# NEVER HOME ALONE: DATA PRIVACY REGULATIONS FOR THE INTERNET OF THINGS

*Branden Ly*[*]

TABLE OF CONTENTS



* J.D., University of Illinois College of Law, 2018; B.A., Foreign Affairs, University of Virginia, 2009. I want to thank my Notes Editor, Sayreed Mohrish, for providing critical feedback through the initial phases of the brainstorming and drafting process. Professor Anderson, my legal writing and research professor, gave substantive comments and feedback in the weeks immediately preceding the fall 2017 semester, for which I am eternally grateful. I want to thank the entire JLTP staff for their hard work in getting this Note published. Lastly, my parents, who immigrated from Vietnam in 1979 and successfully ran a restaurant for nearly two decades in Charlottesville, Virginia, have supported me in all my endeavors throughout law school, and I can never thank them enough.

## I. INTRODUCTION

As the Internet and mobile technology have expanded over time, it has become clear that the Internet will remain an embedded part of our lives.[1] That expansion has also enabled a new phenomenon, known as the "Internet of Things," in which devices and sensors connected to the Internet transmit real-time, individualized information about people.[2] Examples of Internet of Things devices include convection ovens that allow consumers to track cooking from their phone and medical emergency bracelets that allow caregivers to see important medical information about a patient.[3] While the Internet of Things holds great promise, it also poses significant challenges. The primary challenge posed by the Internet of Things is how to ensure that companies that manufacture Internet of Things devices can access consumers' data while respecting principles of data privacy and protecting data security.[4]

This Note will examine how the Internet of Things intersects with data privacy law, and what kind of regulatory regime is best suited to ensure that consumers' data privacy is protected. Part II will look at the full spectrum of what the Internet of Things encompasses, including the potential data privacy implications of the Internet of Things. It will detail the current and potential products that make up the Internet of Things. Part III will analyze potential regulatory approaches to the Internet of Things aimed at protecting consumers' data privacy. The approaches fall into three general categories: free-market/anti-regulation, light regulation with appropriate enforcement tools (Federal Trade Commission (FTC) approach), and proactive regulation. The strengths and weaknesses of each approach will then be highlighted. In Part IV, the Author will recommend that the best regulatory approach to protecting data privacy for the Internet of Things is the FTC approach, because it strikes an appropriate balance between fostering the technological innovation that makes the Internet of Things so valuable, while simultaneously using the appropriate amount of regulation to ensure that consumers' data privacy is protected.

1. Nathan Sinnott, *9 Examples of How the Internet of Things Is Already Disrupting Just About Everything*, ENTREPRENEUR, (September 21, 2017), https://www.entrepreneur.com/article/281757.

2. Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#572b4c086828.

3. Angela Ruth, *25 Innovative IoT Companies and Products You Need to Know*, ENTREPRENEUR (Aug. 8, 2017), https://www.entrepreneur.com/article/298943.

4. Michael Chui et al., *The Internet of Things*, MCKINSEY Q. (Mar. 2010), http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things.

## II. BACKGROUND

### *A. What is the Internet of Things?*

The Internet of Things has been defined in many ways by various technology companies, news outlets, and people in the technology industry. For example, Jacob Morgan, a writer from Forbes Magazine, has defined the Internet of Things as "the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other)."[5] The consulting firm McKinsey provides a more detailed definition, stating that the Internet of Things involves "sensors and actuators" in physical objects that are linked to wired and wireless Internet networks, which in return, produce large amounts of volume for computers to analyze.[6] The consulting firm Booz Allen Hamilton goes a step further and notes that the Internet of Things is not simply about connecting devices to the Internet, but is also about letting devices communicate with other devices to create a unique ecosystem that facilitates information-sharing.[7]

### *B. Examples*

In a prescient 2010 report about the Internet of Things, McKinsey categorized Internet of Things devices into two categories, "Information and Analysis," and "Automation and Control."[8] Furthermore, McKinsey broke down these categories into further subcategories.[9] This Note will discuss these subcategories and provide examples thereof.

#### *1. Information and Analysis*

##### a. Tracking Behavior

McKinsey defines tracking behavior as "[m]onitoring the behavior of persons, things, or data through space and time."[10] The most prominent example of an Internet of Things device that tracks behavior is the Fitbit. Fitbit is a company that has been lauded as an innovator in the field of wearable technology and personal activity tracking.[11] Fitbit is particularly well-known for its wristband fitness trackers, whereby a user can track steps, different types of exercises, calories burned, and other types of fitness-related data.[12]

5. Morgan, *supra* note 2.
6. Chui, *supra* note 4.
7. Craig Swanson & Ron Sokolov, *Internet of Things: Move Past the Rhetoric and Focus on Success*, BOOZ ALLEN HAMILTON (Dec. 2014), https://www.slideshare.net/CiscoPublicSector/internet-of-things-move-past-the-rhetoric-and-focus-on-success.
8. Chui, *supra* note 4.
9. *Id.*
10. *Id.*
11. William Weir, *Fitbit Founder and Upcoming Tech Summit Speaker Eric Friedman is an 'Eternally Optimistic' Entrepreneur*, YALE NEWS (Oct. 25, 2016), http://news.yale.edu/2016/10/25/fitbit-founder-and-upcoming-tech-summit-speaker-eric-friedman-eternally-optimistic-entrep.
12. *Id.*

Furthermore, Fitbit serves as a social activity facilitator, because users can track their fitness data and compare it with their family and friends' data.[13]

b. Sensor-Driven Decision Analytics

McKinsey defines "sensor-driven decision analytics" to be "[a]ssisting human decision making through deep analysis and data visualization."[14] In a report about the Internet of Things, Verizon provided an example of a family-owned winery using Internet of Things technology to provide targeted fertilizer application and irrigation to its winery.[15] Hahn Family Wines ("Hahn"), a winery based in Monterey County, California, started a pilot project with Verizon whereby it would use sensor data and analytics to help it better target its fertilizing and irrigation on its wine lands.[16]

Each block of land includes a water flowmeter, "a battery-operated moisture probe that measures four different levels of soil where the grapes are growing," and a weather station to measure air temperature.[17] Data from the sensors is sent to a computer, allowing Hahn to tailor its application of pesticides.[18] The weather station allows Hahn "to monitor solar radiation, wind velocity, humidity, and temperature," which also allows the winery to figure out the best time to apply its pesticides, and the winery can make these decisions in real time.[19]

*2. Automation and Control*

a. Optimized Resource Consumption

McKinsey defines "optimized resource consumption" as "control of consumption to optimize resource use across network."[20] A prime example of this is the idea of a "smart grid."[21] The current U.S. electronic grid is made up of coal, nuclear, and natural-gas-fired generating stations connected to local distribution networks, with power flowing from power plants to consumers.[22] This system, which has been the backbone of U.S. energy supply, is insufficient to meet the demand for energy, pollutes the environment, and is inefficient.[23] The current electric grid system poses substantial difficulties for grid operators

13. *Id.*
14. Chui, *supra* note 4.
15. VERIZON, STATE OF THE MARKET: INTERNET OF THINGS 2016 (Apr. 2016), https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf.
16. *Id.*
17. *Id.* at 17.
18. *Id.*
19. *Id.*
20. *See* Brian Chemel, *Lighting and the Internet of Things*, *2016 DoE Connected Lighting Workshop*, slide 7, ENERGY.GOV, https://energy.gov/sites/prod/files/2016/06/f32/chemel_ IoTintegration_cls2016.pdf (last visited Oct. 21, 2017) (attributing the taxonomy of the Internet of Things application to McKinsey).
21. Scott DiSavino, *U.S. Smart Grid to Cost Billions, Save Trillions*, REUTERS (May 24, 2011, 3:56 PM), http://www.reuters.com/article/us-utilities-smartgrid-epri-idUSTRE74N7O420110524.
22. *Id.*
23. *Id.*

in terms of anticipating peak demand, and the manner in which grid operators account for peak demand is inefficient.[24] Grid operators bring generation systems known as "peaker plants" online to meet peak demand, and these units are expensive to operate, produce greenhouse gases, and sit idle for much of the year.[25]

In place of the current U.S. electronic grid, the U.S. government is engaging in a sustained effort with the private sector to help create a "smart grid" that is more responsive to consumers' demands and that ultimately helps the U.S. supply energy in a less polluting and more efficient manner.[26] The smart grid will incorporate at least two different types of technology that will greatly enhance its interoperability over the current electronic grid.[27] One is called Advanced Metering Infrastructure (AMI), which essentially allows adjustments to be made real-time by consumers based on the pricing of electricity.[28] Real-time energy prices are relayed to home appliances, which are often among the most energy-intensive appliances in a house, and these devices figure out what the consumers' normal usage habits are, enabling consumers to use energy without disruption and at considerable cost savings.[29] Another significant part of the smart grid will be visualization technology, which will allow for significant integration of information regarding external conditions such as sensor data and weather information, which would affect the supply and demand of power.[30]

b. Complex Autonomous Systems

McKinsey defines "complex autonomous systems" as an "automated control in open environments with great uncertainty."[31] Self-driving cars, an example of "complex autonomous systems," are being driven forward in terms of development by current trends, which make car driving by human beings utterly undesirable. First, human drivers lose significant amounts of time unproductively sitting in traffic.[32] In addition, there is the enormous toll of car accidents, resulting in both injuries and loss of life. A joint report commissioned by KPMG and the Center for Automotive Research noted that in 2010, there were 32,788 traffic deaths as a result of roughly six million car crashes, with ninety-three percent of those crashes attributable to human error.[33] There is also

24. U.S. DEP'T. OF ENERGY, *THE SMART GRID: AN INTRODUCTION* 14, https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf. (last visited Oct. 21, 2017) [hereinafter U.S. DEP'T. OF ENERGY].

25. *Id.* at 14.

26. DiSavino, *supra* note 21; U.S. DEP'T. OF ENERGY, *supra* note 24, at 37.

27. U.S. DEP'T. OF ENERGY, *supra* note 24, at 11.

28. *Id.*

29. *Id.*

30. *Id.*

31. *See* Chemel, *supra* note 20, slide 7 (attributing the taxonomy of the Internet of Things application to McKinsey).

32. Gary Silberg & Richard Wallace, *Self-Driving Cars: The Next Revolution*, KPMG & CTR. FOR AUTOMOTIVE RES. 7 (Aug. 2012), http://www.cargroup.org/wp-content/uploads/2017/02/Self_driving-cars-The-next-revolution.pdf.

33. Silberg & Wallace, *supra* note 32.

the environmental impact of driving, which is worsened by the fact that cars often are using gasoline while the driver is just looking for parking, as noted in an MIT Media Lab report.[34]

Autonomous vehicles work by combining several types of technology which help cars function safely and effectively without the need for human control.[35] First, driverless cars have radar sensors to monitor the position of surrounding cars.[36] Second, driverless cars have video cameras that allow them to detect traffic lights, road signs, cars, pedestrians, and other objects.[37] Autonomous cars have Lidar sensors, which bounce light around the car to detect lane markings.[38] Sensors are also embedded in the wheels in order to detect curbs and other parked cars.[39] Lastly, autonomous vehicles have central computer systems which allow them to handle all the data being received, so they can adjust and apply the appropriate "steering, acceleration, and braking."[40]

The potential benefits of the widespread adoption of autonomous cars are enormous and exciting. The first, and most significant of the potential benefits of autonomous cars is the likely decrease in fatalities resulting from automobile accidents.[41] The Insurance Institute for Highway Safety noted that if all cars had forward collision warning, lane departure warning, side view assist, and adaptive headlights, there would be a thirty-three percent reduction in fatal crashes.[42] Other benefits related to productivity, vehicle-related costs, and land use would also be produced. The Rand Corporation estimated that "a household could save about six thousand dollars in fixed annual costs by joining a car-sharing program rather than owning a vehicle."[43] The Rand Corporation notes that parking would likely decrease with the adoption of autonomous vehicles because in urban areas, cars could simply park themselves far away from the center of a city, thus reducing parking usage.[44] Valuable land used for parking spaces could be freed up for other productive uses by cities.[45] Furthermore, autonomous vehicles in the ride-sharing context would have no need to park for the clear majority of the day, because they would simply be picking up and dropping off passengers.[46]

34. William J. Mitchell, *Personal Mobility*, MIT MEDIA LAB, (May 9, 2007), http://h20.media.mit.edu/pdfs/wjm2007-0509.pdf.

35. James Armstrong, *How Do Driverless Cars Work?*, TELEGRAPH, (July 1, 2016, 10:21 AM), http://www.telegraph.co.uk/cars/features/how-do-driverless-cars-work/.

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.*

41. *New Estimates of Benefits of Crash Avoidance Features on Passenger Vehicles: Status Report*, INS. INST. FOR HIGHWAY SAFETY: STATUS REPORT, (May 20, 2010), http://www.iihs.org/iihs/sr/statusreport/article/45/5/2.

42. *Id.*

43. James M. Anderson, et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, RAND CORP. (2016) http://www.rand.org/pubs/research_reports/RR443-2.html.

44. *Id.* at 27.

45. *Id.* at 16.

46. *Id.* at 27.

### *C. Data Privacy Implications of the Internet of Things*

The Internet of Things provides innumerable benefits, but it also has major potential pitfalls relating to issues of data privacy. The collection of personal information relating to habits and physical conditions means that devices often generate millions of discrete data points.[47] More specifically, companies can collect data on consumers that reveal consumers' stress levels, marital status, sleep patterns, and physical activity.[48]

#### *1. Discrimination*

Consumer products companies can take the data they glean from consumers' devices and make certain inferences about consumers, leading to potential discrimination based not only on such factors as race and ethnicity, but also on economic status and medical issues (e.g., weight management).[49] Given the vast amounts of data generated by Internet of Things devices, it is not unthinkable that employers, for instance, would want to get their hands on that data in order to figure out what employees they want to hire.[50] For example, Fitbit data could be used to infer that a potential hire might have traits relating to impulsiveness based on their exercise habits.[51] Data about an individual's sleeping habits, particularly if those sleeping habits are poor, might also prompt an employer to look at a potential applicant in a negative light.[52]

#### *2. Misuse of Consumer Data*

Data privacy is an ever-growing concern with Internet of Things devices, particularly given the fact that these devices take in, analyze, and produce voluminous amounts of data. One of the major concerns regarding data privacy for Internet of Things devices is that if the data somehow ended up in the wrong hands, a hacker could identify which individual matched with the data.[53] A possible solution is de-identification, a process whereby consumers' data is combined and anonymized, with companies promising not to release consumers' data to anyone else.[54] The anonymization process involves two steps: removing personal identifiers such as "names and Social Security numbers" and then modifying other types of information that also serve an identification purpose,

47. FED. TRADE COMM'N, INTERNET OF THINGS: PRIV. & SEC. IN A CONNECTED WORLD, FTC STAFF REPORT 14 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter CONNECTED WORLD].

48. *Id.*

49. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 117 (2014) (discussing general problems with data privacy).

50. *Id.* at 120.

51. *Id.* at 119.

52. *Id.*

53. *Id.* at 128.

54. *Id.*

such as bank account and student ID numbers.[55] This process seems relatively straightforward and workable. However, MIT researchers analyzed data from one-and-a-half-million cell phone users from a European country and found out that if they had just four data points, they could uniquely identify ninety-five percent of the users, demonstrating the limits of de-identification.[56]

Another major data privacy implication of the Internet of Things is that data collected by Internet of Things devices could be sold to other companies, for marketing and other purposes.[57] Examples of this include data analytics companies allowing retailers to gain access to their Wi-Fi connection in order to track foot traffic by following the location of consumers' smartphones, or Verizon's announcement that it would sell consumers' smartphone data.[58] The concern is that the use of data in this manner is contrary to the wishes of the consumer.[59]

### *3. Problems with Implementing Notice and Consent*

With the worries about how companies will use consumers' data, one possible solution is for companies to provide some sort of consent agreement for consumers to sign or otherwise verify that they consent to how companies will use their data. "Notice and Consent," the traditional approach with which regulators approach issues of data privacy, is much more difficult to enforce in the context of the Internet of Things when devices do not allow consumers to provide consent in traditional ways.[60]

Assuming that an Internet of Things device has a screen, one would think that a notice-and-consent form would be available there for consumers to click through and either consent or not.[61] However, some Internet of Things devices, such as a Fitbit tracker, have small displays, and thus, it is very hard to imagine that a consumer has a notice-and-consent option available on such a device.[62] An alternative manner in which an Internet of Things device manufacturer could provide a consent form would be through the packaging that comes in the box of a device.[63] However, Scott Peppet, a University of Colorado law professor, purchased twenty Internet of Things devices, and found that none of them contained any consent forms related to data privacy.[64]

A further problem with consent forms for Internet of Things devices is the ambiguous language in which the consent forms are written. For instance, some

55. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703 (2010).

56. Larry Hardesty, *How Hard Is It to "De-Anonymize" Cellphone Data?*, MIT NEWS (Mar. 27, 2013), http://newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.

57. Marc Rotenberg et al., *Comments of the Electronic Privacy Information Center to the Federal Trade Commission on the Privacy and Security Implications of the Internet of Things*, ELECTRONIC PRIVACY INFO. CTR. 1, 12 (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

58. *Id.* at 13.

59. *Id.*

60. Peppet *supra* note 49, at 139–40.

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

policies define personal information as only including telephone number, email address, and mailing address, thus excluding a large swath of data gathered from Internet of Things devices, which a consumer would likely categorize as personal data.[65] Some of the actual definitions of personal information include "data that can be reasonably linked to a specific individual or household"[66] or "any information that can be used to identify you."[67] Neither of these definitions is particularly useful to a consumer trying to figure out what data is being collected by a company.

## III. ANALYSIS

With the potential data privacy pitfalls presented by the Internet of Things, there are several competing approaches for how to regulate it in relation to data privacy. The first is a free-market approach that calls for very minimal regulation on the subject; the second is the current approach favored by the FTC, which favors using FTC's Section 5 enforcement authority to prosecute companies that violate consumers' data privacy and advocates for flexible data privacy regulation; the last approach favors an aggressive introduction of legislation meant to protect consumers' data.[68] This Note will compare these three approaches, discussing their strengths and weaknesses, and argue that the FTC approach is the best approach going forward.

### *A. Free-Market Approach*

The free-market approach to data privacy regulation for the Internet of Things argues that while there may be legitimate concerns about protecting the data privacy of consumers, such concerns should not trump concerns about preserving "innovation, entrepreneurialism, economic growth, price competition, and consumer choice."[69] Moreover, free-market proponents believe that regulation of quickly evolving industries will constrain innovation and prevent the development of technologies with substantial social and economic benefits.[70] Instead, this approach envisions using self-regulation, watchdog pressure, and industry best practices to regulate the Internet of Things.[71]

65. *Id.* at 142.

66. *Privacy Statement for Nest Products and Services*, NEST, https://nest.com/legal/privacy-statement-for-nest-products-and-services/ (last visited Oct. 21, 2017).

67. *Belkin Privacy Policy*, BELKIN, http://www.belkin.com/us/privacypolicy/ (last visited Oct. 21, 2017).

68. *See generally* Adam Thierer, *The Internet and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J. OF LAW AND TECH. 3 (2015) (describing the approaches to regulating the Internet that are related to data privacy).

69. *Id.* at 3.

70. *Id.* at 13–15.

71. *Id.* at 114.

### *1. Tenets of the Free-Market Approach*

The free-market approach to regulating the Internet of Things would benefit device manufacturers by avoiding the costs of additional regulation.[72] It also emphasizes the most favorable characteristics of the Internet of Things. Proponents of the free-market approach focus on the concept of permission-less innovation, the idea that businesses should be able to experiment and innovate in creating new technologies, absent any serious foreseeable harms to consumers.[73] These proponents argue that oftentimes, regulatory regimes are too slow to adapt to the fast-changing realities of technology and can end up hindering the development of innovation by increasing the cost of building a business.[74]

The theoretical underpinnings of the free-market approach focus on the fallacies of "privacy paternalism."[75] Privacy paternalism is the belief that regulators, who have certain idiosyncratic preferences, often impose policies that end up limiting the freedom and choices of consumers.[76] For instance, FTC Commissioner Maureen Ohlhausen suggested in a speech given to the U.S. Chamber of Commerce that government regulators should exercise "regulatory humility" when it come to new technologies.[77] "Regulatory humility" entails deferring the proposal of any new regulations until after gaining a thorough understanding of the entities or individuals that might be affected by the regulations, and deciding whether current statutes and regulations are sufficient.[78] Free-market proponents note that regulators believe that consumers exercise irrational decision-making when it comes to purchasing products and being manipulated by companies, but regulators overlook their own ignorance in regards to consumer welfare.[79]

When applied to the Internet of Things, the free-market approach to data privacy regulation focuses on educating consumers, encouraging industry best practices, and using current enforcement tools to help protect consumers' data privacy.[80] This approach does not include any proposals for new regulations. In terms of encouraging industry best practices, free-market proponents focus on "use restrictions" for data.[81] "Use restrictions" focus on how businesses use the data, after they have collected it from consumers.[82] Free-market advocates think that Internet of Things companies should provide information to consumers

72. See *id.* at 47–48 (stating that increased regulations raise the costs of running a business and can limit the range of choices consumers have, thus negatively affecting the free-market).

73. *Id.* at 3.

74. *Id.* at 47.

75. *Id.* at 68.

76. *Id.*

77. Maureen K. Ohlhausen, Commissioner, Federal Trade Commission, The Internet of Things and the FTC: Does Innovation Require Intervention?, Remarks Before the U.S. Chamber of Commerce (Oct. 18, 2013) https://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131008internetthingsremarks.pdf.

78. *Id*. at 3–4.

79. Thierer, *supra* note 68, at 50.

80. *Id*. at 84–87.

81. *Id*. at 64–65.

82. *Id*. at 83.

about their data use policies, limit the amount of data they collect and the third-parties they share the data with, and try to protect the data from intrusions and breaches.[83]

For consumer education, free-market advocates believe that teaching "digital literacy" and providing online resources for consumers to peruse will help them navigate potential data privacy pitfalls.[84] Digital literacy involves teaching children and adults how to manage the information they share online, to ensure that others will not use their information for improper purposes.[85] The behaviors that regulators might target are the use of social media, the need to create and update strong passwords, and avoiding websites and online advertising that might result in consumers providing data or information that they would not want disclosed.[86]

Current enforcement tools primarily reside under Section 5 of the FTC Act to police data privacy relations.[87] Under Section 5, the FTC has the authority to prohibit acts that are "unfair or deceptive . . . affecting commerce."[88] The FTC has used its Section 5 authority to bring enforcement actions against Google, Twitter, and Snapchat, among others, for alleged data-security and privacy-related infractions.[89]

### *2. Analysis of Free-Market Approach*

The free-market approach to regulating the Internet of Things has many positive attributes, but it is deeply problematic in its assumption that use-based restrictions will work and that no regulation is necessary. Use-based restrictions may work in theory, but in practice they pose significant obstacles when it comes to implementation. Use restrictions "depend upon self-enforcement," which assumes that companies are only going to use data for highly-restricted purposes and not for other uses which may be commercially profitable.[90] In addition, use restrictions depend on the assumption that the full range of harmful uses of data is known at the time the data is collected, but it is often difficult to know how data will be used in the future.[91] In addition, it is unclear what can be done once data has been used in a manner inconsistent with a company's use restriction.[92] Restrictions on how much and what kind of data can be collected are also

83. *Id*. at 73.
84. *Id*. at 118.
85. *Id*. at 118–19.
86. *Id*. at 87.
87. *Id*. at 106.
88. *Id*.
89. *Id*. at 148.
90. Marc Loewenthal, *Internet of Things: Current Privacy Policies Don't Work*, INFO. WK. (June 30, 2014, 9:06 AM), http://www.informationweek.com/big-data/hardware-architectures/internet-of-things-current-privacy-policies-dont-work/a/d-id/1278925.
91. Alvaro Bedoya & David Vladeck, Comment Letter on "Big Data and Consumer Privacy in the Internet Economy," Docket No. 140514424-4424-01 (Aug. 5, 2014), https://www.law.georgetown.edu/academics/centers-institutes/privacy-technology/publications-filings/upload/8-5-14-Bedoya-and-Vladeck-Comment-FINAL.pdf.
92. Loewenthal, *supra* note 90.

difficult to enforce because "[i]t is impossible to monitor every device to confirm that the data being collected is consistent with the purpose intended."[93]

Another major flaw with the free-market approach to regulating the Internet of Things is that it acts as if harms caused by mismanaging a consumers' data privacy are negligible. However, that is clearly not the case. For instance, the *New York Times* published an article discussing how companies use data analytics to target specific classes of customers.[94] In the article, the *New York Times* noted an instance where Target applied statistical analysis to its baby shower registry to figure out what products pregnant women purchased at specific stages of their pregnancy, and then used this information to mail coupons for baby care products to women who were likely to be pregnant.[95] A year after Target created this model, a man walked into a Target store in Minneapolis, angry that his daughter was receiving coupons for baby cribs, accusing Target of trying to encourage his daughter to become pregnant.[96] He later apologized after finding out that his daughter was indeed pregnant.[97] This may seem like an extreme example, but it touches on the tip of the iceberg in terms of the lengths companies will go to in order to use consumers' data for their commercial benefit.

The free-market approach also ignores the fact that the current state of data privacy affairs, where there is a lack of both data privacy regulation and understanding of how the Internet of Things works, creates an ideal environment for companies to exploit the public's lack of knowledge. A report by *Politico* noted, for instance, that the federal "government doesn't have a single mechanism to address the Internet of Things or the challenges it's presenting."[98] In addition, the FTC—the primary government agency tasked with policing privacy-related infractions—does not have the necessary statutes or regulations that would allow it to fully tackle data privacy violations.[99] The stunning ignorance of government officials who do not understand the implications of the Internet of Things is illustrated by this quote from Deb Fisher, a Republican senator from Nebraska who sponsored a resolution praising the Internet of Things: "[a]sk me what the Internet of Things is . . . I don't know . . . [b]ut there are people out there that experiment, and they're innovative and they're entrepreneurs and they're creating things like mad, and that's their job."[100]

Moreover, free-market proponents of the Internet of Things ignore the considerable angst among consumers and technology executives regarding the privacy implications of the Internet of Things. Per the abovementioned *Politico* article, a survey of forty technology leaders revealed that the clear majority of

93. *Id.*

94. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp.

95. *Id.*

96. *Id.*

97. *Id.*

98. Darren Samuelsohn, *What Washington Really Knows About the Internet of Things*, POLITICO (June 29, 2015, 5:25 AM), http://www.politico.com/agenda/story/2015/06/internet-of-things-caucus-legislation-regulation-000086.

99. *Id.*

100. *Id.*

them did not believe that the data on their devices would be secure, and most of them supported a national policy on data privacy.[101] Furthermore, according to a recent *Fortune* magazine article, forty-seven percent of consumers expressed some level of discomfort with companies using data collected from their homes, and even more—fifty-six percent—were uncomfortable with companies selling data culled from their home to others.[102]

### *B. The Activist Approach*

The activist approach, as embodied by organizations such as the Electronic Privacy Information Center (EPIC), advocates for the government to take a proactive approach to protecting consumers' data privacy in relation to the Internet of Things.[103] Such an approach would entail the enactment of regulation that would prohibit potential privacy violations by Internet of Things companies.[104] Such an approach may produce substantial benefits by protecting consumers' data from exploitation by companies, but could backfire considerably because the Internet of Things is in its relative infancy, and such an activist approach could hamstring technological innovation and end up harming consumers more than it helps them.

#### *1. Tenets of Activist Approach*

The activist approach to regulating data privacy for the Internet of Things focuses on requiring companies to undertake measures to protect consumers' data.[105] Policies that activists have suggested include imposing use constraints on companies use of consumers' data, requiring companies to gain user consent before using data for purposes not related to the services being provided to the consumer, and imposing limits on the kind of data that companies can collect from consumers.[106] These proposals are not original, and the FTC has, in some measure, encouraged companies to undertake these measures.[107]

One part of the activist approach would require Internet of Things companies to let consumers know about their data collection practices, and to allow consumers to see what kind of data the company collects about them.[108] Advocates of the activist approach support allowing consumers to see the methodology that companies use in determining what kinds of consumer data to collect.[109] The European Union has adopted a similar approach to data

101. *See* Stephen Hueser, *Survey: Experts Don't Trust Their Devices—or Congress*, POLITICO (June 29, 2015, 5:27 AM), http://www.politico.com/agenda/story/2015/06/internet-of-things-tech-leaders-survey-000109 (detailing a survey of technology leaders' views on the Internet of Things and Congress).

102. Stacey Higginbotham, *Companies Need to Share How They Use Our Data. Here Are Some Ideas.*, FORTUNE (July 6, 2015), http://fortune.com/2015/07/06/consumer-data-privacy/.

103. *Id.* at 17–20.

104. *Id.* at 17.

105. *Id.* at 18.

106. Peppet, *supra* note 49, at 150–153; Rotenberg, *supra* note 57, 17–20.

107. CONNECTED WORLD, *supra* note 47.

108. Rotenberg et al., *supra* note 57, at 19.

109. *Id.*

transparency on behalf of consumers, allowing consumers the ability to see "the logic involved in any automatic processing of personal data."[110]

Another part of the activist approach involves requiring Internet of Things companies to not use consumers' data in a manner to which consumers would object.[111] These types of regulations are known as "use constraints," and are classified into two categories: cross-context use constraints and within-context use constraints.[112] Examples of cross-context use constraints include prohibiting Internet of Things companies from using customer data collected as a proxy for race, or other protected categories of individuals, and prohibiting Internet of Things companies that make health and fitness apps from providing data collected from consumers to insurance companies who might set insurance premiums based on such data.[113] Prohibitions on forced disclosure even within a given context means that consumers should not be pressured to reveal certain types of information to companies.[114] For instance, the Electronic Privacy Information Center has argued that insurers should be prohibited from using data gleaned from Event Data Recorders (EDR—i.e., automobile black boxes) to determining premium payments or from "conditioning the payment of a claim" on the ability of the insurer to use EDR data.[115]

Another tenet of the activist approach calls for companies to only collect the minimal amount of data necessary to ensure the functionality of the products being used. Examples of data minimization practices include collecting data periodically rather than collecting data on a regular basis, or collecting data from a representative group of individuals rather than an entire group of individuals.[116] Data minimization serves dual purposes of making sure that companies do not retain so much consumer data that they become an enticing target for hackers, and that companies do not use data in ways that are contrary to the expectations of customers.[117]

### *2. Analysis of Activist Approach*

Having detailed these potential policies above, it is appropriate to focus on the potential flaws with making these policies mandatory rather than voluntary. The activist approach is predicated on the belief that the government knows exactly what types of data should or should not be collected, knows how consent is manifested, and can predict how companies will use consumers' data in the future.[118] As Adam Thierer, a Senior Research Fellow at George Mason's Mercatus Center, has pointed out, "[o]verly prescriptive regulatory systems can

110. *Id*.
111. *Id*. at 12.
112. *See* Peppet, *supra* note 49, at 150–53 (detailing "Use Constraints").
113. *Id*. at 151.
114. *Id*. at 152.
115. *Id*.
116. Rotenberg, *supra* note 57, at 13.
117. Monica Alleven, *FTC Report Focuses on Security, 'Data Minimization' for Internet of Things*, FIERCEWIRELESS, (Jan. 28, 2015, 3:17 PM), http://www.fiercewireless.com/tech/ftc-report-focuses-security-data-minimization-for-internet-things.
118. Thierer, *supra* note 68, at 49.

raise the cost of goods and services, diminish the quality of those goods and services, or limit the range of choices that the public has at its disposal."[119] Furthermore, as privacy scholars Jules Polonetsky, Omer Tene, and Kelsey Finch have noted, "overly strict de-identification rules that are geared at eliminating remote privacy risks may jeopardize valuable data uses in return for small privacy gains."[120]

A major critique of requiring companies to adopt use-based constraints is that the potential scope of legislation may be overbroad and there is insufficient clarity regarding what types of uses of consumers' data should be banned. The FTC noted that since there is currently no widely-accepted definition of what counts as a harmful or beneficial use of consumers' data, it would be unclear who would make that decision.[121] Furthermore, focusing exclusively on use-based constraints for data collection neglects the question of how much data collection is too much.[122]

Data minimization regulation poses the risk of stifling innovation and hurting consumers, because companies use consumers' data to make sure that their devices are tailor made for consumers' needs. For instance, makers of fitness applications provide consumers' information to advertisers, allowing them to show more relevant advertisements to consumers.[123] Limits on data collection also pose potential legal issues regarding the First Amendment, since restrictions on data collection impact the free flow of information.[124] This issue came up in *Sorrell v. IMS Health Inc.*, where the Supreme Court "struck down a state law prohibiting data aggregators from selling personal information to pharmaceutical companies . . . ."[125] This ruling means that any regulation that is crafted for the purposes of limiting data collection needs to be narrowly tailored to preempt any First Amendment challenges.[126]

### *C. FTC Approach*

The FTC's approach to regulating the Internet of Things during the Obama Administration involved using some of the principles that the free-market proponents advocate, but was also marked by pressing for more flexible and broad privacy regulation beyond focus on only the Internet of Things.[127] The FTC is the primary government agency tasked with policing potential data privacy violations related to the Internet of Things.[128] The FTC encourages Internet of Things companies to provide notice to consumers regarding what kind of data companies collect and offering consumers choices about how their

119. *Id*. at 48.
120. Jules Polonetsky, et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 SANTA CLARA L. REV. 594, 619 (2016).
121. CONNECTED WORLD, *supra* note 47, at vi.
122. *Id*. at vi–vii.
123. Thierer, *supra* note 68, at 73.
124. *Id*. at 75.
125. *Id*. at 75–76.
126. *Id*. at 76.
127. CONNECTED WORLD, *supra* note 47, at vii.
128. Samuelsohn, *supra* note 98.

data will be used by companies.[129] Under the Trump Administration, it is unclear what approach the FTC will take, though the Acting Chairwoman of the FTC, Maureen Olhausen, favors the free-market approach to data privacy regulations for the Internet of Things.[130]

*1. Tenets of FTC Approach*

The FTC focuses on encouraging Internet of Things companies to adopt the principles of data minimization and notice and consent, using its Section 5 authority to punish companies that violate consumers' data privacy, and pushing for broad-based data privacy regulation. Data minimization involves efforts by companies to try to limit the amount of consumers' data they collect.[131] The FTC offers four ways in which companies can engage in data minimization: collect no data at all; collect only the data necessary for the product to function; collect data that is less sensitive, or; de-identify consumers' data.[132] De-identification involves the process whereby Internet of Things companies ensure that the data they collect from consumers cannot be re-identified.[133] This process involves removing certain types of identifying information such as a consumer's birth date or zip code.[134]

Notice and choice (also referred to as notice and consent) involves Internet of Things companies providing consumers with notice that they are collecting their data, and allowing consumers to choose whether they want their data to be collected.[135] The FTC suggests a myriad of ways for companies to offer notice and choice. Examples include allowing consumers to opt-in—and allow companies to collect their data—when they purchase a product, providing notices when a consumer is setting up a product, and providing privacy portals for consumers to manage their privacy settings, much like what Facebook does.[136]

The FTC's Section 5 authority allows it to police potential violations of data privacy that are the result of "unfair or deceptive acts or practices in or affecting commerce."[137] The language of Section 5 does not contain any references or inferences relating to data privacy, but the FTC has used its statutory authority under Section 5 for over a decade to police potential data privacy violations.[138]

129. CONNECTED WORLD, *supra* note 47, at 50.

130. Sam Thielman, *Acting Federal Trade Commission Head: Internet of Things Should Self-Regulate*, GUARDIAN (Mar. 14, 2017, 6:00 AM), https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation.

131. CONNECTED WORLD, *supra* note 47, at iv.

132. *Id.*

133. *Id.* at 37.

134. *Id.*

135. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882 (2013).

136. CONNECTED WORLD, *supra* note 47, at 42.

137. Ryan T. Bergsieker et al., *The Federal Trade Commission's Enforcement of Data Security Standards*, ANTITRUST & CONSUMER PROTECTION L. (June 2015), http://gibsondunn.com/publications/Documents/Bergsieker-Cunningham-Young-FTC-Data-Security-Enforcement-06.2015.pdf.

138. *Id.*

The type of legislation that the FTC seeks to pass would be general legislation focused on privacy, not necessarily the Internet of Things per se. Such legislation would be focused on providing standards for companies to follow, such as when to provide privacy notices, as well as guidelines about data collection and usage.[139] The FTC believes that such legislation is necessary to assuage consumers' concerns regarding the data that is collected from their devices and companies' lack of transparency regarding data collection and usage practices.[140]

### *2. Analysis of FTC Approach*

The FTC approach is likely the best way forward when it comes to making sure that companies do not abuse consumers' data privacy, but it does need some improvement to become a more substantive and effective enforcement mechanism. The FTC's focus on data minimization and traditional notions of notice and consent is flawed, but encouraging companies to adhere to basic data privacy principles and proposing general data privacy legislation makes sense. The FTC is correct in trying to strike a balance between being an overzealous regulator and trying to curb the worst abuses by Internet of Things companies.

There is strong reason to believe that the traditional notions of notice and consent when applied to Internet of Things devices is likely to be ineffective. As privacy scholar Daniel Solove has pointed out, the two major problems with the notice and consent model are firstly, that consumers are uninformed about the terms in the notice agreements companies provide, and secondly, that when consumers have to make decisions regarding whether to consent to companies collecting their data, their decision-making processes are skewed.[141] Solove notes that most consumers do not read privacy notices and it is rare for consumers to opt out of allowing companies to collect and use their data.[142] The core problem with using notice to protect consumers is that proposals to simplify notice and consent end up watering down policies and details that need to be explained in order for consumers to understand how their data will be collected and used.[143]

Despite these valid objections to using notice and consent, the FTC has attempted to strike a middle ground between allowing technological innovation to flourish and helping to protect consumers' data from exploitation in the area of notice and consent. The FTC has stated that, "companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer."[144] By making this statement, the FTC recognizes that not all instances where a company collects consumer data are inherently against the interest of consumers. The FTC provides a hypothetical

139. CONNECTED WORLD, *supra* note 47, at 50.
140. *Id.* at 51–52.
141. Solove, *supra* note 135, at 1883–86.
142. *Id.* at 1884.
143. *Id.* at 1885.
144. CONNECTED WORLD, *supra* note 47, at 40.

whereby an oven company collects data to help adjust the temperature of the oven to the consumers' liking (consent authorized) versus the oven company selling consumers' data to a third-party data broker (consent not provided).[145] The FTC also provides an array of options for Internet of Things companies to use in order to provide appropriate notice and consent to consumers, ranging from tutorials to privacy menus.[146]

The idea of using data minimization to protect consumers' data privacy also contains significant flaws. There is considerable and heated debate over whether de-identifying data is even plausible.[147] Furthermore, by forcing companies to minimize the amount of data they collect, the government would hinder potential future uses of data that would produce positive benefits for society, which are not known at the moment.[148] For data de-identification to work, numerous measures, including data retention restrictions, encryption, and automated data validation need to be implemented.[149]

Despite the legitimate criticisms of data de-identification, there is some merit to at least trying to implement it. Data de-identification would allow researchers to share and publish private data, minimizing the potential for data to be used for nefarious ends.[150] Data de-identification strikes a middle ground between not protecting consumers' data from being used for means which consumers would not approve and creating a "black box," whereby no one can use consumers' data. There is a broad recognition that consumers' data has substantial uses that might require disclosing user data, a good example being traffic applications which combine geolocation data to provide drivers using mobile devices "real-time information about their surroundings."[151] Data de-identification is not a foolproof solution, but it serves a valuable purpose in allowing researchers to use data for practical research purposes, while also minimizing the possibility that consumers' data could be used to identify them without their knowledge.[152]

## IV. RECOMMENDATION

This Note recommends that the best approach to regulating the Internet of Things is to follow the current approach favored by the FTC, which favors using the FTC's enforcement powers under Section 5 of the FTC Act to ensure that Internet of Things device manufacturers do not engage in "unfair or deceptive" practices, but to also to formulate preliminary regulations that focus on how manufacturers use the data they accrue from consumers.

The FTC approach, despite its drawbacks, has substantial benefits which help maintain the balance between encouraging technological innovation and

145. *Id.*
146. *Id.*
147. Polonetsky, *supra* note 120, at 594.
148. *Id.* at 619.
149. *Id.* at 621.
150. *Id.* at 595.
151. *Id.* at 625.
152. *Id.* at 622.

safeguarding consumers' data. A good example of this approach is the FTC's emphasis on the concept of data minimization. Data minimization means that "companies should limit the data they collect and retain, and dispose of it once they no longer need it."[153] Data minimization could be hard to apply, since companies may want to keep certain kinds of data for beneficial uses.[154] However, the FTC has taken a flexible approach which balances these twin concerns by noting that companies can decide to not collect any data at all, only collect data that is necessary for whatever product or service they are offering, collect less sensitive data, or de-identify data.[155]

The FTC has also promoted the idea that Congress should pass general privacy legislation, which would provide guidelines for companies to follow to help protect consumers' data privacy. The FTC wants Congress to consider passing legislation that would provide guidance for when to provide privacy notices to consumers as well as encouraging companies to offer consumers "choices about data collection and use practices."[156] These recommendations are meant to nudge companies to take a meaningful first step towards greater transparency regarding how they manage consumers' data and the degree to which consumers have any say in how their data is used.[157]

The FTC's Section 5 Authority, while perhaps not as strong as it would be if there were federal privacy legislation to back it up, has proven to be effective in punishing companies that do not take sufficient measures to protect consumers' data. In cases where the FTC believes a company has engaged in Section 5 violations by failing to protect consumers' data, it has filed lawsuits, which often end in settlements and consent decrees.[158] A consent decree "often requires the defendant to establish and execute a program of improvements to its data privacy and system security practices."[159] In addition, the "program is then subject to periodic outside audits by independent parties . . . for the length of the settlement period, which can be as long as [twenty] years."[160] Lastly, "defendants must agree to pay fines to the FTC if the consent orders are violated at any time during that period."[161]

An additional benefit of the FTC using its Section 5 Authority to punish companies who engage in data privacy violations is that Section 5 is flexible and allows the FTC to fill an enforcement vacuum rather than letting companies act irresponsibly. Section 5 jurisprudence for data privacy and the Internet of Things is evolving.[162] Companies have generally been unsuccessful in challenging the FTC's Section 5 authority when it comes to data privacy

153. CONNECTED WORLD, *supra* note 47, at iv.
154. *Id.*
155. *Id.*
156. *Id.* at 50.
157. *Id.* at 51.
158. Stephen Cobb, *FTC IoT Privacy and Security Push Points Out D-Link Router and Webcam Flaws*, WELIVESECURITY (Jan. 6, 2017, 4:05 PM), http://www.welivesecurity.com/2017/01/06/ftc-d-link-iot-privacy-and-security/.
159. *Id.*
160. *Id.*
161. *Id.*
162. *Id.*

violations, so it appears that the FTC can likely use Section 5 in the near term to ensure that companies do not violate consumers' data privacy.[163]

## V. CONCLUSION

The Internet of Things is a highly exciting phenomenon that has already contributed a substantial amount to technological innovation and making people's lives easier. However, along with the innumerable benefits come challenges in creating an appropriate regulatory regime to ensure that Internet of Things device manufacturers do not misuse consumers' data. The best approach combines the current FTC approach with some proposed regulation to ensure that data is not used inappropriately.

163. *Id.*