into.[192] Scholars have noted that consumers may choose not to read policies not only because of the verbose language but also because of the length.[193] Another study found that if American consumers were to read every privacy policy that they encountered in a year, it would take them approximately 201 hours and cost about $3534 per American internet user.[194] The study concluded that by decreasing the amount of time it takes to read a policy, and by limiting the amount of text displayed within the policy, consumers would be more likely to read and understand it.[195] The iRobot privacy policy, for example, is nearly 2900 words long.[196] The length of the iRobot privacy policy, compared with other

187. *See id.*

188. *See id.* ("We may share your personal information . . . [with o]ther parties in connection with any company transaction, such as a merger, sale of all or a portion of company assets or shares, reorganization, financing, change of control or acquisition of all or a portion of our business by another company or third party or in the event of bankruptcy or related or similar proceedings.").

189. *See* Jan Wolfe, *Roomba Vacuum Maker iRobot Betting Big on the 'Smart' Home*, REUTERS (July 24, 2017, 7:09 AM), https://www.reuters.com/article/us-irobot-strategy/roomba-vacuum-maker-irobot-betting-big-on-the-smart-home-idUSKBN1A91A5 [http://perma.cc/Q364-CFXN].

190. *See id.*

191. *See* Jones, *supra* note 117 ("Depending on a court's interpretation of that language, it would appear that your consent isn't necessarily required if iRobot wanted to sell its user data in bulk to Apple.").

192. *See supra* Part I.C.

193. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1885 (2013).

194. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008) (analyzing the different costs of reading privacy policies).

195. *Id.* at 567.

196. *See Privacy Policy*, *supra* note 53.

privacy policies, is average.[197] For a person reading at a rate of 250 words per minute,[198] the iRobot policy would take between eleven and twelve minutes to read.

4. Omissions from Smart-Device Privacy Policies

Many privacy policies fail to address important concerns altogether.[199] Numerous privacy policies for smart devices, including that of iRobot, do not mention who owns the data that is collected.[200] IoT policies often fail to specify what data the device collects or lack complete detail about the data.[201] Further, many policies do not specify the security measures that are in place to protect the data from security breaches.[202]

Because IoT privacy policies are difficult to find, have complex language, include terms that are ambiguous or vague, are long and difficult to read, or omit information all together, concerns exist about the validity of consumer consent. As noted by the FTC, notice is a prerequisite to choice.[203] Thus, by not putting a consumer on notice, the consumer likely cannot provide an informed choice about whether to use the device. The problem of not receiving the requisite notice and choice is magnified by the limited legal remedies for a consumer who suffers a privacy harm. The next Part explores how certain existing legal frameworks may address privacy harms.

II. CURRENT STANDARDS AND SHORTCOMINGS OF CONSUMER PROTECTION FOR SMART DEVICES

Notice and choice remains the primary mechanism for regulating the collection of consumer data online.[204] Although privacy policies should enable consumers to self-regulate, investigation shows that they consistently fail to adequately equip consumers to make informed choices about their data.[205] The question thus arises: What are the legal options for consumers who experience privacy-related harms?

This Part explores the current laws and legal remedies available. Part II.A discusses common law contract theory and whether privacy policies constitute legally binding contracts. Part II.B discusses existing state and federal privacy statutes that may protect smart-device users. Part II.C then explains the FTC's role under section 5 to take enforcement action against companies that engage in unfair or deceptive trade practices. Ultimately, this

197. *See* McDonald & Cranor, *supra* note 194, at 554–55.
198. This is the average reading rate for individuals with a high school education. *Id.* at 554.
199. *See* Peppet, *supra* note 13, at 144–45.
200. *See Privacy Policy*, *supra* note 53. Scott Peppet's investigation of twenty IoT devices found that only four of the policies explicitly named who owned the data. *See* Peppet, *supra* note 13, at 145.
201. *See* Peppet, *supra* note 13, at 145.
202. *See id.* at 146.
203. FTC, *supra* note 135, at 14.
204. *See supra* Part I.C.
205. *See supra* Part I.D.

Part highlights the lack of legal remedies available to consumers who have suffered a privacy-related harm, which leaves them vulnerable.

A. Privacy Policies as Legally Binding Contracts

The idea that parties have a "freedom to contract" is central to contract theory. Having "the ability to enter into contracts is traditionally viewed as a 'fundamental' right because it reflects the parties' liberties to control the disposition of their property and alter their legal relationships."[206] Thus, contracts allow parties to create and structure an agreement on their own terms and solidify that agreement in the law.[207] For that reason, the principle of effective notice has been central to common law contracts because without notice or knowledge of the terms, a party to a contract cannot structure the agreement on his terms.[208] Further, if a party does not have effective notice at the formation stage, the contract may be deemed unenforceable.[209] Under this common notion of contract theory, many IoT privacy policies that are elusive, vague, unclear, lengthy, or that leave out critical information could be deemed not to provide effective notice, thus making them unenforceable on the terms that are unclear.[210]

While this line of thinking may seem logical, privacy policies have consistently been found to not carry legally binding weight.[211] Although little case law existed on the subject in the early age of the internet when privacy policies became common, some scholars believed that contract law would play a large role in their enforcement.[212] As case law began to develop, however, plaintiffs had difficulty alleging viable breach-of-contract claims against companies that engaged in practices different from those

206. *See* Grannis, *supra* note 130, at 1120–21; *see also* David P. Weber, *Restricting the Freedom of Contract: A Fundamental Prohibition*, 16 YALE HUM. RTS. & DEV. L.J. 51, 56 (2013).

207. *See* RESTATEMENT (SECOND) OF CONTRACTS: REQUIREMENT OF A BARGAIN § 17 (AM. LAW INST. 1981) ("[T]he formation of a contract requires a bargain in which there is a manifestation of mutual assent to the exchange and a consideration.").

208. *See id.*

209. *See id.*

210. One difference between privacy-policy enforcement cases and cases that seek to enforce other online terms is that privacy-policy cases are usually brought by a user of an online service alleging that the website breached its policy and should be bound to the policy. By comparison, in cases that seek to enforce other online terms, the website provider attempts to enforce a term, such as a mandatory arbitration clause, against the user. *See* Thomas B. Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 189 n.37 (2016). Because privacy policies typically stress how a user's information is being protected and omit or are unclear about when or how a user's information is used, users seek to enforce the terms about the protection of their information. *Id.*

211. *See* Solove & Hartzog, *supra* note 131, at 595–97 (providing an overview of whether privacy policies are typically found to be legally binding contracts).

212. *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91 (1999) ("As between the website and the user, a privacy policy bears all the earmarks of a contract, but perhaps one enforceable only at the option of the user.").

outlined in their privacy policies.[213] In these cases, courts have consistently taken the view that privacy policies are a mere statement of a company's policy and thus do not give rise to a viable contract claim.[214] Courts often follow this reasoning by expressing that even if the policy constituted a viable contract, the plaintiffs failed to establish damages—a critical element to a breach-of-contract claim.[215] In short, courts typically do not find privacy policies to be contractually binding.[216] Even if they did, however, plaintiffs would often have difficulty alleging viable damages.[217]

Another reason courts may reject contract claims for breaching a privacy policy is based on the form of the privacy policy.[218] End-user license agreements (EULAs) are contracts used by internet-based providers that outline the services and functionalities a consumer may expect from a product and that establish a consumer's right to use the product or service.[219] EULAs are usually drafted by the party with the stronger bargaining power and are assented to by the party with weaker bargaining power, usually the consumer.[220] In addition, EULAs are generally required at the point of sale.[221] This disparity in bargaining power results in consumers having little, if any, say over the terms of EULAs.[222]

---

213. *See, e.g.*, Jurin v. Google Inc., 768 F. Supp. 2d 1064, 1073–74 (E.D. Cal. 2011) (dismissing a breach-of-contract claim because the plaintiff could not point to a breach of an express provision of its policy and because a broad statement of policy does not constitute a contract); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 324–27 (E.D.N.Y. 2005) (granting a motion to dismiss for an airline that breached its privacy policy by sharing passengers' names because the passengers were unable to allege a viable form of damages); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199–200 (D.N.D. 2004) (granting a motion to dismiss for an airline and holding that broad statements of policy do not give rise to contractual claims).

214. *See, e.g.*, *Jurin*, 768 F. Supp. 2d at 1073–1074; *Dyer*, 344 F. Supp. 2d at 1199–200.

215. *See, e.g.*, *Jurin*, 768 F. Supp. 2d at 1073 ("Even were a contract present, however, Plaintiff points to no breach of any express provision that would give rise to contractual liability."); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126, 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) ("Even if the privacy policy was sufficiently definite and Plaintiffs had alleged that they read the policy before giving their information to Northwest, it is likely that Plaintiffs' contract and warranty claims would fail as a matter of law. Defendants point out that Plaintiffs have failed to allege any contractual damages arising out of the alleged breach.").

216. *See supra* notes 213–14 and accompanying text.

217. *See supra* note 215 and accompanying text.

218. *See* Norton, *supra* note 210, at 193.

219. *See* Caitlin J. Akins, Note, *Conversion of Digital Property: Protecting Consumers in the Age of Technology*, 23 LOY. CONSUMER L. REV. 215, 223 (2010).

220. *See* Richard Warner, *Turned on Its Head?: Norms, Freedom, and Acceptable Terms in Internet Contracting*, 11 TUL. J. TECH. & INTELL. PROP. 1, 3–4 (2008); Akins, *supra* note 219, at 225.

221. *See* Warner, *supra* note 220, at 3 ("No negotiation is allowed, and by the time the buyer can read the agreement the only options are to return the software or accept the terms."); Akins, *supra* note 219, at 223.

222. *See* Warner, *supra* note 220, at 3 ("[W]hen EULAs are used to sell software, the process is currently defective in ways that result in excessively seller-favorable terms that reduce freedom."); Akins, *supra* note 219, at 223 (discussing an Apple EULA permitting the company to remove apps from any phone at any time).

Clickwrap and browsewrap are forms of EULAs.[223] A clickwrap agreement is one that is intended to garner express consent from those that use a website by requiring them to click on an icon to indicate that they agree to the website's terms. These types of agreements have consistently been upheld by courts as enforceable when the user has assented,[224] even if the user did not read the agreement.[225] Under these circumstances, the user has clearly been informed of and willing accepted the terms, which satisfies the common law principle of notice. By comparison, browsewrap agreements, in which a website displays its terms of use at the bottom of the webpage and considers further use of the webpage to constitute acceptance of the agreement, are typically unenforceable due to the difficulty of establishing a clear manifestation of assent by the user.[226]

A smart-device privacy policy typically takes the form of a browsewrap agreement because the user is expected to read and understand the policy on his own, and there is no explicit manifestation of assent to the outlined policy. Users can choose to view the policy or ignore it.[227] Structuring privacy policies in a browsewrap format—without the contracting principle of mutual assent—makes formation of a contract nearly impossible to establish.[228] Furthermore, companies often seek to establish another layer of protection for themselves by including in their terms that the privacy policy is merely a statement of policy and not a contract.[229]

The doctrine of promissory estoppel has failed to be an effective means of bringing a breach-of-contract claim for privacy policies.[230] Promissory

223. Another type of EULA is a shrinkwrap agreement. A shrinkwrap agreement exists where the contract is enclosed in the packaging of a physical product and the user's act of opening the packaging signals assent to the terms. Courts have upheld shrinkwrap agreements inconsistently. *Compare* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (holding that a shrinkwrap agreement included in a product's packaging was binding on a user because he had the opportunity to read the terms and choose to accept or reject them), *with* Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1337–39 (D. Kan. 2000) (finding the reasoning in *ProCD* that upheld the shrinkwrap agreement to be unpersuasive). However, the shrinkwrap form is typically not used for privacy policies for IoT devices because the policies are often left out of the box. *See supra* Part I.D.1.

224. *See, e.g.*, Hancock v. Am. Tel. & Tel. Co., 701 F.3d 1248, 1257–58 (10th Cir. 2012) (upholding a clickwrap agreement because the user affirmatively manifested assent to the terms).

225. *See, e.g.*, Davis v. HSBC Bank Nev., N.A., 691 F.3d 1152, 1163–64 (9th Cir. 2012) (upholding a clickwrap agreement where a plaintiff checked an "I Agree" box, even though the plaintiff had not actually read the terms).

226. *See, e.g.*, Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1177–78 (9th Cir. 2014) (holding that even when a website makes its terms of use available via conspicuous hyperlink on every page of the website, the agreement is not contractually enforceable when no other notice is given to the user to affirmatively assent to the terms); Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 28–30 (2d Cir. 2002) (holding that inconspicuous contractual provisions laid out in a browsewrap agreement are not binding on a plaintiff even when there is an apparent manifestation of assent).

227. *See supra* Part I.D.1.

228. *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 617 (2007).

229. *See* Norton, *supra* note 210, at 193.

230. *See, e.g.*, Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567, 2011 WL 900096, at *10 n.10 (D.N.J. Mar. 15, 2011) (holding that, because there was

estoppel is meant to protect those who rely on promises to their detriment, even when the essential elements of a contract are not met, by enforcing the promise.[231] In privacy-related actions, the few plaintiffs alleging promissory-estoppel claims have failed due to their inability to show detrimental reliance.[232]

In short, although contract law may seem like a logical and reasonable means for enforcing privacy policies, the limited case law on the subject shows the challenges that arise for plaintiffs bringing these claims. Since privacy policies are generally not contractual in nature or form, courts typically find that they are expressions of policy and thus do not have contractually binding weight. Furthermore, due to the way policies are drafted, plaintiffs have difficulty showing reliance to their detriment on a policy, which causes contractual claims to fail. As a result, both formal contract law and promissory estoppel are rarely used in privacy-related actions and thus are not effective legal measures for smart-device users whose privacy has been violated. The next Part investigates and discusses relevant legislation that applies to privacy-related harms.

B. Sectoral Legislation of Privacy Law

U.S. privacy law is sectoral and is created through different laws, which regulate different industries and economic sectors.[233] This is distinct from the approach in many other industrialized nations in which one overarching statute regulates the use of all personal information, irrespective of who wishes to use that information.[234] This Part first discusses federal laws that address privacy-related harms and then examines state laws.

1. Federal Legislation

In the United States, Congress has passed a number of sectoral statutes that protect specific types of information.[235] This approach draws fine distinctions between the collection of similar types of information.[236] For instance, several different laws govern financial data.[237] The Fair Credit Reporting Act protects credit information and how that information is

no evidence that the plaintiff relied on a promise, no reasonable jury could conclude that a contract existed based on the doctrine of promissory estoppel).

231. *See* RESTATEMENT (SECOND) OF CONTRACTS: PROMISE REASONABLY INDUCING ACTION OR FORBEARANCE § 90(1) (AM. LAW INST. 1981) ("A promise which the promisor should reasonably expect to induce action or forbearance on the part of the promisee or a third person and which does induce such action or forbearance is binding if injustice can be avoided only by enforcement of the promise.").

232. *See, e.g.*, *Trusted Universal Standards*, 2011 WL 900096, at *10 n.10.

233. *See, e.g.*, Solove & Hartzog, *supra* note 131, at 587 ("Privacy law in the United States has developed in a fragmented fashion and is currently a hodgepodge of various constitutional protections, federal and state statutes, torts, regulatory rules, and treaties.").

234. *See id.*

235. *See, e.g.*, Brill & Jones, *supra* note 14, at 1205–06.

236. SOLOVE & SCHWARTZ, *supra* note 130, at 790–91 (explaining that the regulation of TV records is different from the regulation of video rental or sale records).

237. *See* Brill & Jones, *supra* note 14, at 1205–06.

reported,[238] while the Gramm-Leach-Bliley Act requires companies that provide financial products to explain their information-sharing practices.[239] Different laws regulate our health and medical information,[240] such as the Health Information Portability and Accountability Act, which protects our medical information,[241] and the Health Information Technology for Economic and Clinical Health Act, which regulates the protection of electronic health records.[242] In addition, information relating to children has varying legislative protections, such as the Family Educational Rights and Privacy Act, which protects students' educational records,[243] and the Children's Online Privacy Protection Act, which regulates data privacy relating to children.[244]

These statutes cover limited and specific types of information and will not cover a significant amount of data that is collected by smart devices.[245] Thus, there is no federal statute that regulates the general collection of consumer data, which leaves the massive amounts of data collected by IoT devices to be addressed at the state level or through regulatory agencies.

2. State Legislation

State law is another area where certain privacy rights are recognized for citizens of that state with the potential to protect consumer data.[246] In a recent article, Professor Danielle Keats Citron highlighted the critical role of state attorneys general in privacy enforcement.[247] She noted that in the 1990s, when the FTC was promoting the self-regulation model for privacy enforcement, state attorneys general were promoting the adoption of FIPPs as part of consumer protection laws.[248] With this encouragement, states enacted unfair and deceptive trade acts and practices laws (known as "UDAP laws").[249] State attorneys general may enforce UDAP laws by seeking civil penalties, injunctive relief, and attorneys' fees and costs.[250] As states have passed more specific privacy and security laws, the enforcement power of

238. 15 U.S.C. § 1681 (2012).
239. 15 U.S.C. §§ 6801–6809, 6821–6827 (2012).
240. *See* Brill & Jones, *supra* note 14, at 1205.
241. Pub L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.).
242. 42 U.S.C. § 17931 (2012).
243. 20 U.S.C. § 1232g(a)(4), (b) (2012).
244. 15 U.S.C. §§ 6501–6506 (2012).
245. *See, e.g.*, Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 787–88 (2016).
246. *See* Brill & Jones, *supra* note 14, at 1206–07; *see also State Laws Related to Internet Privacy*, NAT'L CONF. ST. LEGISLATURES (June 20, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [http://perma.cc/7JVL-KFPN].
247. *See generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016).
248. *See id.* at 749.
249. *See id.* at 754 ("[T]he typical UDAP law bans deceptive commercial acts and practices . . . whose costs exceed their benefits.").
250. *See id.*

attorneys general has expanded, but UDAP laws remain central to privacy enforcement.[251]

States regulate privacy differently, with some regulating it explicitly and others regulating it through UDAP laws.[252] In California, a leading state in protecting online privacy, privacy is classified as a fundamental right.[253] The California Online Privacy Protection Act of 2003 imposes stringent standards on businesses collecting user information.[254] The law requires that websites that collect "personally identifiable information"[255] must "conspicuously" post a privacy policy[256] and comply with that policy.[257] It also requires that the privacy policy outline the categories of personally identifiable information that are being collected about individual users and the third parties with whom the information is shared.[258] Furthermore, because the law applies to any website that would be used by people in California, it essentially requires privacy policies nationwide.[259]

Similarly, Delaware requires that an enterprise that collects personally identifiable information about users residing in Delaware, such as "[a]n operator of a commercial [i]nternet website, online or cloud computing service, online application, or mobile application," must "make its privacy policy conspicuously available."[260] In addition, in 2017, Nevada enacted a law that requires operators of websites or online services that collect personally identifiable information from those residing in Nevada to inform consumers about how their information is being used.[261]

Both Minnesota and Nevada require internet service providers to keep personal information regarding their customers confidential.[262] In addition, Nebraska and Pennsylvania have amended their unfair-business-practice

---

251. *See id.*

252. *See* Brill & Jones, *supra* note 14, at 1206–07.

253. *See* CAL. CONST. art. 1, § 1.

254. *See* CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2018).

255. Statutes may define "personally identifiable information" slightly differently, but it is typically defined as an individual's first and last name, in addition to another identifying characteristic such as a social security number or driver's license number. Peppet, *supra* note 13, at 137–38.

256. *See* CAL. BUS. & PROF. CODE § 22575(a).

257. *See id.* § 22576; *see also State Laws Related to Internet Privacy*, *supra* note 246.

258. *See* CAL. BUS. & PROF. CODE § 22575(b)(1); *see also State Laws Related to Internet Privacy*, *supra* note 246.

259. *See* Lipman, *supra* note 245, at 793.

260. DEL. CODE ANN. tit. 6, § 1205C (a) (2018); *see also State Laws Related to Internet Privacy*, *supra* note 246.

261. S. 538, 79th Leg., Reg. Sess. §§ 2–6 (Nev. 2017); *see also State Laws Related to Internet Privacy*, *supra* note 246.

262. MINN. STAT. § 325M.02 (2017) ("[A]n Internet service provider may not knowingly disclose personally identifiable information concerning a consumer of the Internet service provider."); NEV. REV. STAT. ANN. § 205.498(1)(a) (West 2017) ("A provider of Internet service shall keep confidential: All information concerning a subscriber, other than the electronic mail address of the subscriber, unless the subscriber gives permission, in writing or by electronic mail, to the provider of the Internet service to disclose the information."); *see also State Laws Related to Internet Privacy*, *supra* note 246.

statutes to prohibit knowingly making a false or misleading statement in a privacy policy.[263]

California and Utah both enacted legislation requiring all businesses, online or not, to inform consumers when they plan to sell or share their personal information to a third party.[264] California's "Shine the Light" law requires all nonfinancial businesses to either allow customers to opt out of information sharing or to disclose to customers the types of information it shares or sells to third parties for direct marketing.[265] Utah enacted similar legislation, which mandates that a business may not share nonpublic personal information about a consumer to a third party for compensation unless the business provides specific notice to the consumer.[266]

While these laws mark a step in the right direction for ensuring adequate privacy protection for consumers of smart devices, they come short of addressing all of the concerns. By mandating privacy policies, states like California and Delaware are going further than the FTC by effectively requiring privacy policies nationwide.[267] However, mandating these policies does not eliminate many of the problems associated with smart-device privacy policies.[268] Even if a company "conspicuously" posts its policy, it may avoid litigation by keeping the policy vague, failing to address certain issues, or failing to notify the consumer of the policy.

The same issue arises with laws prohibiting false or misleading statements such as those in Nebraska and Pennsylvania.[269] Companies can find their way around being deemed false or misleading simply by keeping information vague. The Shine the Light law also has limitations.[270] For instance, the law limits "direct marketing purposes" to specific types of solicitations made to consumers, and it does not include ads on websites or phones or collection by data brokers.[271] In addition, the disclosure requirement is only mandated upon request,[272] and the enforcement of the law has been found to be

263. NEB. REV. STAT. ANN. § 87-302(15) (West 2017) ("A person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation, he or she . . . [k]nowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."); 18 PA. STAT. AND CONS. STAT. ANN. § 4107(a)(10) (West 2018) ("A person commits an offense if, in the course of business, the person . . . knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public."); *see also State Laws Related to Internet Privacy*, *supra* note 246.

264. *See* CAL. CIV. CODE § 1798.83 (West 2018); UTAH CODE ANN. § 13-37-201 (West 2017); *see also State Laws Related to Internet Privacy*, *supra* note 246.

265. CAL. CIV. CODE § 1798.83.

266. UTAH CODE ANN. § 13-37-201.

267. *See* Lipman, *supra* note 245, at 793.

268. *See supra* Part I.D.

269. *See supra* note 263 and accompanying text.

270. *See* Lipman, *supra* note 245, at 793–94.

271. CAL. CIV. CODE § 1798.83(e)(2) (West 2018); *see* Lipman, *supra* note 245, at 794.

272. CAL. CIV. CODE § 1798.83(a); *see* Lipman, *supra* note 245, at 794.

inconsistent.[273] Thus, while these laws are effective in certain ways, they have limitations and fail to achieve comprehensive privacy legislation for smart devices.

While privacy concerns for smart devices are not fully addressed at the state level, it is clear that the state has the potential to impact privacy laws in a meaningful way.[274] State attorneys general are uniquely positioned to address issues of security and privacy because they are on the front lines and can address local conditions and concerns related to privacy through legislation, education, and enforcement.[275] In addition, at the state level, there are fewer bureaucratic requirements, which makes it easier and quicker to move forward on initiatives.[276] Further, because state attorneys general are directly accountable to voters, they are more likely to address the privacy and security concerns of their voters.[277]

C. The Federal Trade Commission

Due to the sectoral nature of laws regulating privacy in the United States and the fact that the data collected by smart devices is not subject to a particular law,[278] data falls under the statutory authority of the FTC.[279] The FTC's authority is broad and overlapping and includes the ability to protect consumers who have been the victims of privacy related claims and to take action against companies nationwide.[280] Despite its broad jurisdiction, its ability to make policy or to enforce laws is limited to either enforcement under section 5 or informal guidance through reports, guidelines, and press releases.[281] While important, these types of informal guidance are not generally binding and are instead considered best practices or "soft law"; thus, they are not useful for a victim of a privacy harm.[282] Accordingly, this Part will focus on the FTC's enforcement authority under section 5.

Under section 5, the FTC has authority to take action against "unfair or deceptive acts or practices in or affecting commerce."[283] When the FTC takes action against a business, it prepares a complaint, which serves as the

273. *See* Robert J. Herrington, *Illuminating California's 'Shine the Light' Law*, LAW360 (Jan. 10, 2012, 8:02 PM), https://www.law360.com/articles/299095/illuminating-calif-s-shine-the-light-law [https://perma.cc/PH25-2HXL].

274. *See* Citron, *supra* note 247, at 767 (discussing how California Attorney General Harris's initiatives "transformed the transparency of the mobile app marketplace").

275. *See id.* at 750.

276. *See id.* at 786.

277. *See id.*

278. *See supra* Part II.B.

279. *See* 15 U.S.C. § 45 (2012); *see also* Solove & Hartzog, *supra* note 131, at 597.

280. *See* Brill & Jones, *supra* note 14, at 1207–08.

281. *Id.* at 1209.

282. *See* Solove & Hartzog, *supra* note 131, at 625–26. The FTC published a report in 2015 discussing the IoT and the important privacy and security implications that arise from it. In the report, the FTC encouraged IoT manufacturers to only collect data that is necessary and to dispose of it when they no longer need it, to de-identify the data that they do collect, and to collect the least sensitive data. *See* FTC, *supra* note 49, at 33–39.

283. 15 U.S.C. § 45(a)(1).

basis of a settlement or, in rare cases, the initiation of litigation.[284] If the FTC is successful, it issues a consent order containing provisions binding the defendant, namely, injunctive relief against continued violations, reporting and auditing requirements, or financial penalties.[285] While consent orders are not considered law and are only binding on the business that enters into them, they often have precedential value as other companies follow them to avoid similar charges.[286]

The number of privacy-enforcement actions has been increasing since the early 2000s, which is likely the result of the increasing number of companies that collect and share consumer information.[287] Unfair acts or practices consist of analyzing whether the act "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[288] The majority of FTC section 5 enforcement actions addressing issues of consumer privacy are not brought under the unfairness prong due to the "substantial injury" requirement.[289] Under the "substantial injury" requirement, emotional harm is likely not considered to be substantial enough to qualify, and only monetary harm or risks to health and safety will be sufficient.[290] Thus, the FTC has been successful in enforcement actions using the unfairness prong in situations involving the "unauthorized disclosure of (1) directly-identifiable personal information (2) that is clearly 'sensitive.'"[291]

Deceptive practices occur when a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances to the consumer's detriment."[292] Cases in which the FTC seeks enforcement action under its section 5 authority have been more common under the deception prong.[293] The FTC has expressed that a misleading practice that would rise to the level of being "material" is one that would be likely to affect

284. *See* Solove & Hartzog, *supra* note 131, at 609–10. The vast majority of FTC enforcement actions end in settlement agreements. One of the main reasons that companies elect to settle with the FTC rather than go to court is because doing so allows them to avoid admitting wrongdoing. *Id.* at 610.

285. *See id.* at 613–14.

286. *See id.* at 620.

287. *See* Grannis, *supra* note 130, at 1116.

288. 15 U.S.C. § 45(n).

289. *See* Brill & Jones, *supra* note 14, at 1210–12.

290. *See* FTC, Policy Statement on Unfairness (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/5T5K-YHEJ] (expressing the limited circumstances where emotional harms could be considered to cause "substantial injury").

291. Brill & Jones, *supra* note 14, at 1211; *see, e.g.*, Complaint Counsel's Proposed Findings of Fact and Conclusions of Law at 1, *In re* LabMD, Inc., No. 9357, 2015 WL 4967222 (F.T.C. Aug. 10, 2015) (alleging that sensitive health information failed to be adequately protected from unauthorized disclosure).

292. FTC, Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception [http://perma.cc/T99S-AXYW].

293. *See* JOEL R. REIDENBERG ET AL., PRIVACY HARMS AND THE EFFECTIVENESS OF THE NOTICE AND CHOICE FRAMEWORK 20 (2014), http://moritzlaw.osu.edu/students/groups/is/files/2015/01/Privacy-Harms-and-Notice-and-Choice-01-12-2015-1-4.pdf [http://perma.cc/DC97-NYJR].

a reasonable consumer's choice regarding his or her use of a product.[294] The FTC has brought enforcement actions against businesses under the deceptive prong when companies act in a misleading way, such as by failing to adhere to the promises laid out in their privacy policies.[295]

The problem with the standard granting authority to the FTC under section 5 is that situations under which the FTC can file a complaint are relatively limited.[296] The language of "unfair or deceptive" essentially requires the FTC to catch a company in a lie, unless there was a monetary or health-related harm, because the Commission still lacks the explicit authority to generally protect online consumer privacy.[297] In addition, the FTC cannot mandate that companies have privacy policies, which "leads to the curious situation whereby a company without a privacy policy is arguably less likely to be punished for privacy invasive practices than a company with a privacy policy."[298] Although most companies now have some form of privacy policy,[299] companies that are simply vague about their commitments to privacy or that have a general privacy policy typically will be immune from action under section 5 authority.[300]

Many companies, such as iRobot, maintain these vague policies[301] and thus would not be subject to a complaint by the FTC. Thus, without a grant of more statutory authority, the FTC will remain tied to the language of section 5, and even a flexible interpretation of the statute will limit its applicability IoT manufacturers.[302] In short, because the FTC's reach is limited, and it only has the legal authority to take action against companies who are explicitly misleading or who cause specific types of harm, it lets companies with vague or ambiguous policies, including many IoT companies, off the hook entirely.

III. A PROPOSAL TO IMPLEMENT MANDATORY STATE-LEVEL REQUIREMENTS FOR SMART DEVICES

By applying the legal framework for privacy law discussed in Part II to the smart devices outlined in Part I, this Note recognizes that the current model of self-regulation is insufficient to protect consumers who use smart

294. FTC, Policy Statement on Deception, *supra* note 292.

295. *See, e.g.*, Press Release, FTC, FTC Approves Final Order Settling Charges Against Snapchat (Dec. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat [http://perma.cc/GQ6L-75R2] (discussing the settlement agreement after the misleading promise made by Snapchat that user messages would disappear instantly after viewing).

296. *See* REIDENBERG ET AL., *supra* note 293, at 19 ("The enabling statute's limitation to unfair and deceptive practices severely circumscribes the agency's authority over online privacy issues.").

297. *See id.* at 19–20.

298. *Federal Trade Commission: Overview of Statutory Authority to Remedy Privacy Infringements*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org//privacy/internet/ftc/Authority.html [http://perma.cc/9PDY-874X].

299. *See supra* notes 253–61 and accompanying text.

300. *See* REIDENBERG ET AL., *supra* note 293, at 19.

301. *See supra* Part I.D.

302. *See* REIDENBERG ET AL., *supra* note 293, at 19.

devices.[303] Due to the collection of vast amounts of data about individuals, their habits, and their lifestyle by smart devices, and the fact that most smart-device privacy policies fail to provide adequate notice to consumers about what they can expect from their devices, user choice is often ill informed.[304] Yet, an ill-informed user who suffers a privacy harm and seeks legal redress is often left empty-handed, absent very specific circumstances. As the IoT grows at an exponential rate with minimal legal regulation surrounding it, this Note recommends greater consumer protection to ensure consumers can make informed choices regarding devices that collect their personal data. Accordingly, this Note argues that state governments are in the best position to address the rapidly growing IoT and to mandate specific requirements for IoT companies that collect user data. First, Part III.A addresses existing scholarship and proposals for IoT regulation and explains why these proposals are insufficient. Next, Part III.B proposes specific ways that state governments can regulate smart devices to better protect consumers and highlights why state governments are in the best position to address the IoT.

A. Existing Scholarship and Proposals for Regulating the IoT

Due to the rate at which the IoT is growing and the lack of a legal framework regulating data collected by smart devices, there has been an influx of legal scholarship about how to best regulate IoT privacy and security practices.[305] While scholars have formed nuanced perspectives on the issue, the overarching categories for regulation of the IoT generally fall into three distinct camps.[306] The first camp, the "free-market approach," advocates sparse regulation of the IoT and argues that regulations will stifle innovation and economic competition.[307] In this view, privacy concerns are not salient enough to merit IoT regulation.[308] The second camp, the "FTC approach," highlights the important role of the FTC in providing guidance for IoT companies and argues that section 5's enforcement authority should be the means for prosecuting IoT companies that cause harm to consumers due to poor data-related practices.[309] The final camp, and the one advocated in this Note, takes an "activist approach." This camp argues that due to the pervasive nature of smart devices and the insufficient legal framework to regulate them, legislation must be enacted to protect consumers.[310]

303. Throughout Part I, this Note highlighted the concerns arising from smart home devices, namely, their unique ability to gain personal information about users and their lifestyle from inside the walls of their homes. This Note recognizes, however, that nearly all security and privacy harms arising from smart home devices are applicable to other types of smart devices. Accordingly, this Part proposes a resolution that should apply to all smart devices.

304. *See supra* Part I.D.

305. *See generally* Branden Ly, Note, *Never Home Alone: Data Privacy Regulations for the Internet of Things*, 2017 U. ILL. J.L. TECH. & POL'Y, 539, 547–56 (discussing the competing approaches for how to regulate the IoT).

306. *See id.*

307. *See id.* at 547–51.

308. *See id.*

309. *See id.* at 553–56.

310. *See id.* at 551–53.

The free-market approach stresses self-regulation and industry best practices to regulate the IoT.[311] The theory underlying this approach is that regulating a growing industry such as the IoT will ultimately "constrain innovation and prevent the development of technologies with substantial social and economic benefits."[312] While the theory of the free-market approach and its goal of promoting innovation are laudable, these benefits do not outweigh the rights of consumers. As has been shown, IoT privacy policies make it difficult for consumers to make informed choices and, thus, to self-regulate.[313] Without enforcement action against companies that fail to provide consumers with adequate information, IoT companies will continue to fail to adequately inform consumers of how their data is being used, and consumers will be left legally empty-handed and vulnerable.

Proponents of the FTC approach, by contrast, focus on maintaining the long-standing practices used to protect consumers in the age of the internet.[314] These practices include using the self-regulatory model of notice and choice,[315] using informal guidance documents such as reports and press releases to outline best practices for companies that collect data,[316] and using its section 5 enforcement authority to prosecute companies that employ "unfair or deceptive" data-collection practices.[317] Many proponents of the FTC approach, however, recognize that, due to the impact the IoT will have, the FTC must adjust its current approach in order to become more effective.[318] Some of these scholars have argued for a more robust notice-

311. *See id.* at 548.

312. *Id.* at 547. Adam D. Thierer, a senior research fellow at George Mason University, advocates the free-market approach. *See* Thierer, *supra* note 47, at 2–3, 84–117. Thierer draws a distinction between the "precautionary principle," the idea that innovations should be curtailed until developers demonstrate that they will not cause harm, and "permissionless innovation," the idea that new experimentation and innovation generally should be permitted, not stifled. *Id.* at 39. He argues that "permissionless innovation" is the best way to regulate the IoT because "[r]egulation—especially regulation of fast-moving, rapidly evolving technologies—is likely to be premature and overly rigid and is unlikely to allow the many beneficial uses of these technologies." *Id.* at 3. He thus advocates for a bottom-up approach using a "combination of educational efforts, technological empowerment tools, social norms, public and watchdog pressure, industry best practices and self-regulation, transparency, and targeted enforcement of existing legal standards (especially torts), as needed." *Id.* at 3–4.

313. *See supra* Part I.D.

314. *See* Ly, *supra* note 305, at 554.

315. *See supra* Part I.C.

316. *See supra* text accompanying note 281.

317. *See supra* Part II.C.

318. Ly, *supra* note 305, at 555.

and-choice regime,[319] while other scholars have highlighted the need for greater guidance from the FTC for best practices.[320]

The FTC model is attractive in that it provides a middle ground. It does not overburden IoT companies with regulations and ensures some form of protection for consumers. Further, the proposals to improve the current FTC would certainly make the model more effective in the era of the IoT. However, even with the implementation of these proposals, the FTC's section 5 authority is ultimately limited.[321] Thus, without supporting federal privacy legislation, using the FTC to enforce against unfair or deceptive practices by smart-device manufacturers will ultimately be insufficient.[322]

Proponents of the third approach, the activist approach, argue that the government should actively regulate the IoT by mandating specific data-collection practices for smart devices.[323] This approach is most beneficial because it would proactively ensure that consumers are aware of how their data is being used. As stated above, critics of this approach have argued that enacting legislation in the early stages of the IoT could have a harmful effect on innovation.[324] Critics also argue that limiting data-collection practices through IoT regulation could hurt consumers because data collection can be a useful tool for understanding and addressing consumer needs.[325] Regardless of the strengths and weaknesses of the activist approach, Congress has declined to regulate privacy for years, and it is unlikely that it will do so in the era of the IoT.[326]

B. Addressing Data-Privacy Concerns at the State Level

Due to the problems with the self-regulatory model of notice and choice,[327] the FTC's limited enforcement authority under section 5,[328] and Congress's

319. *See* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 818 (2015) ("Existing notice and choice regimes have been asked to do more than they are capable of."); Lipman, *supra* note 245, at 793–94 (discussing the need for a mandatory notice-and-choice regime that would enable consumers to make informed decisions about their data and regain control over their personal information). Woodrow Hartzog, a professor at Samford University's Cumberland School of Law, argues the need for a federal agency to take the lead on the development of consumer robotics to protect consumers and explains that the FTC is in the best position to do so. *See* Hartzog, *supra*, at 825.

320. *See* Brill & Jones, *supra* note 14, at 1224–29 (explaining that the FTC should provide guidance to businesses, consumers, and other regulators to help them navigate the challenges of the IoT); Peppet, *supra* note 13, at 157–58 (suggesting that regulators should issue guidance to IoT companies about how to define and treat personally identifiable information).

321. *See supra* text accompanying notes 296–302.

322. *See supra* Part II.C.

323. *See* Ly, *supra* note 305, at 551–53. Scott Peppet advocates the activist approach and argues that the "inherent challenges" of the IoT make the need for a regulatory response urgent. *See* Peppet, *supra* note 13, at 165.

324. *E.g.*, Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, 56 SANTA CLARA L. REV. 593, 619 (2016) (explaining that strict de-identification of data rules may harm valuable data in return for small privacy gains).

325. *E.g.*, Thierer, *supra* note 47, at 73 (discussing how fitness applications can provide data about a consumer's wearable device to advertisers to show them relevant advertisements).

326. *See* Reidenberg et al., *supra* note 22, at 43.

327. *See supra* Part I.C.

328. *See supra* Part II.C.

stagnation in legislating privacy, this Note argues that state governments are in the best position to regulate the IoT.[329] This Part discusses why states are in a strong position to regulate the IoT and acknowledges the novel problems posed by the IoT. It goes on to recognize the current problems with the notice-and-choice model and to propose specific state-level requirements to effectively regulate IoT companies.

1. Benefits of Regulating the IoT at the State Level

Both the novelty and complexity of the IoT make it difficult to regulate. Accordingly, experimentation is necessary to expediently find the most effective method for protecting the private data of consumers. Justice Louis Brandeis highlighted the unique role state governments may play in this regard: "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[330] In this spirit, this Note recommends that individual state governments take the lead in formulating IoT regulations to experiment with and ultimately arrive at the most effective policy.

State governments are uniquely positioned to address issues of consumer privacy because they can serve as laboratories without having a negative impact on the rest of the country. In fact, state attorneys general have been addressing issues of privacy for years.[331] Furthermore, while the FTC was promulgating the self-regulatory model, state attorneys general recognized the need for consumer protection and applied UDAP laws for privacy-related enforcement activity.[332] State attorneys general are well positioned to address privacy-related harms because they are closer to the problems, accountable to their voters, and face fewer bureaucratic requirements, which enables them to advance proposals with speed and efficiency.[333]

Critics of state privacy enforcement argue that promoting this model will lead to overenforcement, with fifty states pursuing the same company for a single data-privacy or security violation.[334] However, in reality, states have limited legal resources and, as a result, want to share the burden of pursuing litigation against companies.[335] Furthermore, IoT regulation is unlikely to be implemented in every state. Another criticism of state privacy enforcement is that federal law could preempt state privacy and security laws in favor of a uniform standard.[336] Federal preemption would be beneficial if it would increase efficiency.[337] However, due to the novelty of the IoT, it is

329. *See infra* Part III.B.1.
330. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).
331. *See* Citron, *supra* note 247, at 749 (expressing that state attorneys general have been on the "front lines" of privacy enforcement even before federal agencies).
332. *See id.* at 749–50.
333. *See id.* at 750, 786.
334. *See id.* at 796–97.
335. *See id.*
336. *See id.* at 801–02.
337. *See id.* at 801.

unlikely that a federal law would maximize efficiency at this time because there has been little experimentation with how to regulate the IoT. Quickly implemented, universal, and untested regulation is likely to result in bureaucratic excess and inefficacy. Further, the possibility of Congress enacting privacy legislation remains unlikely.[338]

Finally, critics also point out the dormant Commerce Clause[339] as a restraint on state privacy laws.[340] However, "no court has struck down a state data breach notification law on the basis of the dormant Commerce Clause" to date, and there is no reason to believe that courts will strike down similar state IoT regulations on that basis in the future.[341] In short, the criticisms of state privacy regulation are unlikely to have any impact on the proposed model for state IoT regulation.

2. Suggestions for State Laws to Address IoT Legal Concerns

Recognizing the benefits of implementing regulations for smart-device companies at the state level and the need to experiment with different regulations to establish what will work best, this Part sets forth proposed rules for the states to consider. This Note proposes that an exemplar state should experiment with IoT regulation by mandating specific requirements for smart-device companies to ensure that consumers are adequately informed of devices' data-collection practices. The proposals for the specific notice requirements were determined based on the analysis of problems with smart-device privacy policies.[342] In addition, using basic contract principles, this Note suggests that the exemplar state should require smart-device companies to obtain an active manifestation of assent by users before enabling the device.[343]

a. Notice Proposal

This Note has highlighted specific privacy and security harms that may befall a consumer from the collection of personal data via smart devices.[344] Due to the nature of these harms, consumers must be fully aware of the risks associated with their devices. Because most smart-device privacy policies fail to adequately inform users of these risks,[345] this Note proposes five rules for the exemplar state to implement that require smart-device companies to provide adequate notice, which will ultimately enable users to make informed choices about whether to use smart devices.

---

338. *See* Reidenberg et al., *supra* note 22, at 43.

339. The dormant Commerce Clause is an implied restraint on state activity where states may regulate interstate commerce unless the regulation "clearly discriminate[s] against interstate commerce" and is not "demonstrably justified by a valid factor unrelated to economic protectionism." New Energy Co. of Ind. v. Limbach, 486 U.S. 269, 274 (1988).

340. *See* Citron, *supra* note 247, at 804–05.

341. *See id.* at 805.

342. *See supra* Part I.D.

343. *See supra* Part II.A.

344. *See supra* Part I.A.3.

345. *See supra* Part I.D.

First, because smart-device privacy policies are often difficult to find, consumers lack awareness that a policy exists at all.[346] Thus, consumers who purchase a smart device should be made immediately aware of the existence of a policy either on delivery or upon setting up the device. This could be achieved by including the privacy policy in the box or by having the policy appear for the user upon setting up the device through an application.

Second, the language used in privacy policies is often unclear or vague.[347] There are a number of different rules that could be implemented to make privacy-policy language clearer. For instance, the exemplar state could mandate that privacy policies provide consumers with concrete descriptions of their data-collection practices.[348] Under this model, instead of stating that the device collects "personal information," the policy would list the specific types and amounts of data it collects.[349] In addition, the exemplar state could require policies to use definitive rather than permissive language.[350] For example, policies could be required to state when exactly user data will be shared, instead of saying "we may share your data."[351] Notice rules could also mandate that privacy policies be presented in the active, rather than passive, voice in order to increase clarity.[352]

Third, it is extremely time consuming to read smart-device privacy policies.[353] To address this issue, the exemplar state could implement length restrictions on privacy policies. Some scholars have suggested a policy resembling that of nutrition labels, which would require companies to summarize succinctly the key points from the policy.[354] The "nutrition label" approach would significantly limit the time required to understand the policy and potentially increase the likelihood of consumers reading it.[355]

Fourth, smart-device privacy policies often omit important information.[356] The exemplar state should identify information that it believes is critical for consumers to be aware of regarding a smart device's data-collection practices and mandate that this information be included in the privacy policy. Privacy policies could be required to include information, such as what data is considered personally identifiable, whether the data the device collects is personally identifiable, how the device collects data, how long the data is retained, who owns the data, and when and with whom the data is shared.

---

346. *See supra* Part I.D.1.
347. *See supra* Part I.D.2.
348. *See* Grannis, *supra* note 130, at 1161–62.
349. *See id.*
350. *See id.* at 1162.
351. *See id.*
352. *See id.*
353. *See supra* Part I.D.3.
354. *See generally* Patrick G. Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CYLAB (Jan. 12, 2010), http://www.cylab.cmu.edu/research/techreports/2009/tr_cylab09014.html [https://perma.cc/4QTX-TF9V].
355. *See, e.g.*, *id.* at 8.
356. *See supra* Part I.D.4.

Finally, smart-device users are particularly susceptible to security-related harms.[357] While the majority of states already have data-breach notification laws,[358] it is also critical that smart-device users are put on notice of the security risks associated with their devices. Therefore, the exemplar state should also mandate requirements for smart-device companies to inform users of how they are protecting user data and the potential security risks associated with collection of that data.

b. "Manifestation of Assent" Proposal

Contract law requires the manifestation of mutual assent between parties.[359] Privacy policies have consistently failed to be given contractually binding weight, and one reason for this may be that their browsewrap form makes it impossible to establish clear manifestation of assent.[360] Thus, this Note argues that, similar to legally binding contracts, it is imperative that consumers of smart devices manifest their express assent to the practices laid out in the privacy policy. Currently, privacy policies do not require active manifestation of assent, and as a result consumers do not read them.[361] Requiring consumers to be active in the agreement is likely to make them more willing to read what is being presented before blindly agreeing to it. Furthermore, if the nutrition label recommendation was implemented,[362] consumers could go through the agreement process relatively quickly. By requiring an active manifestation of assent, the exemplar state would be implementing another policy aimed at protecting consumers to make them aware of what they are agreeing to.

This manifestation of assent could be obtained through a format similar to a clickwrap agreement.[363] When setting up the device, users would be required to affirmatively click "I Agree" to show that they consent to the data-collection practice. For devices that do not require an application or a screen for set up, consumers could manifest assent by using products so long as a notice was visibly posted that informed users that their use would constitute assent. Ultimately, requiring the manifestation of assent to the explicit terms laid out in the privacy policy will serve as another protection for consumers using smart devices.

CONCLUSION

As the IoT expands, the amount of data collected from smart devices will grow and create extensive data profiles on consumers. While the IoT promises to make life easier and more efficient, the mass quantities of data

357. *See supra* Part I.A.3.b.
358. *See supra* note 102 and accompanying text.
359. *See supra* note 207 and accompanying text.
360. *See supra* notes 227–28 and accompanying text.
361. *See supra* text accompanying note 169.
362. *See supra* notes 354–55 and accompanying text.
363. *See supra* text accompanying notes 224–25.

that are being collected, stored, and shared open consumers up to security and privacy risks.

Under the current model of self-regulation in the United States, however, consumers are unaware of these risks and are left legally empty-handed when they suffer a harm. Thus, this Note argues that the pervasive nature of smart devices calls for greater privacy regulation. This Note recognizes that the novelty of the IoT will require experimentation and calls on an exemplar state to implement laws to regulate the IoT and ensure that consumers are aware of its risks.