Notes

Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*

I. Introduction

In early 2015, consumers were shocked to discover that Lenovo, a computer company, was selling its computers with a preloaded software that would give hackers[1] a back door into consumers' private communications.[2] This software, called Superfish, tracked "consumers' online movements" without the consumers' full knowledge or consent.[3] This meant that when a consumer thought he was communicating with a secure server, he was actually open to attack because his "personal data and passwords" for "banking, social media, and email websites" could be stolen.[4] Although Superfish was already preloaded onto the computers, consumers had an opportunity to opt out of Superfish when they first started their machines.[5] This option was not exercised by at least 250,000 consumers: while Lenovo has not released information about how many computers were infected or how many consumers opted out of the software,[6] Microsoft created a tool that detected

---

* I am grateful to my husband, Travis, for his encouragement and patience, and to my parents for their support and suggestions. I would also like to thank Professor Sean H. Williams for his guidance and instruction. Finally, thanks to the editors of the *Texas Law Review*—particularly Alix Charles, Chase Cero, Casey Mathews, and Kate Marcom—for their hard work while editing this Note. All remaining errors are my own.

1. Throughout this Note, I use "hacker" in its more modern sense, that is, a person who illegally breaks into computer systems for various purposes, including the extraction of private data. *See* Douglas Thomas, *Hackers*, *in* BERKSHIRE ENCYCLOPEDIA OF HUMAN-COMPUTER INTERACTION 305 (William Sims Bainbridge ed., 2004) (defining "hackers" and giving a brief history of the term).

2. Brayden King, *Lenovo's Superfish Fallout: Can We Forgive and Forget?*, FORTUNE (Mar. 5, 2015, 7:30 AM), http://fortune.com/2015/03/05/lenovos-superfish-fallout-can-we-forgive-and-forget/ [http://perma.cc/4JSL-66HX].

3. Nicole Perlroth, *How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs*, N.Y. TIMES (Mar. 1, 2015), http://www.nytimes.com/2015/03/02/technology/how-superfishs-security-compromising-adware-came-to-inhabit-lenovos-pcs.html?_r=0 [http://perma.cc/ZR3H-ATX6].

4. *MSRT March: Superfish Cleanup*, MICROSOFT MALWARE PROTECTION CTR."Mar. 9, 2015), http://blogs.technet.com/b/mmpc/archive/2015/03/10/msrt-march-superfish-cleanup.aspx [http://perma.cc/9TWT-XMW3].

5. Perlroth, *supra* note 3.

6. *See* Seth Rosenblatt, *Lenovo's Superfish Security Snafu Blows Up in Its Face*, CNET (Feb. 20, 2015, 5:00 AM), http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/ [http://perma.cc/C52H-P2H9] (noting that Lenovo declined to say how many people own laptops infected with Superfish).

Superfish on 250,000 machines, even with the opt out.[7] Consumer reactions to Superfish were immediate, intense, and critical; one article described the scandal as "one of the most irresponsible mistakes an established tech company has ever made."[8]

The reaction to Superfish stands in stark contrast to consumers' everyday privacy-sacrificing behaviors. Whenever a user signs into two or more Google services (such as Gmail, Google Search, Google Maps, or YouTube), Google monitors and aggregates the user's every search and activity.[9] Amazon consolidates data about customers' purchases, product searches, online profiles, and location.[10] Target keeps tabs on its shoppers and can determine if a shopper is pregnant just from her purchase history.[11] Consumers also disregard their privacy rights on a more granular level through what is called the "Internet of Things" (IoT), or a system of devices that connect to each other via the Internet.[12] Surprisingly, consumers purchase these data devices with little knowledge of—and perhaps little regard for—whom the data can be disclosed to.[13] Such devices include a pocket breathalyzer whose results can be used against the consumer in court,[14] fitness-tracking devices that could be used to determine disabilities,[15] and a car plug-in that tracks a consumer's driving data, which then determines the appropriate insurance premium based on the user's driving habits.[16]

---

7. *See MSRT March: Superfish Cleanup*, *supra* note 4, fig.1 (summarizing the "[d]aily number of unique machines detecting . . . Superfish pre-installed on Lenovo machines").

8. David Auerbach, *You Had One Job, Lenovo*, SLATE (Feb. 20, 2015, 8:23 AM), http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html [http://perma.cc/4LUD-X9YK]; *see also* Memorandum of Law in Support of Motion for Transfer of Actions at 1–2, *In re* Lenovo Adware Litig., MDL No. 2624 (J.P.M.L. Feb. 25, 2015) (requesting the consolidation of the four lawsuits that had been filed against Lenovo within one week of Lenovo's confession to using Superfish).

9. PAUL BERNAL, INTERNET PRIVACY RIGHTS: RIGHTS TO PROTECT AUTONOMY 37 (Lionel Bently et al. eds., 2014). Because Google discloses the fact that it aggregates data in its privacy policy, the users are deemed to have expressly consented to having their activities monitored. *Id.* at 36–38; *see also Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy/ [http://perma.cc/BW5A-83KM].

10. *Amazon.com Privacy Notice*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=468496 [http://perma.cc/3CE5-WCHP].

11. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [http://perma.cc/JC4H-N5RN].

12. Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (Mar. 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand [http://perma.cc/KB3Y-S5ES].

13. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEXAS L. REV. 85, 140–43 (2014) (detailing how difficult it is to locate the privacy policies of various IoT manufacturers).

14. *Id.* at 87–88, 89–90.

15. *Id.* at 124.

16. *Id.* at 106.

These devices are increasingly prevalent and convenient, but have great potential for harm when consumers exchange their privacy rights for the convenience of using the devices. First, companies producing IoT products could go in the direction of Google or Target, using customers' private data to create targeted products or advertisements. While legal, this could still rightfully make consumers uncomfortable[17] because companies would possess almost unrestricted information about a consumer, such as how many miles he drives, if he donates to charities, and his health conditions.[18] Second, there are security risks whenever personal data are available via the Internet. Hackers have demonstrated a capability to compromise IoT devices and have broken into online video cameras and baby monitors.[19] Finally, companies can sell data to willing buyers. A prominent example is "data brokers," entities that aggregate consumer profiles that "may reveal where consumers live; how much they earn; and their race, health conditions, and interests."[20] The Federal Trade Commission (FTC) has already discovered that some mobile apps transmit information to third parties "about consumers' workouts, meals, or diets."[21] These data exposures are not limited to third-party data brokers; for example, Fitbit has expanded its market to include sales to employers.[22] While Fitbit insists that it does not

17. *See* Duhigg, *supra* note 11 ("We [at Target] are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy.").

18. *See* OFFICE OF OVERSIGHT & INVESTIGATIONS, S. COMM. ON COMMERCE, SCI. & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 13–15 (2013), http://educationnewyork.com/files/rockefeller_databroker.pdf [http://perma.cc/E6DC-HDZE] (discussing examples of the categories of information that are collected by data brokers).

19. *Home, Hacked Home*, ECONOMIST (July 12, 2014), http://www.economist.com/news/special-report/21606420-perils-connected-devices-home-hacked-home [http://perma.cc/8MKC-4QH9].

20. Julie Brill, *The Internet of Things: Building Trust and Maximizing Benefits Through Consumer Control*, 83 FORDHAM L. REV. 205, 210–11 (2014).

21. *Id.* at 212.

22. *See* Parmy Olson & Aaron Tilley, *The Quantified Other: Nest and Fitbit Chase a Lucrative Side Business*, FORBES (Apr. 17, 2014, 4:30 AM), http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/ [http://perma.cc/4QFN-JLNC] ("Fitbit is selling companies the tracking bracelets and analytics services to better manage their health care budgets, and its rival Jawbone may be preparing to do the same."); Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014, 1:26 PM), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/ [http://perma.cc/645Y-UCHJ] (detailing how "Fitbit's sales to employers are now one of the fastest growing parts of its business").

sell a consumer's individualized data to employers without the consumer's permission,[23] its privacy terms allow it to sell "de-identified data" without a consumer's consent.[24]

As the IoT continues to develop, legal scholarship has called for federal regulation to address the privacy concerns raised by these devices.[25] Because of these consumer-protection concerns, the FTC created the Office of Technology Research and Investigation (OTRI) in March of 2015.[26] The purpose of OTRI is "to help ensure that consumers enjoy the benefits of technological progress without being placed at risk of deceptive and unfair practices,"[27] and it will conduct research on "privacy, data security, . . . big data, and the Internet of Things."[28] While OTRI is a step toward the much argued-for regulation, its focus will remain on research—not regulation—for the foreseeable future.[29]

---

23. *See Let's Talk About Privacy, Publicly*, FITBIT, https://www.fitbit.com/privacy [http://perma.cc/JZH3-TXE6] ("We don't sell data that could identify you to anyone, anywhere, anytime. Ever. Period. That's all, folks. And we only share it when you tell us to, if we're required to by law or to protect Fitbit."). *But cf.* Hunter Walker, *Senator Warns Fitbit Is a 'Privacy Nightmare' and Could Be 'Tracking' Your Movements*, BUS. INSIDER (Aug. 10, 2014, 2:20 PM), http://www.businessinsider.com/senator-warns-fitbit-is-a-privacy-nightmare-2014-8 [http://perma.cc/46M3-2LM6] (discussing the "privacy nightmare" that would result if Fitbit and other similar companies sold consumer data to third parties).

24. *See Privacy Policy*, FITBIT, http://www.fitbit.com/legal/privacy-policy [http://perma.cc/GDN5-2ZGD] ("Fitbit may share or sell aggregated, de-identified data that does not identify you . . . ."); *infra* Part II.

25. *See, e.g.*, THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA: RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY 224–25 (2014) (explaining that a solution to the "future of intrusive technologies" is to "look to governments to set rules that protect our privacy"); Brill, *supra* note 20, at 213–14 (stating that industry adoption of the FTC's best practices "would go a long way toward providing strong and appropriate consumer privacy protections with respect to the Internet of Things"); Peppet, *supra* note 13, at 163–64 ("[R]eform is necessary to minimize consumer confusion and make Internet of Things privacy policies at least plausibly useful."); Eugene E. Hutchinson, Note, *Keeping Your Personal Information Personal: Trouble for the Modern Consumer*, 43 HOFSTRA L. REV. 1151, 1177–78 (2015) (proposing that Congress pass legislation to give consumers a private right of action, change the default to opt-in, and build a national data broker registry).

26. Jessica Rich, *BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection*, FED. TRADE COMMISSION (Mar. 23, 2015, 2:01 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next [https://perma.cc/CX2L-APSY].

27. *Id.*

28. Ashkan Soltani, *Booting Up a New Research Office at the FTC*, FED. TRADE COMMISSION (Mar. 23, 2015, 11:00 AM), https://www.ftc.gov/news-events/blogs/techftc/2015/03/booting-new-research-office-ftc [https://perma.cc/LZ5T-MFJN].

29. *See id.* (announcing that the OTRI will be "an instrumental source for research and information on technology's impact on consumers").

Although legal scholarship has explained the implications of "privacy trading," as I shall call such behaviors in this Note,[30] very few have questioned *why* consumers are willing to trade their privacy for the conveniences offered by the IoT. One scholar, Scott Peppet, has suggested that the reason for the trade may be consumers' ignorance about what companies do with their data.[31] Peppet argues that IoT disclosures and privacy terms are difficult to find and, when located, are ambiguous.[32] But ignorance about how one's data could be used is likely not the full explanation as to why consumers trade away privacy. As Julie Brill—a Commissioner of the FTC—has explained, privacy concerns are unlikely to "keep consumers away from the Internet of Things."[33] This Note attempts to fill the gap in the literature by discussing consumer-privacy trading through the lens of behavioral law and economics (BLE). It aims to offer two explanations as to why consumers may behave in an irrational manner and to apply these explanations to three of the regulatory solutions that have been proposed by legal scholars.

Part II of this Note provides a brief overview of the IoT, defining what types of devices are included in the consumer sector and discussing current regulations. It also explains that many consumers may be unaware of what a "privacy trade" actually entails. Part III presents two theories of BLE and analyzes how these theories can provide insight into privacy trading. The BLE analysis is limited in scope to only those consumers who are aware that they are trading their privacy. Part IV presents three of the currently proposed solutions to the consumer-protection problem and explains how these solutions would address the BLE biases discussed in Part III. This Note concludes in Part V.

II. The Internet of Things Overview

The IoT (sometimes called the Internet of Everything[34]) is a term used to describe a series of devices (or "things") that are connected to each other by a network.[35] These devices—which include home electronics, medical devices, home appliances, automobiles, and more—use the network to communicate, much in the same way that people use the Internet to com-

30. I am not the first to refer to purchasing IoT devices as privacy trading. In one NPR interview, Rick Smolan, the producer of a documentary about the IoT, questioned why we trade "something that sounds so completely horrible . . . for the incredible convenience" of using devices. *PBS Special Probes Benefits and Concerns of Using Big Data*, HERE & NOW (Feb. 24, 2016), http://hereandnow.wbur.org/2016/02/24/human-face-of-big-data-pbs [https://perma.cc/3973-97Q3].

31. *See* Peppet, *supra* note 13, at 139–43 (discussing both the difficulty of locating an IoT manufacturer's privacy policy and the ambiguous language in these policies).

32. *Id.*

33. Brill, *supra* note 20, at 212.

34. MICHAEL MILLER, THE INTERNET OF THINGS: HOW SMART TVS, SMART CARS, SMART HOMES, AND SMART CITIES ARE CHANGING THE WORLD 1 (Greg Wiegand et al. eds., 2015).

35. *Id.* at 6–7.

municate.[36] As the devices communicate, they send data across this network and use the data to execute their specific functions.[37] Because both wired and wireless devices can connect to the network, there is almost unlimited potential for development in this sphere.[38] Indeed, market research estimates that 220 billion devices will be in use by 2020.[39]

New devices emerge at a pace that makes it impossible to track and codify all sensors into one database. One European Union-based survey suggested that IoT devices fall into as many as fourteen different categories.[40] Of these categories, four have been identified as the most important: healthcare, transportation, smart environment (e.g., home and workplace monitoring), and the personal and social domain.[41] Each category covers a broad range of devices. Healthcare devices include devices that track blood pressure, blood glucose, and weight; electronic medical information systems that can diagnose a patient's illness; and wearable devices that can track steps walked and calories burned.[42] Transportation devices include automobile sensors, which can track information about a car's speed and driver data, such as braking and speeding habits, and can be used in a feedback loop to insurance agencies to determine accurate pricing.[43] The transportation category also includes self-moving vehicles—self-driving cars and self-flying drones are two examples.[44] Home-monitoring devices include thermostats, ovens, and lighting systems that can be adjusted remotely,[45] and workplace moni-

36. *Id.* at 7–8.

37. *Id.* at 8.

38. *See id.* ("[A] 'thing' in the IoT can be anything large enough to contain a wireless transmitter . . . and unique enough to be assigned its own Internet Protocol (IP) address. This could include something as small as a paperclip or as large as a house.").

39. Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME (Jan. 13, 2014), http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/ [http://perma.cc/7YCH-GY79].

40. Pasi Pussinen & Hanna Okkonen, *Scenarios for IoT*, *in* INTERNET-OF-THINGS MARKET, VALUE NETWORKS, AND BUSINESS MODELS: STATE OF THE ART REPORT 63, 64 (Oleksiy Mazhelis et al. eds., 2013).

41. *See* Luigi Atzori et al., *The Internet of Things: A Survey*, 54 COMPUTER NETWORKS 2787, 2793–96 (2010) (listing and describing four domains where "applications would likely improve the quality of our lives").

42. *See* Mersini Paschou et al., *Health Internet of Things: Metrics and Methods for Efficient Data Transfer*, 34 SIMULATION MODELING PRAC. & THEORY 186, 187–89 (2013) (describing how IoT devices can improve healthcare).

43. *See* FAWZI BEHMANN & KWOK WU, COLLABORATIVE INTERNET OF THINGS (C-IOT): FOR FUTURE SMART CONNECTED LIFE AND BUSINESS 185–86 (2015) (stating that insurance companies "allow drivers to select an option where their driving habits can be monitored remotely and the insurance companies can provide a discount to drivers with good driving habits").

44. MILLER, *supra* note 34, at 8; *see also* BEHMANN & WU, *supra* note 43, at 85–86 (stating that many cars are equipped with systems "such as active braking and active speed control that detect your car is approaching too close to another object, then decelerate the car by apply[ing] braking, lane change warning that detects your car has drifted away from your lane, blindspot detection detects objects in your blindspot, and so on").

45. Brill, *supra* note 20, at 208.

toring devices include hand-washing monitors, sensors that can track when employees are at their desks, devices that can monitor employees' stress levels, and computer programs that track keystrokes and idle time.[46] Finally, smartphones can connect to everything from televisions and computers to sensors that can track a user's heart rate or examine a user's inner ear.[47]

As the IoT grows larger, so do concerns about consumer privacy. Because the datasets produced by each device are unique to the user, any release of this information poses the danger of associating it with the individual user.[48] One way that companies attempt to have the best of both worlds—that is, mitigate privacy concerns while still selling data—is by "de-identifying" the data.[49] De-identification is a "process to prevent a personal identifier from being connected with information."[50] This process allows some bits of data to be compiled while excluding the information that identifies a particular dataset's owner, such as the individual's name.[51] For example, GPS devices can track the aggregate speed on a road and release real-time traffic updates without compiling the name of each driver currently on that road.[52] But de-identification is not a perfect solution because in most of the de-identified datasets, the information can be *re*-identified.[53] This means that even if data were released "anonymously," it could be reassociated with an individual user, thwarting the de-identification

46. Charles E. Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. LAW. 857, 858–59 (2002); *Forget to Wash? Devices Track Hand Washing Adherence in Hospitals*, CBS NEWS (June 28, 2013, 2:21 PM), http://www.cbsnews.com/news/forget-to-wash-devices-track-hand-washing-adherence-in-hospitals/ [https://perma.cc/KY4H-M7YK]; Bernard Marr, *The Quantified Workplace: Big Data or Big Brother?*, FORBES (May 11, 2015, 10:38 AM), http://www.forbes.com/sites/bernardmarr/2015/05/11/the-nanny-state-meets-the-quantified-workplace/#7f2198d872e5 [https://perma.cc/H8WE-ELDL]; Rachel Emma Silverman, *Tracking Sensors Invade the Workplace: Devices on Workers, Furniture Offer Clues for Boosting Productivity*, WALL STREET J. (Mar. 7, 2013, 11:42 AM), http://www.wsj.com/articles/SB10001424127887324034804578344303429080678 [http://perma.cc/PCX9-QLVN].

47. MILLER, *supra* note 34, at 8; Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, 1 J. SENSOR & ACTUATOR NETWORKS 217, 226 (2012).

48. *See* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 65 (2012) ("Information regarding individuals' health, location, electricity use, and online activity . . . rais[es] concerns about profiling, discrimination, exclusion, and loss of control.").

49. *Id.*

50. Yianni Lagos, *Taking the Personal Out of Data: Making Sense of De-Identification*, 48 IND. L. REV. 187, 187 (2014).

51. *Id.*

52. *Id.*

53. Latanya Sweeney, K-*Anonymity: A Model for Protecting Privacy*, 10 INT'L J. ON UNCERTAINTY, FUZZINESS & KNOWLEDGE-BASED SYSTEMS 557, 558–59 (2002); *see also* Lagos, *supra* note 50, at 192 (discussing how "indirect identifiers" in a dataset may be used to "reconnect personal information with a person's identity").

process.[54] Re-identification could reveal private Internet searches, health and hospitalization history, movie-watching history, and more.[55] While some companies include a clause in their sales contracts that prohibit re-identification,[56] the data that could be used to re-identify the information are still attached, meaning that the third-party buyer could breach the contract and re-identify the data; the contract also does not prevent a hacker from accessing the datasets and re-identifying them. Although the actual likelihood of re-identification is still contested,[57] the potential for danger is high: once a user's private information is released, it cannot be recalled.

Even without the de-identification and re-identification process, data could potentially be used to adversely affect the user.[58] For example, the Breathometer is a smart breathalyzer that interacts with a user's smartphone.[59] The data produced by the Breathometer blood-alcohol tests "are being stored indefinitely in the cloud, cannot be deleted by the user, [and] may be disclosed in a court proceeding if necessary," meaning that any blood-alcohol test a user took could later be used against him.[60] Another example is the Fitbit, a device that records physical activity metrics.[61] Fitbit has an opt-in program that sells users' data to employers,[62] who offer incentives to participating employees.[63] But these data carry the inherent risk of

54. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716–22 (2010); Sweeney, *supra* note 53, at 558–59.

55. Ohm, *supra* note 54, at 1717–22; Sweeney, *supra* note 53, at 558–59; *see also* Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L ACAD. SCI. 10,975, 10,978–80 (2009) (explaining how it is possible to use data that could be obtained from re-identification, such as an individual's place and date of birth, to predict a person's social security number).

56. *See, e.g.*, *Privacy Policy*, *supra* note 24 ("[W]e contractually prohibit recipients of the data from re-identifying it back to you.").

57. *See* Sébastien Gambs et al., *De-Anonymization Attack on Geolocated Data*, 80 J. COMPUTER & SYSTEMS SCI. 1597, 1611 (2014) (contrasting the results from different studies that have analyzed re-identification and showing results that range from 42% to 90% success at re-identifying data). *Compare* Arvind Narayana & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information,"* COMM. ACM, June 2010, at 24, 26 ("[A]ny attribute can be identifying in combination with others." (emphasis omitted)), *with* Daniel C. Barth-Jones, The "Re-Identification" of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now 3–5 (June 18, 2012) (unpublished manuscript), http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2076397 [http://perma.cc/NL65-F5XG] ("[T]he precise conditions required for definitive re-identification can be quite daunting.").

58. *See* Peppet, *supra* note 13, at 89 ("And are consumers aware of the legal implications that such data create—such as the possible use of such data by an adversary in court, an insurance company when denying a claim, an employer determining whether to hire, or a bank extending credit?").

59. *Id.* at 87–88.

60. *Id.* at 90.

61. *Id.* at 88.

62. Olson & Tilley, *supra* note 22.

63. Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1168 (2011).

"reveal[ing] physical disabilities, illnesses, or conditions like pregnancy,"[64] and some employers have already fired employees "who engage in behavior likely to raise the employer's health insurance costs."[65] While the firings mentioned here were related to a smoking ban,[66] it is but a small step for employers to fire employees for health defects unveiled by the employees' data. As a final example, car insurance companies allow users to travel with devices that track the users' driving speed and location.[67] The companies market the device as an opportunity to save on insurance premiums,[68] but because the devices also record when participants are aggressive drivers, an insurance company may end up raising a participant's insurance rate.[69]

These three examples shed light onto how IoT devices can be manipulated to reveal the privacy of the user. Despite the potential dangers of privacy trading, users continue to buy IoT products, and more products enter the market at an ever-increasing rate.[70] Because there currently exists no

64. John G. Browning, *Wearable Tech: The Latest Gadgets Come Wrapped in Legal Issues, From Workplace Privacy to State Wiretapping Laws*, 78 TEX. B.J. 12, 13 (2015).

65. Peppet, *supra* note 63, at 1169; *see also* Jeremy W. Peters, *Company's Smoking Ban Means Off-Hours, Too*, N.Y. TIMES (Feb. 8, 2005), http://www.nytimes.com/2005/02/08/business/08smoking.html [http://perma.cc/BHT2-BA9P] (discussing a Michigan employer that plans to fire employees who fail a random cigarette-smoking test).

66. Peters, *supra* note 65.

67. Teresa Meek, *In-Car Sensors Put Insurers in the Driver's Seat*, FORBES (June 27, 2014, 12:34 PM), http://www.forbes.com/sites/ptc/2014/06/27/in-car-sensors-put-insurers-in-the-drivers-seat/ [http://perma.cc/5T34-XJP7]. Insurers with discount programs include USAA, State Farm, Allstate, Nationwide, and Progressive. *Discount for Driving Research*, USAA, https://www.usaa.com/inet/pages/auto_insurance_driving_research_discount_main?akredirect=true [http://perma.cc/X5XH-WVY5]; *Drive Safe & Save with In-Drive*, STATE FARM, https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive [https://perma.cc/W3NL-M2QK]; *Get Rewarded with Drivewise*, ALLSTATE, https://www.allstate.com/drive-wise.aspx [https://perma.cc/PNX3-RYEC]; *Play It Safe and Get Rewards with SmartRide*, NATIONWIDE, http://www.nationwide.com/smartride.jsp [http://perma.cc/AXJ3-ZAZT]; *Snapshot Common Questions*, PROGRESSIVE, https://www.progressive.com/auto/snapshot-common-questions [https://perma.cc/37Y5-BJ76].

68. *See* Ron Lieber, *Lower Your Car Insurance Bill, at the Price of Some Privacy*, N.Y. TIMES (Aug. 15, 2014) http://www.nytimes.com/2014/08/16/your-money/auto-insurance/tracking-gadgets-could-lower-your-car-insurance-at-the-price-of-some-privacy.html [http://perma.cc/Z5RZ-73GT] (characterizing the privacy trade as one in which privacy is traded "in exchange for an annual discount").

69. *E.g.*, *Snapshot: Terms & Conditions*, PROGRESSIVE, https://www.progressive.com/auto/snapshot-terms-conditions/ [http://perma.cc/TFG8-2VVV] ("For customers who enroll and plug in the device, most will save money at renewal based on their good driving. Some customers who drive more aggressively will receive a surcharge at renewal.").

70. *See* Christin S. McMeley, *Protecting Consumer Privacy and Information in the Age of the Internet of Things*, 29 ANTITRUST 71, 71–72 (2014) (explaining how the growth trajectory of IoT purchases shows "no signs of slowing, with estimates projecting the number of [IoT] devices ranging from 40.9 to 212 billion by 2020"); Larry Dignan, *Internet of Things: $8.9 Trillion Market in 2020, 212 Billion Connected Things*, ZDNET (Oct. 3, 2013, 5:59 AM), http://www.zdnet.com/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things-7000021516/ [http://perma.cc/25RY-4MS9] (reporting that the International Data Corporation estimates that the "installed base of things connected will be 212 billion by the end of 2020").

broad-sweeping regulation about the Internet of Things,[71] consumers must rely on the protections offered by older, untailored federal regulations or by individualized state regulations. Some states have already begun passing legislation about the IoT, but each state's laws vary and may not cover all data-privacy concerns.[72] While the U.S. Department of Health and Human Services requires that anyone with personal health information de-identify this data,[73] de-identification is merely recommended—not required—in other spheres.[74]

Furthermore, there does not currently exist federal regulation requiring manufacturers to notify consumers about when or what types of data are collected when the collected information is used for a purpose consistent with the transaction.[75] The FTC has explicitly announced that it will not recommend requiring manufacturers to notify consumers about data collection in such instances, reasoning that "these data uses are generally consistent with consumers' reasonable expectations."[76] Both houses of Congress have similarly rejected the idea of legislation; the predominant concern seems to be ensuring that the IoT has room to develop. The Senate held a hearing about the IoT in February of 2015, but ultimately decided against regulation because "consumers and entrepreneurs [should] decide where [the Internet of Things] goes."[77] In April of 2015, the House of Representatives saw a resolution that "the United States should develop a national strategy to

71. *See* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at vii (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/N5Y4-A7KZ] [hereinafter PRIVACY & SECURITY REPORT] (summarizing a 2013 workshop at which participants "discussed whether legislation over the IoT is appropriate").

72. *See* Peppet, *supra* note 13, at 152–54 (describing state statutes limiting the use of data by automobile event data recorders and noting that "[m]ost of these state statutes currently would not cover the data generated by [IoT sensor devices]").

73. 45 C.F.R. § 164.514(b) (2015).

74. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 20–22 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/DX2Y-8ZML] [hereinafter PRIVACY REPORT] (clarifying the FTC's recommendations for businesses operating in the IoT sphere).

75. *See* PRIVACY & SECURITY REPORT, *supra* note 71, at v ("[T]he [Federal Trade] Commission 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.").

76. *Id.*

77. Howard W. Waltzman & Lei Shen, *The Internet of Things*, INTELL. PROP. & TECH. L.J., July 2015, at 19, 20 (second alteration in original); *see also The Connected World: Examining the Internet of Things*, U.S. SENATE COMMITTEE ON COM., SCI., & TRANSP. (Feb. 11, 2015), http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=d3e33bde-30fd-4899-b30d-906b47e117ca [http://perma.cc/3B7R-ZVJW] (providing a video recording of the Senate hearing).

encourage the development of the [IoT]"; however, this resolution did not include any reference to regulating the IoT or hint toward any future consumer-protection laws.[78]

With no federal regulations, consumers will likely be bound to the manufacturer's terms through contract law.[79] Many contracts will be in the form of a "clickwrap" agreement, defined as an agreement in which the consumer clicks "I agree" to the manufacturer's standard contract terms.[80] Courts that have considered the issue have generally found clickwrap agreements to be enforceable, with the caveat that the user must know that he is consenting to terms—even if the user does not know what those terms actually are.[81] This means that any rights a user has under a standard IoT contract are merely those afforded to him by the manufacturer or seller, and the only recourse to a user who prefers not to share his data is to refrain from purchasing an IoT device.

Consumer protections for those who do purchase IoT devices vary from state to state.[82] California and Delaware, for example, both require that operators of Internet websites or services conspicuously post their privacy policies online.[83] New York requires that state agencies that collect personal information post a privacy policy online, but remains silent about requirements for private actors.[84] Nebraska does not require that operators of websites post their privacy policies, but does prohibit false or misleading statements in any privacy policy.[85] Other states have no protection at all.[86]

Such lack of protection may prove problematic in the IoT sphere because even if a consumer is aware that IoT devices come with some terms attached, these terms are ambiguous. Privacy policies usually will "provide

78. H.R. Res. 195, 114th Cong. (2015).

79. *See* KENT D. STUCKEY, INTERNET AND ONLINE LAW § 1.01[1], at 1–5 (1996) (explaining that the offeror is "the master of the offer").

80. Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 459 (2006).

81. Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483, 500 (2015); Lemley, *supra* note 80, at 459. For a general overview of cases enforcing clickwrap agreements, see Nathan J. Davis, Note, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577 (2007).

82. To date, there have been no uniform attempts to model how states should regulate the sale of devices that interact through the Internet. While the National Conference of Commissioners on Uniform State Laws has promulgated model rules to govern computer information transactions, these rules would not govern the sale of tangible goods, such as IoT devices. *See generally* Pratik A. Shah, Note, *The Uniform Computer Information Transactions Act*, 15 BERKELEY TECH. L.J. 85 (2000) (giving an overview of the model statute).

83. CAL. BUS. & PROF. CODE § 22575(a) (West 2015); DEL. CODE ANN. tit. 6, § 1205C(a) (West 2015).

84. N.Y. STATE TECH. LAW § 203.2 (McKinney 2002).

85. NEB. REV. STAT. § 87-302(14) (2008).

86. *See Digital Privacy and Security: Overview of Resources*, NAT'L CONF. ST. LEGISLATURES (Dec. 29, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/telecom-it-privacy-security.aspx [http://perma.cc/4WGL-LFHM] (discussing the few states with "greater privacy protections than those provided for in the U.S. Constitution").

little real guidance" to the consumer because they do not provide clear disclosure about how the user's data can be "shared with or sold to third parties."[87] When consumers receive no notice about what type of data are being collected or to whom these data are being sold, it may be difficult for consumers to form *any* expectations—much less reasonable ones—about how the data will be used. A consumer might neither comprehend the full extent of the data collected nor understand why a third party would want to purchase the data. In the ever-growing world of the Internet of Things, the lack of both notification and regulation may be a dangerous combination for consumers.

III. Behavioral Law and Economics in the Internet of Things

This Part will explore why people purchase IoT devices despite the difficult privacy issues described in Part II. To do so, it will examine consumers' behavior through the lens of behavioral law and economics. It offers two BLE theories as to why consumers engage in privacy trades. While other theories (such as the bandwagon effect[88]) may help to explain why consumers trade away their privacy, this Note limits its scope to what I consider to be the two behavioral biases that are most relevant to the proposed regulatory solutions.

As discussed previously in Part II, many consumers may be unaware of the full extent of the privacy that they are trading and to whom their privacy is being sold. Because this problem dissipates once adequate notice is given, this Part analyzes the biases that would remain even if people were adequately informed. This Part similarly does not apply to consumers who are aware of the privacy loss but continue to purchase IoT devices after conducting a cost-benefit analysis and concluding that the convenience of the device is worth more than their privacy. Part III's explanation is therefore limited to consumers who know they are engaging in privacy trades and prefer not to lose their privacy, but continue to purchase IoT devices despite this preference.

The biases explored here may also apply to individuals running the companies that manufacture IoT devices. As a result of their biases, they may underestimate the risks their devices pose to consumers. This Note does not mean to suggest that companies are acting with a nefarious intent, and this hypothesis may be worthy of further explanation. However, this Note is limited to analyzing the risk to consumers, and does not engage in seller-side analysis.

---

87. Peppet, *supra* note 13, at 143.

88. The bandwagon effect increases demand for a consumer good. Consumers tend to adjust how much they desire an item to match the desire of their peers; when some consumers demand a certain good, other consumers begin to want to purchase that good as well. *See* H. Liebenstein, *Bandwagon, Snob, and Veblen Effects in the Theory of Consumers' Demand*, 64 Q.J. ECON. 183, 195–96 (1950) ("Due to the bandwagon effect, however, an additional number of consumers are induced to enter the market or to increase their demands.").

A. Unrealistic Optimism

One reason why people may engage in privacy trades is because they misestimate how likely it is that the trade will have a negative impact on them. Behavioral economics posits that people hold overinflated views of themselves and are therefore not very skilled at assessing the likelihood that they will encounter a negative event.[89] This bias, called "unrealistic optimism" or overoptimism, means that the views a person holds about himself tend to be "too good to be true."[90] The average person will believe that he is better than average—for instance, that he is a better driver than his peers[91] or that he is less likely than the average person to experience a negative health event.[92] This is, of course, a mathematical paradox: more than 50% of people cannot be better off than average.[93]

Illustrative of this bias is one study that asked a group of 296 people about their likelihood of experiencing various negative health events.[94] For each health problem (e.g., drug addiction, asthma, pneumonia, poison-ivy rash, serious auto injury, or heart attack), the participants were asked: "Compared to other men/women my age, my chances of getting [problem] in the future are: much below average, below average, a little below average, average for men/women my age, a little above average, above average, much above average."[95] The "average" here, or the halfway point of 296, falls at 148; this means that about 147 people will be *more* likely than the average person to actually experience the event, and about 147 people will be *less* likely than the average person to actually experience the event. But for almost every health problem, over 147 people estimated that they are better than average, meaning that they were less likely to experience the health

89. *See* Neil D. Weinstein, *Unrealistic Optimism About Future Life Events*, 39 J. PERSONALITY & SOC. PSYCHOL. 806, 806 (1980) ("[P]eople tend to think they are invulnerable.").

90. David Dunning et al., *Flawed Self-Assessment: Implications for Health, Education, and the Workplace*, 5 PSYCHOL. SCI. PUB. INT. 69, 72 (2004).

91. *See* Michael L. Matthews & Andrew R. Moran, *Age Differences in Male Drivers' Perception of Accident Risk: The Role of Perceived Driving Ability*, 18 ACCIDENT ANALYSIS & PREVENTION 299, 309–10 (1986) ("Young drivers also viewed the chances of an accident as being much higher for other young drivers than for themselves."); D. R. Rutter et al., *Perceptions of Risk in Motorcyclists: Unrealistic Optimism, Relative Realism and Predictions of Behavior*, 89 BRIT. J. PSYCHOL. 681, 686–87 (1998) (finding that, statistically, respondents saw themselves as less likely than other motorcyclists to have an accident).

92. Neil D. Weinstein, *Unrealistic Optimism About Susceptibility to Health Problems: Conclusions from a Community-Wide Sample*, 10 J. BEHAV. MED. 481, 486 tbl.1, 488 (1987). For a discussion of other biases that may impact health decisions, see generally Marysia Laskowski, Note, *Nudging Towards Vaccination: A Behavioral Law and Economics Approach to Childhood Immunization Policy*, 94 TEXAS L. REV. 601 (2016).

93. *See* Christine Jolls, *Behavioral Economics Analysis of Redistributive Legal Rules*, 51 VAND. L. REV. 1653, 1659 (1998) ("[I]f everyone were below (or above) 'average,' then the average would be lower (or higher).").

94. Weinstein, *supra* note 92, at 485, 488.

95. *Id.* at 485 (alteration in original).

problem than the average person.[96] Many studies have found the same effect: people believe that they are above average.[97] This type of overoptimism, also called the "above average effect,"[98] is a statistical impossibility.

An IoT user may be subject to the above average effect because he may believe that he is less likely than the average person to experience harm from data loss. While unrealistic optimism has not been studied in the IoT sphere specifically, it has been proven to exist in online interactions.[99] Even when Internet users are concerned about their online privacy and security, they still engage in risky online behaviors.[100] Moreover, the more Internet experience a person has, the lower his perceived risk toward risky online behaviors.[101] This bias could be extended to people who trade their privacy by buying IoT devices. Even if a consumer is concerned about his privacy, he may still engage in the risky behavior of purchasing an IoT device. His unrealistic optimism will work against him—he will think that he is less likely to experience harm from privacy loss than the average person, and if he has a substantial amount of Internet experience (or owns several IoT devices), he may be more susceptible to the bias.

Furthermore, an IoT user is likely to believe not only that he is better off than the average person, but also that he is better off than actual statistics suggest. People tend to underestimate not just how they will fare against the average, but also how they will fare against actual probabilities.[102] Put another way, when asked about the probability of having a car accident, a person will experience both the above average effect and overall unrealistic optimism.[103] The above average effect is shown when a person believes that he is less likely to have an auto accident than the average person, while overall overoptimism is demonstrated when a person believes that his likeli-

96. *See id.* at 486 tbl.1 (averaging the survey responses and finding that most answers had a mean below zero).

97. *See generally* James A. Shepperd et al., *Taking Stock of Unrealistic Optimism*, 8 PERSP. ON PSYCHOL. SCI. 395 (2013) (listing and describing various studies that have demonstrated unrealistic optimism).

98. Christine Jolls & Cass R. Sunstein, *Debiasing Through Law*, 35 J. LEGAL STUD. 199, 204 (2006).

99. Jamonn Campbell et al., *Unrealistic Optimism in Internet Events*, 23 COMPUTERS HUM. BEHAV. 1273, 1278 tbl.2, 1278–80 (2007); *see also* Anthony D. Miyazaki & Ana Fernandez, *Consumer Perceptions of Privacy and Security Risks for Online Shopping*, 35 J. CONSUMER AFF. 27, 38 (2001) (finding "that higher Internet experience and the use of other remote purchasing methods are related to lower levels of perceived risk toward online shopping, which in turn results in higher online purchase rates").

100. *See* Miyazaki & Fernandez, *supra* note 99, at 38 (stating that concerns about "privacy issues and potential fraudulent behavior by online retailers . . . were not predictive of online purchase rates").

101. *Id.*

102. Jolls, *supra* note 93, at 1658–60; *see also* Jolls & Sunstein, *supra* note 98, at 204–05 (discussing examples of when people misestimate the actual probabilities of a risk, even when the risk is within their field of expertise).

103. Jolls, *supra* note 93, at 1660–61.

hood of an accident is lower than the actual probability.[104] The overall unrealistic optimism is not limited to self; an overly optimistic person will assume that the probability of an auto accident in the population as a whole is less than the actual probability.[105] This bias may be shown in an IoT user if he assumes that any harm from an IoT device is less likely to occur than the true probability. As a result, he may be more likely to make the privacy trade by purchasing an IoT device.

The above average effect is not absolute; it can be influenced by how a person thinks about the event. For example, overoptimism is more likely to result when an event is perceived as controllable.[106] A person will consider "personal actions, plans, or attributes" that might allow him to mitigate the likelihood of a negative event, and when he views the event as more controllable, he is more likely to misestimate how likely he is to experience it.[107] The less controllable the event, the less likely a person is to be overly optimistic.[108] If an IoT user believes that he can control the input into his device (and therefore control the risk of harm), he may be more likely to misestimate how likely it is that the data would actually harm him.

A good example of this in the IoT sphere is car insurance. Progressive, an insurance company, offers a usage-based insurance program in which a driver plugs a device into his car.[109] The device, called Snapshot, records information such as the time of day a driver is in the car, if and when the driver brakes hard, how and when the driver accelerates, and the amount the car is driven; it then calculates an insurance rate based on the driver's habits.[110] While this program traditionally has offered only discounts to participants, Progressive has announced that it will start increasing rates for bad drivers.[111] This change may potentially harm an IoT user who believes he can control when he drives, how often he drives, and his driving behaviors. Even if, however, an IoT user believes he has little control over the data or how it is used, he will still be overly optimistic, just less so.[112] While drivers

104. *Id.* at 1660.

105. *Id.*

106. Weinstein, *supra* note 89, at 814.

107. *Id.* at 818–19.

108. *Id.* at 814; *see also* Marie Helweg-Larsen & James A. Shepperd, *Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature*, 5 PERSONALITY & SOC. PSYCHOL. REV. 74, 86 (2001) (summarizing multiple studies on controllability and the optimistic bias and finding "that controllability functions as a personal risk moderator" because people believe that they are more likely than others to take precautions).

109. *Snapshot Common Questions*, *supra* note 67.

110. *Frequently Asked Questions About Snapshot*, PROGRESSIVE, http://www.progressiveagent.com/auto/snapshot-faqs.aspx [http://perma.cc/YPQ9-JNU4].

111. Robert Passikoff, *Progressive Adds 'Bad Driver' Surveillance to Snapshot Telematics*, FORBES (Mar. 31, 2015, 9:34 PM), http://www.forbes.com/sites/robertpassikoff/2015/03/31/progressive-adds-bad-driver-surveillance-to-snapshot-telematics/ [http://perma.cc/L9P3-LBT2].

112. *Cf.* David M. DeJoy, *The Optimism Bias and Traffic Accident Risk Perception*, 21 ACCIDENT ANALYSIS & PREVENTION 333, 338 (1989) (finding that college students "were quite

are less likely to be overly optimistic about events they feel they cannot control, they still tend to underestimate how likely they are to experience the event compared to the average person.[113] This point can be extrapolated to any IoT device—even if a user feels as though he is in control, he will still underestimate his risk.

Another factor that may influence the estimation of a negative event's likelihood is how salient the event is.[114] The more "available" the event is—that is, the more readily it comes to a person's mind—the less likely it is that the person will underestimate the likelihood of the event.[115] This is also called the "availability heuristic."[116] Examples of highly salient events include nuclear-power-plant accidents and toxic-waste contamination: these events tend to receive media attention and are intrinsically memorable, so people are more likely to overestimate the likelihood of them happening.[117] Because there is not currently widespread media coverage on the dangers of the IoT—at least, not as compared to a nuclear-power accident—the harm from an IoT device may be less "available" to a user. Therefore, there is not a substantial mitigating effect on his unrealistic optimism, meaning that at least some IoT privacy trades are due to consumers underestimating their risk of harm.

B. Hyperbolic Discounting

A second reason people may trade away their privacy is because their preferences change over time. Classical economics assumes both that consumers discount future utilities and that they do so at a constant rate.[118] In other words, economic models predict that if a consumer prefers $10 today over $12 tomorrow, he would prefer $10 in one year over $12 in one year plus one day.[119] This assumption has proven false.[120] While consumers do discount future utilities, they do not do so at a constant rate.[121] The consumer

---

optimistic in evaluating their risk of being involved in a wide variety of accidents, and were particularly optimistic for accidents that they perceived as being controllable").

113. *Id.*

114. Jolls, *supra* note 93, at 1662.

115. *Id.* at 1662–63.

116. Amos Tversky & Daniel Kahneman, *Availability: A Heuristic for Judging Frequency and Probability*, 5 COGNITIVE PSYCHOL. 207, 208 (1973).

117. Jolls, *supra* note 93, at 1662–63.

118. Paul A. Samuelson, *A Note on Measurement of Utility*, 4 REV. ECON. STUD. 155, 156 (1937).

119. *See* Jess Benhabib et al., *Present-Bias, Quasi-Hyperbolic Discounting, and Fixed Costs*, 69 GAMES & ECON. BEHAV. 205, 205 (2010) (stating that a person who prefers $10 today over $12 tomorrow but prefers $12 in a year plus a day over $10 in a year is not acting consistent with exponential discounting).

120. *Id.* at 205–06.

121. E. S. Phelps & R. A. Pollak, *On Second-Best National Saving and Game-Equilibrium Growth*, 35 REV. ECON. STUD. 185, 185, 197–98 (1968).

who prefers $10 today over $12 tomorrow *does not* prefer $10 in one year over $12 in one year plus one day—he prefers the $12 in one year plus one day.[122] In layman's terms, a consumer is impatient in the present and patient when thinking about the future; he discounts the future utilities. But this patience is short-lived: when the year is up, the consumer's preferences change; he would pick the $10 "today" over the $12 "tomorrow."[123] This shift is called hyperbolic or quasi-hyperbolic discounting.[124] Discounting occurs because a consumer will heavily discount events that happen in the near future, but will assign only a small additional discount to events that will happen in the more distant future.[125] Consumers are more impatient while thinking about the near future than they are while thinking about the far future.

While the above example describes how hyperbolic discounting may apply to delayed rewards, discounting can also be used to explain why people engage in risky behaviors with delayed consequences.[126] Notably, Oren Bar-Gill has written about discounting in the credit-card area.[127] A credit-card user purchases an item on credit and pays for the purchase later; thus, credit cards involve delayed consequences.[128] As Bar-Gill explains, when a hyperbolic discounter considers a future credit-card purchase, he will apply roughly the same discount to the future cost.[129] Because the cost of credit-card purchases is so high, his preference is not to make the purchase.[130] Nevertheless, as time passes and the future purchase becomes "today's" purchase, his preferences reverse and he will prefer to purchase now and pay later.[131] This effect can also be seen in health preferences. Obese persons experience this preference reversal while eating: despite a preference for

122. Benhabib et al., *supra* note 119, at 205.

123. *See id.* ("[R]eversals of preferences are . . . consistent with a rate of time preference which declines with time.").

124. Oren Bar-Gill, *Seduction by Plastic*, 98 NW. U. L. REV. 1373, 1396 (2004); Benhabib et al., *supra* note 119, at 205.

125. Bar-Gill, *supra* note 124, at 1396; *see also* Shane Frederick et al., *Time Discounting and Time Preference: A Critical Review*, 40 J. ECON. LITERATURE 351, 360 (2002) (detailing how "the implicit discount rate over longer time horizons is lower than the implicit discount rate over shorter time horizons").

126. *See* David Laibson et al., *A Debt Puzzle*, *in* KNOWLEDGE, INFORMATION, AND EXPECTATIONS IN MODERN MACROECONOMICS 228, 230 (Philippe Aghion et al. eds., 2003) (affirming that hyperbolic or quasi-hyperbolic time preferences "have been used to explain . . . procrastination, contract design, drug addiction, self-deception, retirement timing, and saving").

127. Bar-Gill, *supra* note 124, at 1396–99.

128. *See id.* at 1388–94 (explaining the pricing system for credit cards, which includes purchasing items and then paying down the outstanding balance with a low minimum monthly payment).

129. *Id.* at 1396–97.

130. *Id.* at 1397.

131. *Id.*

becoming healthier, at any given meal an obese person will consume more calories than a healthy person.[132] Similarly, cigarette smokers discount future health losses, which could help explain why smokers continue to smoke.[133]

Privacy trading is similarly a risky behavior with delayed consequences. If a consumer trades away his privacy, the benefit is felt immediately (via the "thing"), whereas the consequence (harm from privacy loss) is delayed. Therefore, hyperbolic discounting may explain this privacy-trading behavior, just as it explains why consumers engage in risky credit-card debt. Granted, this will not apply to every consumer; some consumers may place little value on privacy and therefore always prefer consumption. For these consumers, the choice is always rational: consume. Furthermore, not every consumer is a hyperbolic discounter.[134] Just as some consumers choose not to borrow on a credit card, some of the consumers who prefer not to trade their privacy might choose not to purchase any IoT devices. For these consumers, the choice is always rational: don't consume. As was mentioned earlier, this analysis is limited to those consumers who prefer not to trade away their privacy but still purchase privacy-trading devices.

If a potential IoT-device purchaser is a hyperbolic discounter, then he may underestimate the future cost of trading away his privacy. Consider a consumer deciding whether or not to purchase a wearable fitness device, such as a Fitbit. He may be concerned about his privacy, and his preference may be that his data not be sold—even as de-identified data—to his employer. Nevertheless, he will choose to purchase the device because his preference today is the convenience of using a fitness tracker. He may then decide that a month from now, once he has formed the habit of working out, he will stop using the device, but when a month has passed, his preferences again reverse and he will keep using the device.

These smart devices are not a perfect equivalent to credit cards. While a consumer knows that a credit card will cost the debt incurred plus interest,[135] an IoT consumer faces uncertainty. While each purchase is a privacy trade, there is no guarantee that this trade will result in a negative event; the risk of the risky behavior may never manifest. When there is a chance that the future event may not be realized, it becomes more rational to discount the future; a person may therefore be more likely to be a hyperbolic discounter

---

132. *See generally* Robert L. Scharff, *Obesity and Hyperbolic Discounting: Evidence and Implications*, 32 J. CONSUMER POL'Y 3 (2009) (detailing how hyperbolic discounting affects the dieting choices of obese persons).

133. *See* Amy L. Odum et al., *Discounting of Delayed Health Gains and Losses by Current, Never- and Ex-Smokers of Cigarettes*, 4 NICOTINE & TOBACCO RES. 295, 301 (2002) (finding that "[s]mokers and ex-smokers discounted health losses more steeply than health gains").

134. *See* Bar-Gill, *supra* note 124, at 1396 (defining a hyperbolic discounter as an individual whose "short-run discount rate is larger than her long-run discount rate").

135. *See, e.g.*, 15 U.S.C. § 1637a (2012) (mandating that lenders disclose to borrowers the interest rate and minimum monthly payment on a credit card or other loan).

when the future is uncertain.[136] In fact, studies have shown that introducing uncertainty tends to impact the present choice more than the future choice.[137] When both the present and the future are uncertain, people are less impatient and prefer to wait for the uncertain event; when the present is certain, then it does not matter if the future is certain or uncertain: people are more impatient and prefer the present option.[138] An IoT user is therefore especially likely to be a hyperbolic discounter because the immediate benefit of the device is certain.

IV. Regulatory Solutions to the BLE Biases in the Internet of Things

Part II demonstrated that the IoT is an expanding world of largely unregulated devices that can easily lead to the sale of a consumer's data without the consumer's knowledge. Part III discussed why people might engage in these privacy trades, even when they prefer to keep their privacy intact. After analyzing why people make these trades, it becomes obvious that if policy makers want to protect biased consumers, then there is a need for some regulatory action. This Part analyzes three potential changes that could be enacted to help protect consumer privacy. In doing so, I do not advocate for any one particular change, but instead aim to provide a survey of positives and negatives in adopting each potential change. The response to each potential change is framed around whether the potential solution would address the behavioral biases that IoT users experience. A regulatory change would debias the consumers if it offered a direct response to irrationality that "attempt[s] to help people either to reduce or to eliminate" their biases.[139]

A. Debiasing Through Mandatory Disclosures

Consumers may be purchasing IoT devices because they are not aware of the privacy dangers posed by these devices.[140] Similarly, they may be unaware of their own biases that affect their purchasing behaviors.[141] One way

136. *See generally* Omar Azfar, *Rationalizing Hyperbolic Discounting*, 38 J. ECON. BEHAV. & ORG. 245 (1999) (arguing that when consumers are uncertain about the distant future, it may be rational to discount the future hyperbolically instead of exponentially).

137. *See, e.g.*, Gideon Keren & Peter Roelofsma, *Immediacy and Certainty in Intertemporal Choice*, 63 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 287, 290–91 (1995) (demonstrating that introducing uncertainty "has little effect in altering preferences for the delayed rewards (which already contain an element of uncertainty), but has a profound influence on immediate preferences").

138. *Id.* at 290.

139. Jolls & Sunstein, *supra* note 98, at 200.

140. *See* Peppet, *supra* note 13, at 142–45 (reviewing the privacy policies of various IoT devices and concluding that the policies are ambiguous with respect to what data the devices collect and who owns that data).

141. *See* James Friedrich, *On Seeing Oneself as Less Self-Serving Than Others: The Ultimate Self-Serving Bias?*, 23 TEACHING PSYCHOL. 107, 107–08 (1996) (demonstrating that even after being informed of a self-serving bias, people are still subject to that bias); Emily Pronin et al., *The*

to change consumer behavior could be to force knowledge upon consumers through mandatory disclosures. When the problem of consumer behavior "merely reflects a lack of information, then the traditional corrective is the straightforward provision of additional information."[142] Mandatory disclosures are already required in some areas where consumers would engage in risky behavior due to a lack of knowledge.[143]

Although there has been relatively little research conducted to explore expectations for IoT devices,[144] one study has noted that "users can make informed privacy trade-offs only if they understand what the technology is doing, why [it is doing so], and what the potential privacy and security implications are."[145] Accordingly, any mandated disclosures should include this information and answer the questions that consumers have about what information is collected, where such information is stored, if the user can edit or delete the data, and with whom the manufacturer will share the data.[146] Including this information should impact the consumer's view of how much control he has over his data; if he learns how little control he has over his data, then he will be less likely to underestimate his risk of harm. For maximum effectiveness, these disclosures should either be included in the box at purchase or in-the-box packaging should provide clear direction to how a user can find the disclosures.[147]

While these mandatory disclosures may help educate the consumer and therefore solve both the knowledge problem discussed in Part II and the control aspect of unrealistic optimism, they may not fully solve the bias problems explored in Part III.[148] Even if people are informed about the danger of privacy loss, the overoptimism bias "may lead [them] to underestimate their personal risks."[149] Therefore, to successfully change consumer behavior, the disclosures will need to debias the consumers; that is, they must inform consumers both of the risk involved with buying a product and of their

---

Bias Blind Spot: Perceptions of Bias in Self Versus Others, 28 PERSONALITY & SOC. PSYCHOL. BULL. 369, 370–71 (2009) (same).

142. Jolls & Sunstein, *supra* note 98, at 207.

143. *See, e.g.*, 15 U.S.C. § 1453 (2012) (compelling sellers of packaged consumer commodities to adequately label the goods); 15 U.S.C. §§ 1631–1632 (2012) (mandating that lenders provide disclosures to borrowers); 49 U.S.C. § 32705 (2012) (requiring that a person transferring ownership of a motor vehicle give disclosures to the transferee).

144. Peppet, *supra* note 13, at 160.

145. Predrag Klasnja et al., *Exploring Privacy Concerns About Personal Sensing*, *in* PERVASIVE COMPUTING 176, 182 (Hideyuki Tokuda et al. eds., 2009).

146. Peppet, *supra* note 13, at 161.

147. *Id.* at 162.

148. *See* Howard Latin, *"Good" Warnings, Bad Products, and Cognitive Limitations*, 41 UCLA L. REV. 1193, 1243 (1994) ("People may not respond properly to many risks designated in warnings because they are unduly optimistic about their ability to avoid these hazards.").

149. Jolls & Sunstein, *supra* note 98, at 207.

own biases.[150] Problematically, even when informed of the above average effect, a consumer will still view his perceived risk as being less than the average person's.[151] Therefore, an effective debiasing campaign will have to take a form other than mere education about biases.

There are several forms an effective debiasing campaign could take. First, a debiasing effort could use the availability heuristic to make information about risk more available for the consumer.[152] As discussed in Part III, the more available a negative event is to a person—that is, the more readily it comes to the person's mind—the less likely he is to underestimate the probability of the negative event occurring. Second, a debiasing cam-paign could reframe the risk by stressing the negative consequences of purchasing the device.[153]

Unfortunately, it is difficult to determine when disclosures and education campaigns making use of the availability heuristic will be successful.[154] For example, one study asked patients to estimate their likelihood of experiencing a heart attack, stroke, cancer, or motor-vehicle crash.[155] The researchers then estimated the patients' actual risk of experiencing these events and provided this personalized risk assessment to the patients.[156] The tailored feedback mitigated the unrealistic optimism bias for perceived stroke risk, but it did not substantially reduce the optimism in predicting the other three health problems.[157] This suggests that tailored feedback may not reduce the unrealistic optimism bias for IoT users. Furthermore, tailored feedback is impractical in mass campaigns; this debiasing method is more suited for

150. *See* Scott O. Lilienfeld et al., *Giving Debiasing Away: Can Psychological Research on Correcting Cognitive Errors Promote Human Welfare?*, 4 PERSP. ON PSYCHOL. SCI. 390, 393 (2009) (summarizing studies that have shown that "basic education about specific cognitive biases . . . also decreases participants' tendency to fall prey" to these biases).

151. *See* Linda Babcock & George Loewenstein, *Explaining Bargaining Impasse: The Role of Self-Serving Biases*, 11 J. ECON. PERSP. 109, 115 (1997) (finding that "being informed of the bias had no effect on the discrepancy in the parties' expectations").

152. Jolls & Sunstein, *supra* note 98, at 209–10.

153. *See id.* at 210–11 ("[M]aterial that describes the positive effects . . . produces significantly less behavioral change than material that stresses the negative consequences . . . .").

154. *Compare* Matthew W. Kreuter & Victor J. Strecher, *Changing Inaccurate Perceptions of Health Risk: Results from a Randomized Trial*, 14 HEALTH PSYCHOL. 56, 62 (1995) (finding that when patients were given a detailed assessment of the increased risk of stroke caused by smoking, they were more likely to have quit smoking at their next appointment than those who had not received the assessment), *with* Neil D. Weinstein, *Exploring the Links Between Risk Perceptions and Preventive Health Behavior*, *in* SOCIAL PSYCHOLOGICAL FOUNDATIONS OF HEALTH AND ILLNESS 22, 37 (Jerry Suls & Kenneth A. Wallston eds., 2003) ("None of the experiments [we] conducted had succeeded in . . . decreasing optimistic bias.").

155. Kreuter & Strecher, *supra* note 154, at 57.

156. *Id.* at 57–58.

157. *Id.* at 61 & tbl.4.

"settings that provide direct contact with your intended audience."[158] The cost of tailoring a message to the users of 220 billion devices would likely render this option impossible.

Nontailored disclosures may be successful if they use the availability heuristic by incorporating a specific instance of a negative occurrence.[159] When people are told a narrative about a person in similar circumstances, they become less overly optimistic.[160] One fairly successful use of the availability heuristic was when the Canadian government introduced a campaign to place pictures of diseased lips and gums on cigarette packages.[161] These pictures made the harm from smoking more available to smokers and therefore encouraged them to quit smoking.[162] Similarly, when a person is told a detailed story about how a drowning accident may occur, he will rate the probability of drowning as higher than he would otherwise.[163] An IoT user may be similarly impacted if the disclosures include a narrative about a negative experience a user had while using the specific device. For example, if computers came with an in-the-box disclosure about Superfish, then a consumer may be less likely to underestimate the risk of harm and, therefore, more likely to disable the privacy trading software. Similarly, if Progressive included a story about a person who used Snapshot only to see his rates increase, then a potential user may be less likely to underestimate the risk of harm.

Even if the disclosures are structured to mitigate overoptimism, they are unlikely to be the only regulatory solution. There are numerous problems with disclosures as a solution. First, the disclosures must be tested in multiple subcommunities to determine when a story triggers the availability heuristic and when it does not.[164] Second, the disclosures may have the unintentional effect of causing consumers to become overly pessimistic; this would be a negative outcome because "the goal is not to make all people as pessimistic as possible but rather to increase the accuracy of their predictions."[165] In other words, the goal is not to drive consumers away from an IoT product,

158. Weinstein, *supra* note 154, at 38.

159. *See* George Loewenstein et al., *Statistical, Identifiable, and Iconic Victims, in* BEHAVIORAL PUBLIC FINANCE 32, 33 (Edward J. McCaffery & Joel Slemrod eds., 2006) (summarizing multiple studies finding "that individual cases motivate people more powerfully than statistics").

160. *Id.*; Sean Hannon Williams, *Sticky Expectations: Responses to Persistent Over-Optimism in Marriage, Employment Contracts, and Credit Card Use*, 84 NOTRE DAME L. REV. 733, 751–52 (2009).

161. D Hammond et al., *Impact of the Graphic Candian Warning Labels on Adult Smoking Behavior*, 12 TOBACCO CONTROL 391, 391, 392 fig.1 (2003); Williams, *supra* note 160, at 751.

162. Hammond et al., *supra* note 161, at 393–94.

163. Laurie Hendrickx et al., *Relative Importance of Scenario Information and Frequency Information in the Judgment of Risk*, 72 ACTA PSYCHOLOGICA 41, 50, 55–56, 58–59 (1989).

164. Williams, *supra* note 160, at 752.

165. *Id.*

but rather to make consumers aware of the risk so that they can be intelligent purchasers. Finally, when disclosures are not individually tailored to the consumer—as would necessarily be the case for IoT devices—it is unlikely that the disclosures will impact a hyperbolic discounter.[166] While disclosures may help to mitigate the biases that IoT consumers experience, stronger regulatory action may be necessary.

B. Debiasing Through Regulatory Action

1. Changing the Default Rule.—A second way that policy makers could affect consumers' behavior is by changing the default rule.[167] A default rule is a background rule created by the courts and legislatures that fills in an unaddressed gap in contracts.[168] A commonly used default rule in consumer law is the opt-out system, whereby a consumer's consent to a manufacturer's terms "may be *inferred* from the fact that . . . the consumer did not object."[169] In layman's terms, opt out means take it or leave it: unless a consumer opts out of the terms either by not purchasing the item or by contracting with the manufacturer for more favorable terms, he is deemed to have agreed to the terms when he uses the purchased item. In reality, consumer contracts do not "afford[] the consumer a realistic opportunity to bargain," meaning that the only way to opt out is by not purchasing the desired product.[170] IoT devices are generally opt-out purchases—the consumer can either purchase the device and be subject to the manufacturer's chosen terms about how their data are collected, stored, and used (take it) or not purchase the device at all (leave it).

---

166. *See* Bar-Gill, *supra* note 124, at 1419 (explaining that disclosures more effectively target consumers when they are individualized); Kathryn W. Bailey, Note, *Fine Tuning Nutrition Disclosures: A Behavioral Law and Economics Critique of the Menu-Labeling Provision of the Affordable Care Act*, 93 TEXAS L. REV. SEE ALSO 103, 125–26 (2015) (arguing that personalized disclosures would counter hyperbolic discounting "by providing a record of past behavior"); Karen E. Francis, Note, *Rollover, Rollover: A Behavioral Law and Economics Analysis of the Payday-Loan Industry*, 88 TEXAS L. REV. 611, 635 (2010) ("Personal narratives . . . may do well to debias overoptimism in consumers, but . . . hyperbolic discounting may require a disclosure tailored specifically to the borrower.").

167. For an in-depth proposal of an opt-in system, see generally Joseph A. Tomain, *Online Privacy & The First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1 (2014).

168. Russell Korobkin, *The Status Quo Bias and Contract Default Rules*, 83 CORNELL L. REV. 608, 609–10 (1998).

169. Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745, 748 (2003).

170. Batya Goodman, Note, *Honey, I Shrink-Wrapped the Consumer: The Shrink-Wrap Agreement as an Adhesion Contract*, 21 CARDOZO L. REV. 319, 321 (1999).

By contrast, an opt-in data protection system would require that manufacturers "obtain *explicit* consent from individuals before collecting, using or exchanging information about them."[171] There are multiple ways policy makers could construct an opt-in system. For example, the system could "require opt-in consent before personal information could be disclosed to third parties outside the organization."[172] In the IoT sphere, this could work in one of two ways: first, the manufacturer could be required to obtain explicit consent whenever it wants to disclose the user's data; or second, the user could manually change a broad privacy setting from automatically opting out of disclosure to automatically opting in. Legislators could also choose a more restrictive opt-in system that would require explicit consent before a company was permitted to use any data, both internally and externally.[173] A more restrictive option seems unlikely because IoT devices rely on internal communication of data to have effective devices and services.[174]

Changing the default rule tends to have a large impact on consumers because consumers prefer to maintain the status quo.[175] In other words, consumers tend to "pick" the default rule—if the default is opt out, a consumer will rarely opt out, but if the rule is opt in, a consumer will rarely opt in.[176] A telling example is organ donation: countries with opt-in default rules, where a citizen must explicitly consent to donation, tend to have very low rates of consent, whereas countries with opt-out default rules, where consent is presumed, have very high rates of consent.[177]

A compelling reason to change the default rule for IoT devices is that such regulatory action would eliminate, or at least dramatically mitigate, the behavioral biases in purchasing discussed in Part III. Because data can be hacked or leaked without a consumer's consent,[178] the risk of harm would

171. Staten & Cate, *supra* note 169, at 748–49.

172. *Id.* at 762.

173. *Id.* at 765.

174. *See supra* Part II.

175. *See* Korobkin, *supra* note 168, at 625 ("[P]eople systemically favor maintaining a state of affairs that they perceive as being the status quo rather than switching to an alternative state, all else being equal.").

176. *See id.* at 675 ("Because individuals tend to prefer the status quo to alternative states, they are likely to prefer the default term, whatever it may be, to other options, all other things being equal.").

177. Eric J. Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 SCIENCE 1338, 1338–39 (2003).

178. *See* Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015, 7:06 PM), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/ [http://perma.cc/7A68-JMQC] (listing data leaks from 2014, including leaks from: Sony, in which the hackers exposed over 47,000 Social Security numbers; JP Morgan Chase, in which hackers obtained customers' personal information; and Home Depot, in which hackers stole the information of 56 million credit and debit cards); Michael S. Schmidt & David E. Sanger, *Russian Hackers Read Obama's Unclassified Emails, Officials Say*, N.Y. TIMES (Apr. 25, 2015), http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?_r=0

still be greater than zero; however, because a company would no longer be able to sell data (even de-identified) without the user's consent, the risk would be much lower than it is in the opt-out system. This mitigation of risk would bring an overly optimistic person's expectations more in line with the actual risk. Similarly, a hyperbolic discounter would no longer have the future to discount because a future preference of not trading privacy would be aligned with the current preference of purchasing the device.

The opt-in system would not, however, be a perfect system. There are three major flaws with changing the default rule. First, manufacturers may offer incentives to opt in, reducing the effectiveness of the regulation. Second, the biases analyzed in Part III may make consumers more likely to opt in, especially when an incentive is offered. Finally, changing the default rule could be criticized as being a paternalistic regulatory action.[179] I tackle each of these potential flaws below.

First, manufacturers may respond to a change in default rules by offering opt-in incentives to consumers. For example, manufacturers could offer two price packages for each device: first, a default, privacy-protective device at one price point; and second, an opt-in, privacy-threatening device at a lower price point. This two-tiered system would create an inadvertent penalty for users who do not opt in. In fact, this inadvertent penalty already exists in the employer insurance market.[180] Employers may offer financial incentives, such as a lower insurance rate or a higher bonus, to employees for participating in a "wellness program" to lose weight, reduce cholesterol, or improve other health goals.[181] Employees who choose not to participate are penalized when they cannot receive the financial incentives,[182] and this penalty may be unmerited when a person declines to answer a health survey for privacy reasons or cannot participate in the program because of a disability. Any dual-pricing structure for IoT devices would similarly shift the burden on to consumers who choose not to opt in to a privacy trade.

[http://perma.cc/TV7W-5DF8] (chronicling a 2014 data attack on the White House, including the breach of some of President Obama's unclassified email correspondence).

179. *See* Cass R. Sunstein & Richard H. Thaler, *Libertarian Paternalism Is Not an Oxymoron*, 70 U. CHI. L. REV. 1159, 1162 (2003) (explaining how default rules are "libertarian paternalism" at work).

180. *See* Sharon Begley, *Coming Soon to a Workplace Near You: 'Wellness or Else,'* REUTERS (Jan. 13, 2015, 4:48 PM), http://www.reuters.com/article/2015/01/13/us-usa-healthcare-wellness-insight-idUSKBN0KM17C20150113 [http://perma.cc/QF52-V3VX] (detailing incentives that employers offer to employees who participate in wellness programs, as well as penalties for those who do not); Alex Wayne, *Employers Can Pay Workers for Weight, Exercise, U.S. Says*, BLOOMBERG BUS. (Apr. 16, 2015, 3:18 PM), http://www.bloomberg.com/news/articles/2015-04-16/employers-can-pay-workers-to-track-weight-exercise-u-s-says [http://perma.cc/GK66-YHYF] (exploring a recent clarification by the EEOC that permits employers to offer financial incentives for participating in wellness programs).

181. Begley, *supra* note 180.

182. *Id.*

While the dual-pricing problem may seem like a large flaw, it would still be an improvement over the current out-opt model because the choice of privacy-sacrificing behaviors would be shifted to the consumer. Currently, if a consumer's preference is not to engage in privacy trading, his only recourse is to refrain from purchasing an IoT device. Under the opt-in model with dual pricing, consumers who value their privacy would have the option to use the device without engaging in privacy trades. Changing the default rule would allow privacy-valuing consumers to determine whether their privacy is worth the higher price tag.

The second potential problem with the opt-in model is that the likelihood of a consumer opting in may be exacerbated if he is unrealistically optimistic or a hyperbolic discounter, especially in a dual-pricing structure. If a consumer is overly optimistic, then he may underestimate the risk of harm and purchase the more tempting, lower priced option. Similarly, if he is a hyperbolic discounter, then he may prefer the privacy-protecting plan in the future, but the smaller price of the privacy-threatening plan now; the changed regulation would not impact his preference reversal. Nevertheless, incentive-based pricing may help to debias consumers because it would clarify to consumers how much their data are worth to manufacturers and third-party purchasers. A dual-pricing structure would "educat[e] consumers of both front-end and back-end costs," which would enable consumers to make more sophisticated, rational purchasing decisions.[183] The point of changing the default rule is not to remove choice from the individual, but to afford him the opportunity to make an educated decision. At a minimum, changing the default rule would leave those who still purchase the privacy-trading option no worse off than they were before the rule was changed.

The final problem of changing the default rule is that such action may be criticized as "paternalistic and partisan."[184] Paternalistic regulations may be seen as problematic when the government regulates an individual's choice "for the individual's own good, much as when parents limit their child's freedom to skip school or eat candy for dinner."[185] Depriving individuals of choice is problematic because only an individual knows his "true interests and motivations" behind a particular choice; therefore, each individual is in

183. *See* RONALD J. MANN, CHARGING AHEAD: THE GROWTH AND REGULATION OF PAYMENT CARD MARKETS 136–37 (2006) (implying that increased competition in a market helps to debias consumers and enable them to make educated decisions).

184. Cass R. Sunstein, *Switching the Default Rule*, 77 N.Y.U. L. REV. 106, 132 (2002).

185. Colin Camerer et al., *Regulation for Conservatives: Behavioral Economics and the Case for "Asymmetric Paternalism,"* 151 U. PA. L. REV. 1211, 1211 (2003). For a discussion of antipaternalism, see generally JOHN STUART MILL, ON LIBERTY (Gertrude Himmelfarb ed., Penguin Books 1982) (1859).

the best position to maximize his choice.[186] When the government steps in by regulating choice, the probability of error—assigning the wrong "choice"—is high.[187]

Behavioral economists, and in particular Cass Sunstein, counter this argument by proposing that paternalism can be used as a solution for "behavioral market failures," or market failures that are caused by human error and biases.[188] Sunstein has argued that just as market failures may justify paternalistic action, so should behavioral market failures justify action.[189] For example, when an industry has a negative impact on the environment (or in economic terms, there exists a negative externality on the environment), the government may impose restrictions on that industry or on individual companies.[190] Intervention may similarly be warranted when an individual's immediate choice is not reflective of his true preferences.[191] However, limiting choice may not always be warranted; paternalism may therefore be most appropriate when the risks of harm from government error are low and the risks of harm from private error are high.[192]

The risk of harm from government error is low if a regulation benefits the consumers who make errors, but does not cause harm to the consumers who are rational. Such a regulation would be "asymmetrically paternalistic."[193] A classic example of asymmetric paternalism is a default rule because, in most instances, a default rule must exist; there must be some default

186. MARK D. WHITE, THE MANIPULATION OF CHOICE: ETHICS AND LIBERTARIAN PATERNALISM, at xiii (2013).

187. *See id.* at xiii–xv (professing that policy makers cannot make the correct choice for every individual because they do not know the interests and motivations of every individual).

188. *See* JAMIE TERENCE KELLY, FRAMING DEMOCRACY: A BEHAVIORAL APPROACH TO DEMOCRATIC THEORY 17–21 (2012) (outlining Sunstein's thoughts on when paternalism is appropriate); Cass R. Sunstein, *The Storrs Lectures: Behavioral Economics and Paternalism*, 122 YALE L.J. 1826, 1834 (2013) (justifying paternalism because of behavioral market failures based on human error).

189. CASS R. SUNSTEIN, WHY NUDGE?: THE POLITICS OF LIBERTARIAN PATERNALISM 16–17 (2014).

190. *See* Daniel W. Bromley, *Environmental Regulations and the Problem of Sustainability: Moving Beyond "Market Failure,"* 63 ECOLOGICAL ECON. 676, 676–77 (2007) (arguing that if governments are going to enact environmental regulation in response to pressure "from the victims of externalities . . . then those changes . . . must pass a benefit-cost test"). The government also regulates industries with high barriers to entry, such as the electricity or water industries. DANIEL F. SPULBER, REGULATION AND MARKETS 8 (1989).

191. *See* SUNSTEIN, *supra* note 189, at 16 (arguing that when behavioral market failures happen, regulatory response may be justified).

192. *See id.* at 116 (imagining a world called Benthamville "in which we would want to make some distinctions designed to maximize welfare by, for example, authorizing paternalism when the risks of widespread private error are especially high (and the risks of government error low)").

193. Colin Camerer et al., *supra* note 185, at 1212.

if the consumer does nothing.[194] Changing the default rule would therefore be minimally paternalistic because it merely flips the current default if the customer does nothing.

In IoT devices, the current default terms are the privacy policies—and the terms thereof—that manufacturers have on their websites.[195] Under this model, there are three outcomes for consumers who wish to purchase an IoT device: first, the rational consumer who prefers not to engage in privacy trading will not purchase the device; second, the rational consumer who prefers to engage in privacy trades will purchase the device; and third, the irrational consumer who prefers not to engage in privacy trading will purchase the device. Changing the default rule in IoT purchases would be an example of asymmetric paternalism because it merely eliminates the first outcome, as the first consumer no longer has to choose between purchasing the device or making a privacy trade. While the second outcome is slightly impacted, such impact is minimal because if a rational consumer prefers a privacy-trading option, then he can choose to opt in to that privacy trade by choosing the alternative opt-in option.[196] The harm to this rational consumer would be the minimal transaction cost of picking the alternative option.

Furthermore, changing the default rule may be especially appropriate in IoT purchases because the transactions are structured to prevent learning. One prevalent criticism of paternalistic regulations is that they deprive people of "information that might educate [them] on how to improve decision-making."[197] If a regulation is paternalistic, critics argue, then it will always block true choice because people who cannot determine their true preferences will never be able to do so, and will "simply stick with the default."[198] Though it is important to allow consumers to determine "their true 'preferences,'"[199] it may be less important to do so in situations that do not provide an opportunity for learning.[200] When the opportunity for consumers to improve their decision making is low, either because the choice is infrequently made or because the cost of learning is high, then paternalistic action may be merited.[201] Two examples are retirement savings and choosing a

194. *Id.* at 1225.

195. *See supra* notes 78–80 and accompanying text.

196. *Cf.* Williams, *supra* note 160, at 765 (arguing that "[c]hanging the default rule of divorce would be an example of asymmetric paternalism" because "[c]ouples who are not optimistic are in a much better position to contract out of the default rule").

197. Gregory Mitchell, Review Essay, *Libertarian Paternalism is an Oxymoron*, 99 NW. U. L. REV. 1245, 1254 (2005).

198. *Id.*

199. Sunstein & Thaler, *supra* note 179, at 1164.

200. *Id.* at 1170; *see also* Mitchell, *supra* note 197, at 1254 n.34 (noting that some situations, such as retirement planning, may merit paternalistic action).

201. Jonathan Klick & Gregory Mitchell, *Government Regulation of Irrationality: Moral and Cognitive Hazards*, 90 MINN. L. REV. 1620, 1646 (2006).

spouse: by the time an employee retires and realizes that he did not save enough for retirement or a spouse realizes that he did not pick a good partner, it is too late for any beneficial learnings.[202]

At first blush, IoT purchases may seem not to fit this schema; after all, IoT purchases tend to be smaller and more frequent decisions than choosing a spouse. However, like with retirement savings, any harm from a privacy trade comes far too late for any beneficial learning. Just as an employee's working years cannot be repeated so that he saves more, once a consumer's information is released, it cannot be recalled. The cost of learning is extremely high and may merit the paternalistic regulatory action of changing the default rule.

2. Limiting Sellers Through Regulatory Action.—Yet another way—and the final way discussed in this Note—that policy makers could safeguard consumers is by taking more paternalistic, protective regulatory action. One such action could be "use constraint" rules that would limit how private data could be used by third parties.[203] As Scott Peppet, who proposed such use constraints in a recent article, explains:

> [D]ata from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public-health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decision making. A woman tracking her fertility should not fear that a potential employer could access such information and deny her employment; a senior employee monitoring his fitness regime should not worry that his irregular heart rate or lack of exercise will lead to demotion or termination; a potential homeowner seeking a new mortgage should not be concerned that in order to apply for a loan she will have to reveal her fitness data to a bank as an indicator of character, diligence, or personality.
>
> . . . Currently there is little to prevent a lender, employer, insurer, or other economic actor from seeking or demanding access to such information.[204]

Use constraint rules would limit the ability of the aforementioned third parties to access private information. Indeed, several states have passed similar use constraint rules to limit an employer's ability to examine an appli-

---

202. *See* Sunstein & Thaler, *supra* note 179, at 1170 ("[M]any of the most important decisions (for example, buying a home or choosing a spouse) are made infrequently and typically without the aid of impartial experts.").

203. Peppet, *supra* note 13, at 150–53.

204. *Id.* at 152–53.

cant's credit report.[205] These laws vary from state to state but generally require that an employer either give notice or obtain consent before accessing a credit report.[206]

In the IoT sphere, use constraints could limit how companies may collect, store, and use data. Just as some states limit an employer's ability to examine an applicant's credit report, so too could state law prohibit an employer from examining an employee's personal data collected by an IoT device. Such action would effectively eliminate the consumer biases discussed in Part III because it would remove any choice from the consumer—there would be no default rule from which a consumer could opt in or opt out; the consumer's only option would be for his data not to be used in the prohibited manner. As a result, use constraints would eliminate any lingering traces of bias that a less paternalistic solution, such as changing the default rule, might leave.[207] Because there would be no choice about use, the only decision left to the consumer would be whether or not to purchase the device. While this solution offers large benefits to biased consumers, there are two major problems with such a heavy-handed regulation. First, the removal of choice is highly paternalistic; as a result, it carries inherent harm to consumers. Second, use constraints may be difficult to implement and may freeze the market.

Unlike changing the default rule, creating a broad-sweeping use constraint that eliminated consumer choice would not be asymmetric paternalism because it would cause harm to rational people.[208] If a rational consumer wanted to trade his privacy for additional benefits, he would be deprived of the option, much like how a parent deprives a child of the option to eat candy for dinner.[209] Even advocates of asymmetric paternalism are hesitant to endorse such broad, sweeping paternalistic action.[210] Furthermore, paternalistic action here may create a "slippery slope" of moral

205. Lea Shepard, *Toward a Stronger Financial History Antidiscrimination Norm*, 53 B.C. L. REV. 1695, 1697 (2012); *see also* ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 14–21 (2013) (describing each state's laws about credit reporting and investigation).

206. SMITH, *supra* note 205, at 14–21. For example, Rhode Island prohibits businesses and persons from requesting a credit report in connection with a consumer's application for employment unless they inform the consumer the credit report might be requested, 6 R.I. GEN. LAWS § 6-13.1-21(a) (2014), and Vermont bars third-party disclosure of credit records without prior notice or consent, respectively. VT. STAT. ANN. tit. 9 § 2480b (2014).

207. *See supra* section IV(B)(1).

208. *See* Camerer et al., *supra* note 185, at 1250 ("Asymmetric paternalism aims to help boundedly rational people avoid making costly mistakes, while at the same time causing little or no harm to rational people.").

209. *See id.* at 1211 (analogizing paternalism to parental restrictions).

210. *See, e.g.*, Sunstein & Thaler, *supra* note 179, at 1199 ("So long as paternalistic interventions can be easily avoided by those who seek to adopt a course of their own, the risks emphasized by anti-paternalists are minimal.").

hazards.[211] Use constraints would prevent consumers from learning self-correction skills, and when people expect protection against excessive optimism, they may be less likely to develop "critical thinking skills that will guard against . . . optimism."[212] Use constraints are therefore a double-edged sword: they both deny rational consumers a choice and prevent biased consumers from learning rational behavior.

Another potential problem with use constraints is that they may freeze the market. While companies do not release information about how much money they have made by selling data, "the opportunity [to be had by exploiting data] is huge."[213] Amazon, for example, was estimated to generate between $500 million to $1 billion in advertising revenue in 2012.[214] This advertising revenue was generated by sharing data about users, such as the categories Amazon assigned to a user (e.g., "fashionista, gadget geek, mom or coffee enthusiast") or items that a user has viewed on Amazon's site.[215] Twitter and Facebook similarly employ users' data to generate revenue from targeted ads.[216] It is certainly possible that IoT manufacturers rely on the ability to sell, exploit, or otherwise use the data generated by consumers to increase revenue. If so, use constraints may be a disincentive for new companies to enter the IoT market or for existing companies to create additional products. Consequently, paternalistic use-constraint laws may be an impractical solution in the IoT market.

V. Conclusion

The Internet of Things (IoT) is an ever-growing, largely unregulated industry with potential for great harm. Each IoT device collects a variety of information about a user, including his location, biorhythmic data, fitness information, driving habits, and more. These datasets—either alone or in tandem—provide information that is valuable to employers, insurance companies, or other third parties, and IoT manufacturers are increasingly capitalizing on this value by selling the data to third parties. As a result, a consumer trades away his privacy whenever he purchases a device.

---

211. Douglas Glen Whitman & Mario J. Rizzo, *Paternalist Slopes*, 2 N.Y.U. J.L. & LIBERTY 411, 430–31 (2007).

212. *Id.* at 430.

213. Marcus Wohlsen, *Amazon's Next Big Business is Selling You*, WIRED (Oct. 16, 2012, 11:00 AM), http://www.wired.com/2012/10/amazon-next-advertising-giant/ [http://perma.cc/9MQG-4XFZ].

214. *Id.*

215. *Id.*

216. Davey Alba, *Twitter Starts Selling Ads on Other Apps and Sites*, WIRED (Feb. 3, 2015, 2:14 PM), http://www.wired.com/2015/02/twitter-starts-selling-ads-apps-sites/ [http://perma.cc/T4H5-5AKU].

This Note has demonstrated that at least some of these privacy trades are errors. Although some consumers value the benefit of the device over the loss of privacy, and therefore make the rational decision to purchase the device, other consumers would prefer not to lose their privacy, but nevertheless engage in privacy trades. These consumers purchase IoT devices both because they are overly optimistic about the risk of harm and because they are more impatient in the short run than in the long run. Furthermore, many consumers may be unaware of the privacy trades because of the lack of in-the-box disclosures upon purchase.

Policy makers have several regulatory options for protecting IoT consumers. First, they could compel manufacturers to include mandatory in-the-box disclosures that would advise consumers about the potential for privacy loss. These disclosures would include information about how these data are collected, where they are stored, and how they could be shared. To counter overoptimism, the disclosures should include a vivid anecdote about a person who had a negative privacy-loss experience while using the device. Second, legislators could take more paternalistic regulatory action by either changing the default rule or imposing use constraints on manufacturers. These actions would negate or limit the behavioral biases by allowing consumers to purchase the devices without sacrificing their privacy.

This Note does not present all of the possible behavioral biases affecting IoT consumers, nor does it analyze every regulatory action that legislators and other policy makers could implement to protect IoT purchasers. Instead, it offers a narrow look into how already-proposed regulatory action can be tailored to address *why* consumers purchase IoT devices. Perhaps with greater disclosure and more protection, consumers will become as concerned with privacy loss in the IoT market as they were when Superfish—an isolated event that posed less risk to privacy than everyday IoT use—was uncovered.

—Melissa W. Bailey