The Internet of Things and Potential Remedies in Privacy Tort Law

ALEXANDER H. TRAN*

The Internet of Things (IoT) is an intriguing digital phenomenon in technology that creates many legal challenges as the world becomes more interconnected through the Internet. By creating a connected system, the IoT links a network of physical objects, like consumer devices, and enables these devices to communicate and exchange data. In the very near future, almost every consumer device, from cars to a coffee mug, may connect through the Internet. The IoT has incredible potential to better society by providing immense amounts of rich sensory data for analytics and other uses. Nevertheless, there are also many latent dangers that could manifest as the IoT proliferates, including privacy violations and security risks.

The legal scholarship surrounding privacy issues with respect to the IoT is currently underdeveloped. This Note adds to the discussion of privacy law by analyzing the legal repercussions of the IoT and its relationship to privacy tort law. It summarizes the foundations of privacy law and current regulations that apply to the IoT and concludes that current laws and regulations provide limited remedies for consumers harmed by the IoT. It then provides a potential solution by suggesting that two privacy torts, the public disclosure of private facts tort and the intrusion upon seclusion tort, can provide partial civil remedies for those consumers. Each of the two privacy torts has evolved in different ways since its creation, and this Note explores the advantages and disadvantages of both. Finally, this Note advocates for the expanded use and revitalization of these privacy torts through judicial application in IoT cases as a potential strategy for regulating the IoT.

---

* Notes Editor, Colum. J.L. & Soc. Probs., 2016–2017. J.D. Candidate 2017, Columbia Law School. The author extends his gratitude to his advisor, Professor Clarisa Long, and to the editorial staff of the *Columbia Journal of Law and Social Problems*. He also thanks his family for their love and support. The author dedicates this Note to Tyler Parr.

I. INTRODUCTION

The proliferation of smart technology and wearable devices is culminating in a technological phenomenon known as the Internet of Things (IOT) — an all-encompassing network of Internet communication connecting everyday consumer devices. Although the IoT has no single, universally accepted definition, most scholars would agree that the IoT refers to a "world of interconnected, sensor-laden devices and objects."[1] Many devices contain microelectronmechanical systems sensors, which are sensors that translate physical phenomenon, like movement, heat, pressure, or location, into digital information.[2] These sensors are incorporated into consumer devices and, together, the collective interaction of these consumer devices creates the digital phenomenon known as the IoT. Examples of IoT devices include smart technology like smart fridges,[3] thermostats,[4] and most devices that record and analyze personal data.[5] Further, wearable technologies like FitBit/JawBone bracelets are part of the IoT.[6] This Note only analyzes privacy issues related to consumer devices like those listed above. Other IoT devices that contain factory and environmental sensors are undoubtedly important to the IoT, but are excluded from the scope of this Note.[7]

---

1. Thomas Goetz, *Harnessing the Power of Feedback Loops*, WIRED (June 19, 2011), http://www.wired.com/2011/06/ff_feedbackloop/ [http://perma.cc/H9D3-V6D3].

2. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98 (2014).

3. *See Smart ThinQ™ Super-Capacity 3 Door French Door Refrigerator with 8" Wi-Fi LCD Screen*, LG ELECTRONICS, http://www.lg.com/us/refrigerators/lg-LFX31995ST-french-3-door-refrigerator [https://perma.cc/C5SA-YJQC] (last visited Mar. 5, 2016).

4. *See Nest Thermostat*, NEST, https://nest.com/thermostat/meet-nest-thermostat/?alt=5 [https://perma.cc/C5SA-YJQC] (last visited Mar. 5, 2016).

5. For additional examples of IoT devices, see *Ember Coffee Mug*, EMBER TECHNOLOGIES, http://www.embertech.com/ [https://perma.cc/MDD6-3WJM] (last visited Mar. 5, 2016); *Self-Driving Car Project*, GOOGLE, https://www.google.com/selfdrivingcar/ [https://perma.cc/4GNE-D4R2] (last visited Mar. 5, 2016).

6. *See generally FitBit products*, FITBIT, https://www.fitbit.com/ [https://perma.cc/4FNU-9AQU] (last visited Mar. 5, 2016); *Jawbone Fitness Trackers*, JAWBONE, https://jawbone.com/ [https://perma.cc/29M3-STDU] (last visited Mar. 5, 2016).

7. For more information about smart factories and machinery, see Hyoung Seok Kang et al., *Smart manufacturing: Past research, present findings, and future directions*, 3 INT'L J. PRECISION ENG'G & MFG.-GREEN TECH. 111–28 (2016), http://link.springer.com/article/10.1007/s40684-016-0015-5 [https://perma.cc/CA9L-738H]; Detlef Zuehlke, *SmartFactory: Towards a factory-of-things*, 34 ANN. REV. CONTROL 129–38 (2010), http://www.sciencedirect.com/science/article/pii/S1367578810000143 [https://perma.cc/QN6X-LEAA].

The IoT is currently growing at a prolific rate. Experts predict that there were 25 billion connected devices in 2015, and by 2020, there will be 50 billion devices.[8] Others estimate that three and one-half billion sensors are already in the marketplace and expect that number to increase to trillions within the next decade.[9] The dramatic increase in sensor devices will likely result in more data collection. As a result, all of these connected devices will lead to an exponential increase in global consumer data generated, transmitted, stored, and shared. Much of this new sensor data will be highly personal, such as health information and financial spending patterns.[10] This Note therefore proposes a potential remedy for consumers when injury results from breaches or other violations of IoT device privacy.

This Note suggests that the IoT creates new privacy issues that can lead to consumer harms not covered under traditional privacy statutes, because those statutes generally govern data from particular industries like health data or financial records. In particular, this Note argues that the common law, specifically of privacy torts, provides a partial remedy for individual consumer harms. It proposes that privacy torts are suitable to regulate the illegal distribution of sensitive IoT data not meant for public dissemination. In particular, the "disclosure of private facts" and "intrusion upon seclusion" torts are suitable vehicles to regulate the IoT. IoT devices create detailed sensor data that require heightened protections only the law can provide. For this reason, these privacy torts should be extended and revitalized.

This Note proceeds as follows: Part I provides a brief introduction to the IoT. Part II discusses the potential privacy issues and

---

8. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1 (2015).

9. *Id.*

10. *See id.* at 1–2. Personal data could include health data — such as body weight, composition, and other body metrics — or personally identifiable information. The National Institute of Standards and Technology defines personally identifiable information as:

> any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUBLICATION 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) ES-1 (2010).

dangers the IoT creates. Part III surveys the current privacy framework that regulates the IoT, and Part IV details the proposed common law solution. Overall, the purpose of this Note is to suggest that privacy tort law can be a partial remedy for consumers injured by IoT devices and whose injuries are not covered by traditional privacy legislation such as HIPAA and the FCRA. This Note argues that the nature of sensitive sensor data created by the IoT warrants an extension of privacy tort law to IoT regulations in order to provide greater protection for consumers. Currently, U.S. privacy law is enforced through a mixture of federal and state legislation, executive agency enforcement, and some common law remedies in tort, contract, and property law.[11]

II. POTENTIAL PRIVACY ISSUES AND DANGERS CREATED BY THE IOT

The proliferation of the IoT creates several unique privacy problems. Section A of this Part will discuss a recent FTC staff report regarding the IoT that discusses the potential privacy and security risks inherent in the IoT.[12] Additionally, Professors Daniel Solove and Scott Peppet have advanced two additional theories of unique problems the IoT creates. First, Section B will discuss Professor Solove's "data aggregation problem," which considers the dangers of building "digital biographies" for individual consumers composed of disparate pieces of data.[13] Second, Section C will discuss Professor Peppet's "unexpected discrimination problem," which considers the inappropriate inferences that occur when these disparate portions of data are examined through analytics.[14]

---

11. *See generally* Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2012); Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1301 et seq. (2012); California Security Breach Notification Law, CAL. CIV. CODE § 1798.82 (West 2005); RESTATEMENT (SECOND) OF TORTS §§ 652B–D (1965).

12. *See* FED. TRADE COMM'N, *supra* note 8.

13. *See generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002); *see also infra* Part II.B.

14. *See infra* Part II.C.

A. THE IOT PRIVACY PROBLEMS CONSIDERED BY THE FTC

The IoT represents an amazing technological advancement that can provide enormous benefits to consumers. A recent FTC Staff Report lists several of these benefits.[15] For instance, IoT health devices can provide better access to consumer health data, resulting in increased monitoring of serious health conditions and regular interaction between physician and patient.[16] Further, home-automation devices like smart thermostats and smart alarms can allow consumers to control features in their homes while they are commuting to and from work.[17] Despite the many benefits associated with the growth of the IoT, however, these connected devices generate enormous amounts of consumer data resulting in greater privacy and security concerns.[18] Specifically, some IoT devices collect sensitive sensor data that many consumers may not want to share with the public, such as health information like body weight and sleep patterns.[19]

According to the FTC report, expert IoT panelists suggested that IoT devices present potential security risks in three forms: (1) enabling unauthorized access and misuse of personal information, (2) facilitating attacks on other systems, and (3) creating physical safety risks.[20] First, unauthorized access of sensor data is dangerous, because these breaches may result in exploited vulnerabilities in IoT devices and lead to identity fraud and theft.[21]

---

15. *See* FED. TRADE COMM'N, *supra* note 8.

16. *See* FED. TRADE COMM'N, *supra* note 8, at 2 ("These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases.").

17. *See id.* ("Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work.").

18. *See id.* at 14 (finding 10,000 households using IoT home-automation products can "generate 150 million discrete data points a day or approximately one data point every six seconds for each household" (footnotes omitted)).

19. Sensor data could include personal data like health information such as body weight and fitness logs. But there are many other types of sensor data, such as: position, velocity & acceleration, pressure, acoustic, humidity, light, radiation, temperature, chemical, and biosensors, which all collect varying types of sensor data. *See* JONATHAN HOLDOWSKY ET AL., INSIDE THE INTERNET OF THINGS (IOT) 7 (2015).

20. FED. TRADE COMM'N, *supra* note 8, at 10.

21. *See id.* at 11 (For example, "new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of

The growth of the IoT exacerbates this risk because "as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information."[22] Second, by installing more connected IoT devices, security vulnerabilities in one device may facilitate attacks on the consumer's network and enable attacks on other systems.[23] Finally, the IoT implicates safety concerns, because unauthorized persons may create risks to physical safety such as controlling internal computer networks in cars or remotely controlling individual health devices such as insulin pumps used by consumers.[24] Although all of these security risks present potential dangers related to the IoT, this Note focuses on the first issue presented: unauthorized access and misuse of sensitive sensor data relating to personal information.

The IoT creates several privacy risks due to the large amount of sensor data recorded, stored, and transmitted by each IoT device. For example, the FTC noted that fewer than 10,000 households using IoT home-automation products can "generate 150 million discrete data points a day or approximately one data point every six seconds for each household."[25] This immense volume of sensor data causes privacy issues that several different leading scholars have explored, such as the dangers of data aggregation and cross-contextual inferences discussed in this Note.[26]

---

information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud." (footnotes omitted)).

22. *Id.* (footnote omitted).

23. *See id.* at 12 (suggesting that "a compromised IoT device could be used to launch a denial of service attack. Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks. Another possibility is that a connected device could be used to send malicious emails." (footnotes omitted)).

24. *See id.* One IoT panelist noted he was "able to hack into a car's built-in telematics unit and control the vehicle's engine and braking, although he noted that 'the risk to car owners today is incredibly small,' in part because 'all the automotive manufacturers that I know of are proactively trying to address these things.'" *Id.* (footnotes omitted). Nevertheless, although these risks may seem small, the FTC noted that risks "could be amplified as fully automated cars, and other automated physical objects, become more prevalent." *Id.* at 12–13.

25. *Id.* at 14 (footnote omitted).

26. This Note adopts the privacy definition discussed in Professor Paul M. Schwartz's law review article. "The leading paradigm on the Internet and in the real, or offline world, conceives of privacy as a personal right to control the use of one's data." *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000). For a more in-depth discussion about privacy theory, see Pamela Samuelson, *A New Kind of Privacy?*

B. THE DATA AGGREGATION PROBLEM

Privacy scholar and professor Daniel Solove suggests that large data sets can create an "aggregation problem" for privacy[27]: while individual data (like one's social security number) is less harmful when viewed in isolation, it can be more damaging when combined with other data, such as one's financial information, educational records, medical records, because it can paint a portrait about an individual's personality called a "digital biography."[28] Compiling information in this manner is problematic because consumers' lives are not only "revealed and recorded, but also can be analyzed and investigated" by unauthorized or unknown third parties like employers and the government.[29] Moreover, Solove argues that the digital biography captures a "distorted persona [that] is constructed by a variety of external details," and is often inaccurate[30] because individuals may omit details explaining cross-contextual inferences.[31] Thus, third parties may

---

Regulating Uses of Personal Data in the Global Information Economy, 87 CAL. L. REV. 751, 777 (1999) (assessing the implications of Professor Schwartz's desire to treat data protection as a civil liberty); *see also* SIMON G. DAVIES, RE-ENGINEERING THE RIGHT TO PRIVACY: HOW PRIVACY HAS BEEN TRANSFORMED FROM A RIGHT TO A COMMODITY, TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 153 (Philip E. Agre & Marc Rotenberg eds., 1997) (asserting that many privacy scholars attempt to find a single definition of privacy, but even after decades of discussion, there is still no agreed upon definition); Anita L. Allen, *Privacy-As-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 864 (2000) (suggesting three reasons why there is wide variation in definitional accounts of privacy).

27. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1185 (2002) ("Viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities. The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined. Even information in public records that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information.").

28. *See id.* (asserting that "although one's Social Security number does not in and of itself reveal much about an individual, it provides access to one's financial information, educational records, medical records, and a whole host of other information").

29. *Id.* at 1186 (For example, "the firm HireCheck serves over 4000 employers to conduct background checks for new hires or current employees. It conducts a national search of outstanding warrants, a Social Security number search to locate age, past and current employers, and former addresses, a driver record search, a search of worker's compensation claims 'to avoid habitual claimants or to properly channel assignments,' a check of civil lawsuit records, as well as searches for many other types of information. These investigations occur without any external oversight, and individuals often do not have an opportunity to challenge the results.").

30. *Id.* at 1187.

31. *See id.* (Professor Arthur Miller observes that an "individual who is asked to provide a simple item of information for what he believes to be a single purpose may omit explanatory details that become crucial when his file is surveyed for unrelated purposes.").

draw potentially inappropriate conclusions when analyzing two separate forms of data collected in different contexts without additional information explaining the relationship, or lack of relationship, between the two. For instance, credit companies may use health information collected from a health-tracking device like a FitBit to make determinations about a consumer's creditworthiness for a loan.[32] By using the "rich, accurate, and fine-grained" sensor data gathered by IoT devices, credit companies can make powerful inferences about consumers' personalities and habits.[33] Without pertinent details explaining cross-contextual inferences, information viewed in other contexts may become unrepresentative and inaccurate, because researchers are still uncertain whether sensor data can "correlate with or predict certain economically valuable traits."[34] Finally, even if the digital biographies contain accurate information, the unregulated cross-contextual analysis raises its own privacy issues, mainly the unpermitted invasion of privacy.

From an efficiency theory perspective, inaccurate or false information is inefficient because it allows sellers to engage in disadvantageous transactions after forming an incomplete picture of the product.[35] In the IoT setting, the aggregation problem may lead to inefficiencies, because third party data brokers, who engage in the buying and selling of personal data, may cause disadvantageous transactions by selling inaccurate and incomplete consumer data biographies. Both buyers of consumer data and consumers themselves are injured by inaccurate transactions, which results in reduced efficiency. For example, a business organization (buyer) may hire a background screening company

32. For example, credit card companies may use health information collected from a health-tracking device to make determinations about a consumer's creditworthiness for a loan. *See* Peppet, *supra* note 2, at 118.

33. *Id.* at 119.

34. *Id.* at 120; *see* Solove, *supra* note 27, at 1181.

35. *See* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399–400 (1977) (posing an analogy to the world of commerce: "[w]e think it wrong (and inefficient) that the law should permit a seller in hawking his wares to make false or incomplete representations as to their quality. But people 'sell' themselves as well as their goods. They profess high standards of behavior [to] induce others to engage in social or business dealings with them from which they derive an advantage but at the same time they conceal some of the facts that these acquaintances would find useful in forming an accurate picture of their character. . . . But everyone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities.").

(third-party data broker) to conduct background checks on prospective employees (consumers). In this instance, an inaccurate digital biography could be devastating for both the buyer and the consumer. The buyer may miss qualified candidates, and a qualified consumer could lose a potential job opportunity.[36]

C. THE UNEXPECTED DISCRIMINATION PROBLEM

As applied to the IoT, the data aggregation problem suggests that sensor data collected from IoT devices may allow unexpected inferences by Big Data analytics.[37] The large aggregation of data in digital biographies could result in unexpected inferences when analytics make conclusions through cross-contextual analyses. Professor Peppet asserts that cross-contextual analyses may lead to unforeseen discrimination problems.[38] He suggests that the "massive amounts of sensor data from the IoT devices can give rise to unexpected inferences about individual consumers" that employers, insurers, lenders, and others may use when making important economic decisions.[39] For example, a consumer using a fitness-tracking device may store information online relating to weight loss and other health information.[40] If this hypothetical consumer decides to apply for a job, mortgage, or loan, a prospective employer or lender may ask for the consumer's health-tracker records from prior months.[41] Employers have many good reasons for seeking information collected by wearable health-

---

36. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 45–47 (2004) (Professor Solove provides a frightening example of the dangers of inaccurate digital biographies: a Maryland woman wrongly arrested for burglary was not cleared from the state's criminal databases. Her name and SSN also migrated to a different database relating to child protective services cases. She was fired from her job as a substitute teacher, and only after she could establish that the information was in error was she rehired. When she later left that job to run a day care center, she was questioned about the erroneous arrest. Later on, when employed as a child care director, she was terminated when her arrest record resurfaced in a background check. "Since she could not have the error expunged in sufficient time, the job was given to another person. . . . As our digital biographies are increasingly relied upon to make important decisions, the problems that errors can cause will only escalate in frequency and magnitude.").

37. *See* Peppet, *supra* note 2, at 117.

38. *See generally* Peppet, *supra* note 2.

39. *Id.*

40. *See, e.g.*, *Fitbit products*, *supra* note 6; *Jawbone Fitness Trackers*, *supra* note 6.

41. *See* Peppet, *supra* note 2, at 118–19 ("In March 2013, for example, CVS Pharmacy announced that employees must submit information about their weight, body fat composition, and other personal health metrics on a monthly basis or pay a monthly fine. It is not a big step to imagine employers incorporating such data into hiring as well.").

tracking devices like FitBit and Jawbone. For example, FitBit data could suggest behavioral patterns like impulsivity and inability to delay gratification, both of which may be inferred from one's exercise habits.[42] Furthermore, impulsivity also correlates with "alcohol and drug abuse, disordered eating behavior, cigarette smoking, higher credit-card debt, and lower credit scores,"[43] which may impact a consumer's job prospects or creditworthiness. FitBit also tracks sleeping patterns, some of which can be "linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear."[44] Therefore, seemingly harmless sensor data collected from a FitBit can lead to unexpected inferences by third parties with access to such data, which may then result in difficult discrimination problems, such as denying consumers mortgages or loans based on behavioral inferences gathered from a FitBit device.[45] Researchers are still uncertain whether sensor data can "correlate with or predict certain economically valuable traits" because "[f]itness may not predict creditworthiness; driving habits may not predict employability."[46] Therefore, until there is empirical verification that sensor data can accurately predict behavioral characteristics, consumers should not be subjected to powerful discriminatory inferences by data analytics employed by companies.

Some employers already have access to sensor data collected by health-tracking IoT devices, which they could potentially use

---

42. *See id.* at 119.

43. Peppet, *supra* note 2, at 119. For more information on the correlation between impulsivity on the one hand and substance abuse and eating disorders on the other hand, see generally Sharon Dawe & Natalie J. Loxton, *The Role of Impulsivity in the Development of Substance Use and Eating Disorders*, 28.3 NEUROSCIENCE & BIOBEHAVIORAL REV. 343, 346 (2004) ("Specifically, when given a choice, substance users consistently show a greater preference for small, immediate rewards (typically hypothetical access to preferred drugs and money) over larger, delayed rewards.").

44. *Id.*; *see Sleep, Performance, and Public Safety, HealthySleep*, DIV. OF SLEEP MED., HARV. MED. SCH. (2007), http://healthysleep.med.harvard.edu/healthy/matters/consequences/sleep-performance-and-public-safety [https://perma.cc/38HD-J877] ("Sleep deprivation negatively impacts our mood, our ability to focus, and our ability to access higher-level cognitive functions.").

45. *See* Peppet, *supra* note 2, at 147 ("[S]ensor data might be used as proxies in illegal racial, age, or gender discrimination and because highly tailored economic sorting is itself controversial."). Fitbit sensor data is already being used as evidence in court rooms. *See* Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, WALL ST. J. BLOG (Apr. 21, 2016, 1:53 PM), http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case/ [https://perma.cc/6DNV-NTL4] (describing how prosecutors used Fitbit data as critical evidence to disprove a rape allegation).

46. *See* Peppet, *supra* note 2, at 120.

for discriminatory purposes. For example, in September 2015, Target joined a list of Fortune 500 companies that implemented a "Wellness Initiative" promoting healthy lifestyles by providing Target employees with a free or discounted FitBits.[47] As part of the corporate wellness program, Target employees participate in an "average daily steps challenge" monitored by the FitBit Wellness Division that analyzes other corporate wellness programs across America.[48] Target's program is just one example of the proliferation of the IoT; many other organizations are implementing their own corporate wellness programs.[49] Companies may use analytics to interpret this sensor data and monitor employee productivity or efficiency, potentially violating an employee's expectations of privacy. Corporate wellness programs are especially suspicious because employers could consider data collected outside work hours, such as sleep patterns or dietary habits, when making important economic decisions like determining employee benefits or compensation. As a result, employers could potentially discriminate against employees by analyzing data gathered entirely outside the conventional workplace. Therefore, these privacy and security concerns, such as the data aggregation and unexpected discrimination problem, demonstrate that the IoT deserves close attention by the government and the courts to protect consumers from injury.

III. SURVEY OF CURRENT IOT PRIVACY REGULATION

Currently, American privacy law is a collection of federal and state legislation, executive-agency enforcement, and some common-law enforcement in tort, property, and contract law. This Part details IoT regulation that could occur within each of these categories.

---

47. *See Target Kicks off New Team Member Wellness Initiatives*, TARGET, https://corporate.target.com/article/2015/09/team-member-wellness [https://perma.cc/Z5TG-6TJW] (last visited Mar. 5, 2016).

48. *See id.*

49. *See The Best of 2015: 9 Companies that Nailed It*, FITBIT, http://content.fitbit.com/Best_Of_2015.html?promosrc=website [https://perma.cc/P5HT-UGJK] (last visited Mar. 5, 2016).

A. FEDERAL LEGISLATION

First, federal privacy legislation may regulate the IoT, including the Fair Crediting Report Act (FCRA),[50] the Children's Online Privacy Protection Act (COPPA),[51] and the Health Insurance Portability and Accountability Act (HIPAA).[52] Each statute governs privacy in a separate category. For example, COPPA applies to the online collection of information from children. COPPA states that "[i]t is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed . . . ."[53] The regulations require the Internet operator to provide notice on the website of what data is being collected and to obtain verifiable parental consent.[54] In the event of a breach, COPPA delegates the Federal Trade Commission (FTC) authority to pursue legal enforcement for a violation of an unfair or deceptive act or practice.[55] Similarly, the FCRA governs the accuracy and fairness of credit reporting and reasonable procedures used by consumer reporting agencies.[56] And HIPAA, through its privacy provisions, gives consumers rights to their health information and sets rules and limits on

50. *See generally* 15 U.S.C. § 1681 et seq. (2012).

51. *See generally* 15 U.S.C.A. § 6502 (West 2012).

52. *See generally* 42 U.S.C. § 300gg (2012); 29 U.S.C. § 1181 et seq. (2012); 42 U.S.C. 1320d et seq. (2012).

53. 15 U.S.C.A. § 6502(a) (West 2012) ("It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b) of this section.").

54. *See* 15 U.S.C.A. § 6502(b) (West 2012) ("(b) Regulations . . . (A) require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child — (i) to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and (ii) to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children . . . .").

55. *See* 15 U.S.C.A. § 6502(c) (West 2012) ("[A] violation of a regulation prescribed under subsection (a) of this section shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 57a(a)(1)(B) of this title.").

56. *See* 15 U.S.C. § 1681 et seq. (2012) ("(a) Accuracy and fairness of credit reporting. The Congress makes the following findings: (1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.").

who can look at and receive this health information.[57] Therefore, if an IoT operator commits a violation pertaining to the above categories governed by federal statutes, consumers may have remedies pursuant to the prescribed statute.[58] For example, the FTC pursued its first IoT case after a home webcam company failed to provide adequate security measures and allowed hackers to access private live-streams of consumer households.[59]

B. STATE LEGISLATION

Second, some state legislation may provide remedies to consumers for IoT harms. For example, many states have data-breach notification statutes that alert consumers when there is a breach of personal information.[60] Almost all of these states' statutes cover "personal information," which refers to an individual's name, "plus one or more of the individual's social security number, driver's license number, or bank or credit card account information."[61]

These state statutes, however, likely do not cover sensor data from IoT devices and are insufficient to provide a remedy to consumers. Specifically, many state breach notification statutes do not adequately define "personal information" to include sensitive sensor data collected from IoT devices.[62] For example, only Texas's statute defines "sensitive personal information" to include "information that identifies an individual and relates to [. . .] the physical or mental health or condition of the individual" in its definition of "sensitive personal information."[63] Texas's statute

57. *See* Privacy Rule (Subpart E), 45 C.F.R. §§ 164.500–34 (2015).

58. *See infra* Section III.C and accompanying text (discussing the first IoT case pursued by the Federal Trade Commission in 2013).

59. *See In re* Trendnet, Inc., No. 122-3090, 2013 WL 4858250, at *2 (F.T.C. Sept. 3, 2013).

60. *See* STATE DATA BREACH STATUTE FORM, BAKER HOSTETLER 1 (2014), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf [https://perma.cc/HV4L-Q5TY] (providing "standard definitions of Personal Information and Breach of Security based on the definition commonly used by most states").

61. Peppet, *supra* note 2, at 137; *see* STATE DATA BREACH STATUTE FORM, *supra* note 60, at 1.

62. *See* Peppet, *supra* note 2, at 137–38 (considering the possible treatment of IoT security violations under state data-breach notification statutes).

63. *Id.* at 138 n.321; *see* TEX. BUS. & COM. CODE ANN. § 521.002(a)(2)(B)(i) (West 2009) ("(2) 'Sensitive personal information' means, subject to Subsection (b): (A) an individual's first name or first initial and last name in combination with any one or more of the following items . . . : (i) the physical or mental health or condition of the individual; (ii)

likely includes sensor data like fitness-tracking data, which relates to the physical and mental health or condition of an individual. Only a few states have breach notification statutes that adequately define "personal information" to include sensitive sensor data collected from IoT devices.

C. EXECUTIVE AGENCY ENFORCEMENT

Third, the FTC is the executive agency that oversees consumer privacy enforcement. The FTC uses its general authority under the Federal Trade Commission Act (FTC Act) to penalize companies for security lapses.[64] The FTC Act states that "unfair or deceptive acts or practices in or affecting commerce" are unlawful.[65] The first IoT device case the FTC pursued was the 2013 TRENDnet home webcam action.[66] TRENDnet provides "cameras for consumers to conduct security monitoring of their homes or businesses, by accessing live video and audio feeds (live feeds) from their cameras over the Internet."[67] The TRENDnet action was brought because, as the FTC later found, TRENDnet misrepresented its security measures to consumers[68] and failed to provide "reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras."[69] As a

---

the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.").

64. *See* 15 U.S.C. § 45(a)(2) (2012) ("(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."); Peppet, *supra* note 2, at 136–37.

65. 15 U.S.C. § 45(a)(1) (2012) ("(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade. (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

66. *In re* Trendnet, Inc., No. 122-3090, 2013 WL 4858250, at *2 (F.T.C. Sept. 3, 2013).

67. *Id.* at *1.

68. *See id.* at *2 (TRENDnet "b. described the IP cameras as 'secure' or suitable for maintaining security, including through: i. a sticker affixed to the cameras' packaging, the same as or similar to the one depicted below, which displays a lock icon and the word 'security' . . . ii. a statement on the cameras' packaging that it may be used to 'secure,' or 'protect' a user's home, family, property, or business . . . and iii. product descriptions on respondent's website and in other advertisements . . .[; and] c. provided an authentication feature, which requires users to enter login credentials before accessing the live feeds from their IP cameras over the Internet." (internal cross references omitted)).

69. *Id.*

result, hackers exploited the security vulnerabilities leading to "compromised live feeds display[ing] private areas of users' homes and allow[ing] the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[70] The FTC found significant consumer harm because the breach allowed exposure of sensitive information permitting consumer homes to be targeted for theft or otherwise observed and recorded by strangers, impaired ability for consumers to peacefully enjoy their homes, and reduced consumer ability to control the dissemination of personal information.[71] The final settling charges required TRENDnet to establish a comprehensive security program and to notify customers about security issues and the availability of software updates to correct these issues.[72] The TRENDnet order marks the first IoT device action pursued by the FTC and shows that the FTC has some authority to enforce IoT related cases.

However, while the FTC may have authority to pursue IoT-related cases, as shown in the TRENDnet action above, the scope of its authority is unclear. For example, Professors Gerard Stegmaier and Wendell Bartnick noted that the FTC has not formally made rules or developed a formal adjudication process related to data security, instead regulating data security through complaints and consent orders.[73] Professor Stegmaier says this "method creates ambiguity because complaints and consent orders differ when identifying noncomplying practices and imposing data-security safeguards."[74] These complaints create ambiguity, because they "do not provide a blueprint for entities to follow because the FTC cryptically states that the [different] failures 'tak-

70. *Id.* at *3.

71. *See id.* at *4.

72. *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against TRENDnet, Inc. (Feb. 7 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc [https://perma.cc/QE76-3MBM].

73. *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 692 (2013) (asserting "the FTC has not used its rulemaking authority to issue rules related to data security. Instead, the agency has used an enforcement approach to implement its policy, and in at least some circles the agency's work in privacy and data security has been referred to as creating an emerging 'common law' of privacy.").

74. *Id.* at 693; *see also* Timothy E. Deal, Note, *Moving Beyond "Reasonable": Clarifying the FTC's Use of Its Unfairness Authority in Data Security Enforcement Actions*, 84 FORDHAM L. REV. 2227, 2241–43 (2016) (discussing two recent cases challenging FTC's unfairness authority in the data security context).

en together' violate Section 5 [of the FTC Act], and each complaint lists different data security practices."[75] The FTC, however, asserts that the Commission's data security requirements provide adequate notice by means of the complaints and consent decrees from previous FTC data enforcement actions published weekly on its website.[76]

Another problem with FTC regulation is that consumers have limited remedies for IoT violations that occur outside the scope of state and federal legislation or FTC authority. For example, the FCRA is one potential remedy, but the FCRA excludes most "first parties" that collect consumer information, and therefore does not cover IoT manufacturers who conduct in-house analytics concerning determinations about credit, insurance, or employment purposes.[77] In addition, the FCRA does not cover companies that collect data directly from consumers' connected devices and use this data to make in-house credit, insurance, or other eligibility decisions.[78] The FTC staff report gives an example of an insurance company offering consumers the option to submit fitness-tracker data in exchange for lower health insurance premiums.[79] In such circumstances, FCRA provisions requiring the "ability to access the information and correct errors, may not apply" because the insurance company itself would not have the ability to access consumers' FitBit trackers.[80]

In conclusion, consumers have limited remedies when an IoT violation resulting in consumer harm is not covered by legislation

---

75. *See* Stegmaier, *supra* note 73, at 693 (noting such failures include "fail[ure] to have an information security policy, implement system monitoring, fix known vulnerabilities, maintain firewalls and updated antivirus software, use encryption, implement intrusion detection and prevention solutions, store information only as long as necessary, and prepare for known or reasonably foreseeable attacks").

76. *See* Deal, *supra* note 74, at 2242.

77. *See* 15 U.S.C.A. § 1681a (West 2012) (The FCRA, however, does not cover "first parties" who conduct direct transactions between the consumer and the reporting agency. This exception potentially including IoT manufacturers who do not transmit information to third parties and instead conduct in-house analytics.); FED. TRADE COMM'N, *supra* note 8, at 16–17 (The FCRA covers business entities that are transmitters of information by reporting information to consumer reporting agencies or other third parties, or to affiliates. IoT devices are likely not included because IoT manufacturers do not fall under the definition of a consumer reporting agency.).

78. *See* FED. TRADE COMM'N, *supra* note 8, at 17.

79. *See id.* ("For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA's provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.").

80. *Id.*

or FTC authority. Due to the expansive nature of the IoT, there are several circumstances in which IoT devices do not cleanly fall under industry-specific privacy legislation such as the FCRA or HIPAA.[81] In these specific situations involving breaches of sensitive consumer information, this Note advocates for the increased use of privacy torts to provide a partial remedy for consumers.[82]

IV. PRIVACY TORTS AND THE IOT

Privacy tort law is immensely influenced by the theories of legal scholars Samuel Warren, Louis Brandeis, and William Prosser.[83] In their groundbreaking 1890 law review article, Warren and Brandeis advocated for the legal recognition of a "right to be let alone," rooted in the protection of individual dignity.[84]

Influenced by Warren and Brandeis, Professor William Prosser categorized the four privacy torts later recognized by the Restatement (Second) of Torts: public disclosure of private facts, intrusion upon seclusion, false light, and appropriation of name or likeness.[85] This Note focuses on the privacy torts of public disclosure of private facts and intrusion upon seclusion as potential remedies in tort for consumers who suffer injuries from IoT de-

81. For example, although FitBit is HIPAA-compliant with HIPAA-covered entities, FitBit itself is not a recognized covered entity that must comply with HIPAA rules. Thus, if a consumer receives a FitBit from a covered entity, such as a health care provider, that data is covered by HIPAA, but if a consumer buys a FitBit from a regular electronics store, this data is no longer covered by HIPAA. *See Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/hipaa/for-professionals/covered-entities/ [https://perma.cc/RMD6-EDP5] (last visited Mar. 3, 2016). As a result, some health information collected by FitBits and other wearable devices could fall outside the scope of HIPAA.

82. *But see* Eugene Volokh, *Tort Law vs. Privacy*, 114 COLUM. L. REV. 879, 881 (2014) ("But tort law, and especially negligence law, can also reduce privacy. Tort law can pressure property owners, employers, and consumer product manufacturers into engaging in more surveillance. Tort law can pressure colleges, employers, and others into more investigation of students', employees', or customers' lives. Tort law can pressure landlords, employers, and others into more dissemination of potentially embarrassing information about people. Tort law can require people to reveal potentially embarrassing information about themselves.").

83. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1888 (2010) ("It is impossible to talk about privacy in American tort law without considering William Prosser. Samuel Warren and Louis Brandeis may have popularized privacy in American law with their famous 1890 article, The Right to Privacy, but Prosser was the law's chief architect.").

84. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

85. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); *see also* RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW INST. 1977).

vices. Although other sources of law exist that can serve as remedies for IoT breaches, such as the duty of confidentiality in tort law,[86] this Note argues that the sensitive sensor data generated by IoT devices warrants an extension of these privacy torts to provide a remedy for consumers injured by breaches or violations committed by IoT companies and third parties. In particular, the public disclosure of private facts and intrusion upon seclusion torts are suitable remedies.

By advancing the argument that sensitive sensor data warrants an extended use of privacy torts, this Note hopes to influence the American Law Institute's next publications of the Restatement of Torts and Restatement of Data Privacy. Currently, the Restatement (Second) of Torts sets forth a framework for analyzing the disclosure of private facts and intrusion upon seclusion torts.[87] The ALI should refine the Restatement principles to consider the privacy issues accompanying emerging technologies like the IoT. For example, in Comment B of the intrusion upon seclusion tort, the Restatement says that an intrusion need not be physical to be actionable and that an intrusion can occur when the defendant uses his or her senses, "with or without mechanical aids, to oversee or overhear the plaintiff's private affairs."[88] This comment seems to consider IoT devices like mechanical aids that can transmit plaintiff's private affairs. Therefore, the drafters should include more relevant examples — beyond the traditional devices like wire taps or binoculars — that cover the wide range of sensors that are part of the IoT.[89] By updating these comments with new examples that include a broader range of emerging technologies, the American Law Institute can signal to courts that the privacy torts remain durable vehicles for private plaintiffs to seek reparations. As a result, courts will have the option

86. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 126 (2007) (arguing the right to privacy constructed by Warren and Brandeis can be found in the robust body of confidentiality law).

87. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B, D (AM. LAW INST. 1977).

88. *Id.* § 652B cmt. b.

89. For example, mechanical aids could be clarified to include new sensors. Currently, Comment B includes the following examples of intrusion:

> [Intrusion could be] looking into his upstairs windows with binoculars or tapping his telephone wires. [Intrusion] may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents.

Id.

of adopting the Restatement of Law proposals in addition to fashioning their own legal solutions in response to future data breaches and consumer harms, which will supplement existing IoT regulation to provide remedies for consumers. This Note explores these privacy torts as potential solutions in the following Sections.

A. PUBLIC DISCLOSURE OF PRIVATE FACTS TORT

The public disclosure of private facts (private facts) tort can be applied to the IoT because of its flexibility and an emerging judicial willingness to extend this tort to remedy consumer harms. The private facts tort creates a cause of action for the public disclosure of a private matter that is "highly offensive to a reasonable person."[90] According to the Restatement (Second) of Torts, the private facts torts arises when:

> one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[91]

This privacy tort "provides for tort liability involving a judgment for damages for publicity given to true statements of fact."[92]

This privacy tort is potentially useful because the richness of IoT sensor data may mean this data can be considered "private facts," and any publications or disclosures of this data could be considered an invasion of privacy. However, part (b) above, known as the "newsworthiness defense," proves to be the strongest hurdle a plaintiff must overcome when bringing a private facts claim. Since the private facts tort is the most controversial privacy tort with respect to freedom of speech and the First Amendment, courts have been wary in applying this tort.[93] In

90. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).
91. *Id.*
92. *Id.*
93. *See* Jenkins v. Dell Publishing Co., 251 F.2d 447 (3d Cir. 1958) (finding a sufficient public interest to exonerate defendants for publishing the story of how Jenkins had been kicked to death by a teen-age gang); Kelley v. Post Publishing Co., 98 N.E.2d 286 (Mass. 1951) (finding sufficient public interest to exonerate defendants after they published a photo of the body of plaintiff's daughter immediately after her death in a car accident); Harry Kalven, Jr., *Privacy in Tort Law: Were Warren and Brandeis Wrong?*, 31 LAW

fact, Professor Harry Kalven noted that the newsworthiness defense may be so overpowering as to essentially swallow the tort.[94] Due to this powerful defense, the private facts tort has experienced stunted development as compared with the other privacy torts. This Section will explore how the tort comes into tension with the First Amendment. Second, it will discuss instances when courts have applied the private facts tort. And finally, it will apply the private facts tort to the IoT.

1. *The First Amendment, the Private Facts Tort, and the Newsworthiness Defense*

The tension between the right to free speech and the protection of privacy in the form of the private facts tort was observed by the U.S. Supreme Court in *Florida Star v. BJF*.[95] In *Florida Star*, a newspaper published a rape victim's name after obtaining the information from a police department press release.[96] The plaintiff filed a negligence per se lawsuit against the newspaper and the police department under a Florida statute banning the publication of sexual offense victims' names.[97] The trial court ruled in favor of the plaintiff and found the Florida statute constitutional because it "reflected a proper balance between the First Amendment and privacy rights, as it applied to a narrow set of 'rather sensitive . . . criminal offenses.'"[98] The Florida Star appealed to the U.S. Supreme Court, which reversed the Florida court's decision. The Supreme Court relied on the First Amendment in finding the newspaper not liable because the State could not punish the media for releasing information that came from a government press release.[99] The Court explained that a press release indicates the "government considered dissemination lawful, and indeed expected the recipients to disseminate the information further."[100] However, the *Florida Star* Court did not sweep so far as to hold all truthful publications immune to liabil-

---

& CONTEMP. PROB. 326, 336–37 (1966) (citing several cases where courts were hesitant to apply the private facts tort).

94. *See* Kalven, Jr., *supra* note 93, at 336.
95. Florida Star v. B.J.F., 491 U.S. 524 (1989).
96. *Id.* at 527.
97. *Id.* at 528.
98. *Id.* at 528–29.
99. *Id.* at 538.
100. *Id.* at 538–39.

ity.[101] Instead, the Court limited its holding and stated that "the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case."[102]

Some have considered the *Florida Star* opinion as the end of the private facts tort.[103] Since *Florida Star* was the most recent Supreme Court decision regarding the private facts tort, the lower courts have been left with little guidance as to the scope and application of the privacy tort. Despite the *Florida Star* opinion, however, it seems that the private facts tort is resurfacing as a potential remedy for privacy regulation.[104] For example, there is an emerging pattern of judicial willingness to protect certain types of information, such as medical, financial, and intimate information under the private facts tort.[105]

This Note argues that the private facts tort could be a suitable vehicle for plaintiffs to seek damages for IoT invasions of privacy. Before the private facts tort can be applied to IoT violations, however, the plaintiff must show that the alleged IoT violation overcomes the newsworthiness defense — a powerful defense that has stemmed the development and use of this privacy tort. Several tests have developed to determine if the disclosed facts can overcome a newsworthiness defense.[106]

First, the Restatement (Second) of Torts describes a newsworthiness test that relies upon the public perception of norms and values. Specifically, to determine if a matter is of legitimate public interest to invoke the defense that it is newsworthy, the Restatement requires courts to consider the customs and conventions of the community to draw a distinction in determining what is a matter of legitimate public interest.[107] The Ninth Circuit

101. *Id.* at 532–33.

102. *Id.* at 533.

103. *See* Lorelei Van Wey, Note, *Private Facts Tort: The End is Here*, 52 OHIO ST. L.J. 299, 300 (1991) (arguing the *Florida Star* opinion ended the vitality of the private facts tort).

104. *See generally* John A. Jurata, Jr., Comment, *The Tort That Refuses to Go Away: The Subtle Reemergence of Public Disclosure of Private Facts*, 36 SAN DIEGO L. REV. 489 (1999).

105. *See infra* Part IV.A.3 and accompanying text.

106. *See* Jurata, Jr., *supra* note 104, at 502–08 (describing the five major newsworthiness tests that developed).

107. RESTATEMENT (SECOND) OF TORTS § 652D cmt. h (AM. LAW INST. 1977) ("The extent of the authority to make public private facts is not, however, unlimited. There may be some intimate details of her life, such as sexual relations, which even the actress is

adopted the Restatement approach in *Virgil v. Time*, finding that this approach does not offend the First Amendment, but rather serves as "breathing space needed by the press for the exercise of effective editorial judgment."[108] The Ninth Circuit conceded that while the distinction between "that which is of legitimate public interest and that which is not" is not as clear as one would wish, the Restatement expressed this distinction as well as any court could do, and accepted the Restatement standard.[109]

Second, Professor Diane Zimmerman coined a "leave-it-to-the-press model" that defers the newsworthy determination to the press, not the courts.[110] Professor Zimmerman claims that the press is better positioned to determine whether material is newsworthy because the media market demands news to be responsive to public desires in order to make revenue.[111] Therefore, the "[a]udience and advertiser response is more likely to restrain publishers from certain kinds of communications than the uncertain threat of an award of damages [from the private facts tort.]"[112] According to Professor Anupam Chander, however, the newsworthiness test deferring to editorial decisions of the press is suspect in the age of the Internet.[113] Professor Chander argues that in the age of the Internet, there may be no editorial review before information is released to the public, and former constraints of printing costs and limited headline space are irrelevant.[114] Instead, Professor Chander argues that "blogs are available for free to self-appointed editors" and concludes that "blogworthiness is not the same as newsworthiness."[115] Therefore, although Zimmerman's "leave-it-to-the-press model" once had

---

entitled to keep to herself. In determining what is a matter of legitimate public interest, account must be taken of the customs and conventions of the community; and in the last analysis what is proper becomes a matter of the community mores. The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.").

108. Virgil v. Time, Inc., 527 F.2d 1122, 1129 (9th Cir. 1975).

109. *Id.*

110. *See* Diane L. Zimmerman, *Requiem for A Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 353 (1983).

111. *See id.* at 353–54.

112. *Id.* at 354.

113. *See* Anupam Chander, *Youthful Indiscretion in an Internet Age*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 124, 131 (Saul Levmore & Martha C. Nussbaum eds., 2010).

114. *See id.*

115. *Id.*

greater authority, the advent of the Internet and the simultaneous decline of print news and increase in blogging seems to favor a different approach when testing for newsworthiness.

While commentators have argued that, based on *Florida Star*, many private facts are shielded by the First Amendment privilege, recent case law seems to suggest otherwise.[116] Specifically, courts seem to be more willing to curtail the strong privilege of the First Amendment in certain situations relating to medical data, financial information, and intimate sexual information involving visual and aural details.

2. *Circumstances When Courts Have Applied the Private Facts Tort*

The private facts tort has been an important remedy for the unauthorized disclosure of confidential medical information. Plaintiffs have used this tort to recover damages following the public disclosure of their illnesses, such as HIV and AIDS, as well as their autopsy photos[117] and other private medical information. For example, in *Multimedia WMAZ v. Kubach*, an AIDS patient obtained a favorable jury verdict under a private facts tort claim after a television station identified the plaintiff as being diagnosed with AIDS.[118] The television station attempted to invoke the newsworthiness privilege by claiming that the disclosure of a patient's AIDS diagnosis was a matter of public interest, but the Georgia court rejected this argument, relying on a Georgia statute that stated that "identities of those suffering from AIDS are generally not a matter of public interest."[119]

In another medical information case, *Doe v. High-Tech Institute, Inc.*, results of a student's non-consented HIV test were sent to the Colorado Department of Health by the student's college.[120]

---

116. *See generally* Jurata, Jr., *supra* note 104.

117. *See* Reid v. Pierce Cty., 961 P.2d 333, 342 (Wash. 1998) (holding plaintiffs have alleged sufficient facts to survive a motion to dismiss on a private facts tort action after autopsy photos of plaintiffs' deceased relatives were displayed).

118. Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 493 (Ga. Ct. App. 1994).

119. *Id.* at 495. Although *Kubach* relied on a state statute referring to patients with AIDS diagnoses, the Court's reasoning is still helpful because the Court considers the position of the television station. The Court considered whether the defendant had promised the plaintiff not to disclose the plaintiff's identity. Similarly, many IoT operators promise not to disclose information they obtain from consumer sensors.

120. Doe v. High-Tech Inst., Inc., 972 P.2d 1060, 1064 (Colo. App. 1998).

The college was found liable under the private facts tort.[121] Furthermore, in *Blackwell v. Harris Chemical North America, Inc.*, an employee sued her employer after her personal medical information, including detailed information of her serious illness, was disclosed to fellow employees.[122] The District Court denied the defendant employer's motion to dismiss the claim, finding that the alleged disclosure of personal medical information was sufficient to state a claim under the private facts tort.[123]

The private facts tort has also been successfully employed in a case relating to financial information. In *Hood v. National Enquirer, Inc.*, actor Eddie Murphy's illegitimate son and the son's mother sued a tabloid newspaper after an article revealed the plaintiffs' names and financial support they were receiving.[124] In an unpublished decision, the California Court of Appeals held that although Eddie Murphy's relationship with the plaintiff may be newsworthy, the details of financial support were not entitled to the First Amendment privilege.[125] Thus, restraining the publication of sensitive financial information, such as child support payments, may be another judicial limitation on the newsworthiness defense.

Finally, the private facts tort has been applied in an Internet case relating to the distribution of intimate sexual information. In *Michaels v. Internet Entertainment Group, Inc.*, celebrity Bret Michaels sued an Internet adult video distributor, claiming that its online distribution of a pornographic video depicting him having sex with actress Pamela Anderson Lee would constitute a public disclosure of private facts.[126] The defendant argued that since Michaels was a "sex symbol" because he appeared nude in magazines and movies, his sex life was no longer private.[127] Further, the defendant stated that Michael's status as a "sex symbol"

---

121. *Id.* (explaining that on appeal, the private facts liability was not contested).

122. Blackwell v. Harris Chem. N. Am., Inc., 11 F. Supp. 2d 1302, 1305 (D. Kan. 1998).

123. *Id.* at 1310.

124. Gary Williams, *On the QT and Very Hush Hush: A Proposal to Extend California's Constitutional Right to Privacy to Protect Public Figures from Publication of Confidential Personal Information*, 19 LOY. L.A. ENT. L. REV. 337, 345 (1999).

125. *See id.* ("[C]ourts have repeatedly held that even when an event is generally newsworthy, the publication of certain facts may not be such. . . . We cannot say as a matter of law that the details of a celebrity's financial support of his child and Ms. Hood are newsworthy. While the fact of that support may be newsworthy, the financial details may not.").

126. Michaels v. Internet Entm't Grp., Inc., 5 F. Supp. 2d 823, 839 (C.D. Cal. 1998).

127. *Id.* at 840.

made the sex acts depicted in the tape newsworthy.[128] The District Court rejected the defendant's arguments, finding that even though Michaels was a public figure, "even people who voluntarily enter the public sphere retain a privacy interest in the most intimate details of their lives."[129] Most importantly, the District Court focused on the "visual and aural details" of the tape, details "which are ordinarily considered private even for celebrities."[130] As a result, the District Court applied a three-prong test that considers (1) the social value of the facts published; (2) the depth of the intrusion into ostensibly private affairs; and (3) the extent to which the party voluntarily acceded to a position of public notoriety.[131] The Court found that the first two factors (insignificant social value in distributing the sex tape and significant depth of intrusion into the most intimate affairs of a relationship) weighed heavily against a finding of newsworthiness.[132] The District Court granted a preliminary injunction preventing distribution of the tape, finding that Michaels demonstrated a likelihood of success in meeting his burden of showing the tape was not covered by the newsworthiness privilege.[133]

3. *The Private Facts Tort Applied to the IoT*

As applied to the IoT, the private facts tort is a promising vehicle to help consumers recover after suffering harm related to distribution of information gathered from an IoT device. Although the newsworthiness privilege is a powerful defense, recent case law shows that courts are willing to limit the scope of newsworthiness with respect to the release of certain information, including medical information, intimate financial records, and visceral details relating to sexual relations.

First, the courts' willingness to protect medical information may extend to that of consumers injured by breaches of their health-tracking and fitness data. Arguably, data relating to HIV and AIDS, or other serious illnesses, is more substantial than heart-rate data and steps taken per day. Nevertheless, the impact of health-tracking and fitness data may be substantial when

128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.* at 841.
132. *Id.* at 841–42.
133. *Id.* at 842.

considering the data aggregation and unexpected discrimination problems.[134]

Second, smart homes, smart cars, and other IoT devices contain sensitive records that can be extremely valuable to corporations because they can lead to valuable financial inferences. For example, car insurance companies may align driving behavior with premium insurance rates.[135] Also, home insurance companies may consider data collected by smart appliances — like locking doors or turning off ovens — to reward consumers for safe practices in their household.[136] As a result, sensitive financial figures relating to insurance rates and banking information could be uncovered through IoT devices. As illustrated in *Hood v. National Enquirer, Inc.*, some courts are receptive to protecting sensitive financial information relating to child support, even if the case involves a public figure.[137] Generally, the presence of a public figure suggests that disclosed facts would be considered "newsworthy." Nevertheless, given the sensitive nature of child support financial information, the *Hood* court did not provide First Amendment protection to the distributor of this data.[138] Therefore, extending this reasoning to IoT devices, the private facts tort should allow consumers, even public figures, to claim partial remedy if their financial information is inappropriately and illegally disclosed or distributed.

Finally, and most importantly, the District Court decision in *Michaels v. Entertainment Group, Inc.*, recognized a distinct importance in protecting the "visual and aural" details of an intimate relationship between Michaels and Anderson.[139] The *Michaels* decision is the most salient case relating to IoT regulation because it involves the regulation of sensitive sensory data distributed through the Internet. Although IoT devices collect

134. *See infra* Part II.B, C.

135. *See* Sachin Modak, *The "Fin"-ternet of Things: How IoT affects Financial Services*, FINTECH FIN. BLOG (July 29, 2015) http://www.fintech.finance/news/the-fin-ternet-of-things-how-iot-affects-financial-services/ [https://perma.cc9977T-BVTW] (explaining that the emergency of telematics (in-vehicle communications devices) permits cars to transmit drivers' behavior data back to insurance companies so these companies can assess drivers' risks and premiums accordingly).

136. *See id.* (extending the previous example with car insurance to the home insurance context and considering how home owners minimize risk through behaviors collected by IoT devices such as locking doors or turning off stoves).

137. *See* Williams, *supra* note 124, at 345.

138. *See id.*

139. Michaels v. Internet Entm't Grp., Inc., 5 F. Supp. 2d 823, 840 (C.D. Cal. 1998).

sensitive sensor data, given the California district court's recognition that even celebrities deserve privacy protections relating to sensory information involving sex, this protection should extend the private facts tort to consumer harms relating to sensor data collected by IoT devices. In particular, the "visual and aural" details collected by IoT devices deserve special recognition from the courts, because this sensitive sensor data portrays aspects of private life that were impossible to record until the invention and emergence of the microelectronmechanical systems sensors in IoT devices.

Specifically, IoT devices cultivate millions of sensitive sensor data relating to aspects of life many reasonable individuals would consider private, like sleeping patterns, mental conditions, and eating habits. Further, IoT devices like smart thermostats or webcam devices — like those involved in the FTC TRENDnet action[140] — are used in the sanctuary of our homes, arguably the most private aspect of human life.[141] By allowing these devices into their homes, consumers permit the collection of sensitive sensor data, including health data like sleeping patterns or dietary information. This sensor data can be compiled in a digital biography that allows third parties to make unpermitted inferences and conclusions derived from data collected in consumer homes. Although not all IoT sensor data involves vivid information like the visual and aural details of a sex tape, there is a direct parallel between sensitive sensory data and sensitive sensor data that should be recognized by the courts, and as such, the

140. *In re* Trendnet, Inc., No. 122-3090, 2013 WL 4858250, at *2 (F.T.C. Sept. 3, 2013).

141. For the first time, the U.S. government recognized an IoT threat on February 9, 2016, when the U.S. Director of National Intelligence, James Clapper, admitted that "intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials." *See* JAMES R. CLAPPER, SENATE SELECT COMM. ON INTELLIGENCE, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 1 (2016), *available at* http://arstechnica.com/wp-content/uploads/2016/02/clappertestimony.pdf [https://perma.cc/3BEN-TYBM]; *see also* Jonathan L. Zittrain et al., *Don't Panic: Making Progress on the "Going Dark" Debate*, HARV. BERKMAN CTR. FOR INTERNET & SOCIETY 13 (2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/cy52-xezy] ("The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications."); David Kravets, *Feds don't need crypto backdoors to spy: your TV and toothbrush will do*, ARS TECHNICA (Mar. 5, 2016), http://arstechnica.com/tech-policy/2016/02/feds-dont-need-crypto-backdoors-to-spy-your-tv-and-toothbrush-will-do/ [https://perma.cc/K5N7-DFYN] (suggesting the federal government could circumvent the 2016 Apple debate concerning back-door access for Internet devices by accessing real-time, recorded communications through the IoT).

privacy torts are suitable vehicles to provide consumers with civil remedies for potential invasion of privacy harms.

If a plaintiff is successful in a privacy suit, he or she can generally recover special damages or noneconomic damages, and potentially punitive damages if the defendant's tortious conduct was particularly malicious.[142] In the IoT context, an application of the privacy torts with more-severe penalties, such as a lower threshold for punitive damages or treble damages, could serve the tort law goals of deterrence and compensating the victim. This Note does not attempt to lay out the exact framework for an invasion of privacy suit in the IoT context, but instead, attempts to emphasize the flexible and adaptable nature of privacy torts in the digital world.

B. INTRUSION UPON SECLUSION TORT

The intrusion upon seclusion (intrusion) privacy tort imposes liability on individuals who behave in an intrusive manner that violates the solitude of another, if this intrusion is highly offensive to the reasonable person.[143] This privacy tort is classified in the Restatement (Second) of Torts,[144] which provides several examples of intrusions, such as "opening [ ] private and personal mail, searching [an individual's] safe or [ ] wallet, examining [an individual's] private bank account, or compelling [an individual] by a forged court order to permit an inspection of [ ] personal documents."[145] Further, the intrusion tort does not consider the content of the information discovered.[146] For example, a "voyeur who peers through the windows and observes a mundane family scene has intruded upon the family's seclusion even though he has not learned any secrets."[147] Moreover, the intrusion tort requires that the intruder have notice of a person's reasonable expectation

142. *See* RESTATEMENT (SECOND) OF TORTS § 652H (AM. LAW INST. 1977).

143. *See id.* § 652B.

144. *Id.* (The Restatement states: "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

145. *Id.* at cmt. b.

146. Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 231 (2012).

147. *Id.*

of seclusion and intentionally make the observation despite this knowledge.[148]

Additionally, the intrusion must be by invasion into a place in which the plaintiff has secluded himself.[149] When considering a technological intrusion claim, "the fact-finder must decide whether a computer user was justified in expecting seclusion. This requires the fact-finder to determine whether an observation would interfere with solit[ude]."[150] However, this requires a fact-finder to define seclusion, which can be difficult, because definitions must strike a balance between the "remoteness every human legitimately counts on and the curiosity that every human legitimately explores."[151] For example, if seclusion were to be defined very narrowly, intrusion would become an extension of trespass law and only protect physical locations such as the home.[152] On the other hand, an expansive definition of seclusion might constrain everyone, including those conducting positive observations such as exposing crime or promoting effective journalism.[153] Professor Jane Bambauer argues that state courts are in the best position to define seclusion and "identify circumstances in which we should be able to expect seclusion while surfing the World Wide Web."[154] For these reasons, Professor Bambauer claims that the intrusion tort offers the best theory to target legitimate privacy concerns in the information age, and that the tort is "conceptually adaptable to changing technology" and "legal enforce-

148. *See id.* ("Intrusion guards our affairs from the 'prying eyes or ears of others.' It only offers a remedy when the eyes and ears are prying — that is, when an intruder has notice of a person's reasonable expectation of seclusion and intentionally makes an observation anyway. An intrusion requires a deliberate investigation.").

149. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b. (1977) ("The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs . . . .").

150. Bambauer, *supra* note 146, at 242.

151. *Id.* at 233.

152. *See id.* at 232 ("A narrow version of seclusion might prevent parabolic microphones, binoculars, and other sense-enhancing technologies that effectively transport the intruder into the home, but this is little more than a conceptual extension of a property line, and leaves out many contexts where the observed might expect and profit from respite.").

153. *See id.* at 232–33 (giving examples of positive information-gathering practices, like "the aggressive newsgathering that helped break stories about the sexual exploits of John Edwards and the investigative reporting tricks that helped expose abusive medical facilities").

154. *Id.* at 244.

ment of the right to seclusion can expand sensibly, outlawing the most disconcerting data practices without imposing unrealistic demands on industry and regulatory enforcement agencies."[155] Professor Bambauer's argument is further strengthened because the intrusion tort is not confined by the strong First Amendment limits the private facts tort faces.[156]

The discussion of the intrusion upon seclusion tort proceeds as follows. First, this Section explores some advantages the intrusion tort has over the private facts tort. Second, it discusses defenses courts have considered in intrusion tort cases. And finally, it applies the intrusion tort to the IoT.

1. *Advantages of the Intrusion Tort*

The intrusion tort has several advantages over the private facts tort for private plaintiffs. First, the intrusion tort requires only that information be observed, not disseminated.[157] For example, in *Hamberger v. Eastman*, the New Hampshire Supreme Court held an intrusion tort existed when a landlord installed a listening device in the plaintiff's bedroom.[158] The defendant contended that the "right of privacy should not be recognized on the facts of the present case . . . because there are no allegations that anyone listened or overheard any sounds or voices originating from the plaintiff's bedroom."[159] The New Hampshire Supreme Court rejected the defendant's argument because the intrusion tort "does not require publicity and communication to third persons."[160] Therefore, unlike the intrusion tort, the disclosure tort is uniquely positioned to preemptively address harms of offensive observation before collected information is disseminated.[161]

Second, since the intrusion tort monitors conduct rather than its connection to speech and the news, the intrusion tort avoids

---

155. Bambauer, *supra* note 146, at 210.

156. *See infra* Part IV.A.1.

157. *See* Bambauer, *supra* note 146, at 228 ("[I]n their haste to find a new means of controlling dissemination, privacy scholars have overlooked a tort that operates at the stage of observation — the tort of intrusion.").

158. Hamberger v. Eastman, 206 A.2d 239, 242 (N.H. 1964).

159. *Id.* at 242.

160. *Id.*

161. *See* Bambauer, *supra* note 146, at 206–07 ("The tort's focus on behavior, as opposed to content, allows intrusion to coexist comfortably with the First Amendment and other core liberal values that safeguard information exchange. The intrusion tort penalizes conduct — offensive observations — not revelations.").

the First Amendment limitations present in the private facts tort. For example, "intrusion-styled provisions in federal statutes like the U.S. Wiretap Act[162] (prohibiting the interception of conversations), the Stored Communications Act[163] (prohibiting the unauthorized access of e-mail and other electronic communications), and the Computer Fraud and Abuse Act[164] (prohibiting hacking into another's computer accounts and personal files)" have avoided First Amendment scrutiny.[165] Therefore, the intrusion tort seems adaptable to changing technology, and legal enforcement can evolve to prevent disconcerting data practices.[166]

Finally, the right to seclusion or solitude is supported by a number of different theories. According to Judge Richard Posner, communications are more effective when individuals are not concerned that someone is eavesdropping.[167] Professor Julie Cohen suggests that privacy requires "zones of personal autonomy" for the values of "self-determination and community-building."[168] And, privacy may be linked to important goals such as "creativity, growth, autonomy, and mental health."[169]

2. *Defenses to the Intrusion Tort*

There are two main defenses to the intrusion tort. First, the defendant may claim the observation or interference was not truly intrusive because the plaintiff failed to fully seclude himself or

---

162. 18 U.S.C. §§ 2510–2522 (West 2016).

163. 18 U.S.C. § 2701 (West 2016).

164. 18 U.S.C. § 1030 (West 2016).

165. *See* Bambauer, *supra* note 146, at 232.

166. *See id.* at 207 ("Intrusion has great, untapped potential to address privacy harms created by advances in information technology. Though the tort is associated with conduct in real space, its principles apply just as well to operations in the era of Big Data.").

167. *See* Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 408 (1981) ("The economic objection to eavesdropping is that its principal effect is not to obtain information — not in the long run at least — but to reduce the effectiveness of communications. Knowing that people are overhearing my conversations, I will speak less frankly. The costs of communicating will be higher. Anyone familiar with the practical consequences of allowing student observers in faculty meetings will confirm the truth of this observation.").

168. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1377 (2000) (describing privacy as a theory of individual autonomy and urging society to "take seriously a conception of data privacy that returns control over much personal data to the individual. We must carve out protected zones of personal autonomy, so that productive expression and development can have room to flourish. We can do so — constitutionally — by creating a limited right against certain kinds of commercial collection and use of personally-identified information").

169. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 444 (1980).

herself.[170] This argument depends on how broadly seclusion is defined.[171]

Second, the defendant may claim that the observed individual consented to the interference or observation.[172] For example, in *Lewis v. LeGrow*, a woman prevailed in an action involving the use of the intrusion tort against a boyfriend who secretly recorded their sexual relationship with her in his bedroom.[173] The defendant claimed that the plaintiff had consented to being videotaped.[174] On appeal, the court rejected defendant's arguments and asserted that consent "presents an issue of the degree or extent of waiver or consent granted, which depends on the facts and circumstances of the case."[175] The court stated that, generally, the issue of consent is a jury question.[176] The *LeGrow* court held that sexual intimacy is a private matter and, on the evidence presented, there was a possible factual question for the jury.[177] As a result, the trial court did not err in denying defendant's motions for summary disposition before trial.[178] Thus, the pattern of judicial willingness to protect intimate details as private matters under the private facts tort is further reflected in the intrusion case law.

3. *The Intrusion Tort Applied to the IoT*

As applied to the IoT, the intrusion tort seems like another promising vehicle for repairing consumer harm and deterring deceptive and manipulative IoT practices. Because the intrusion

---

170. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) ("The defendant is subject to liability under the rule stated in this Section only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs."); 62A Am. Jur. 2d *Privacy* § 39 (2016) ("The tort of intrusion into private matters is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the invaded place, conversation, or data source.").

171. *See infra* Part IV.B.1.

172. Lewis v. LeGrow, 670 N.W.2d 675, 688 (Mich. Ct. App. 2003) ("Like other torts, there can be no invasion of privacy under the theory of intrusion upon the seclusion of plaintiffs if plaintiffs consented to defendant's intrusion (videotaping). In the context of invasion of privacy, express or implied consent is often referred to as a waiver of the right to privacy." (citations omitted)).

173. *Id.* at 681–82.

174. *Id.*

175. *Id.* at 688.

176. *See id.*

177. *Id.*

178. *Id.* at 688–89 (holding the trial court did not err in denying defendant's motion for summary disposition before trial, or by denying defendant's motion for directed verdict).

tort is not confined by First Amendment limits and addresses conduct rather than content, this tort seems poised to become more prominent in Internet privacy controversies.[179] Being able to apply this tort to the IoT could give individuals the "breathing space to be and to act without having to worry about social and economic consequences."[180] If data is accessed for an inappropriate purpose, inconsistent with a device manufacturer's privacy policy or consumer expectations, this would lead to consumer harm in the form of potentially intrusive observation.[181] Therefore, the intrusion tort can serve as a partial remedy to protect consumer interests and deter overzealous observation by IoT devices and third parties. As a partial remedy, the privacy torts provide another vehicle of relief that can be supplemented by statutory or administrative remedies. The benefit of common law remedies, however, is that the privacy torts can adapt to changing technologies and do not impose the same burdens on regulatory agencies.

The intrusion tort can also be useful in addressing the aggregation and unexpected discrimination problems.[182] Professor Neil Richards suggests that, importantly, the intrusion tort seeks to prevent "unwanted collections or accumulations of information, rather than preventing the dissemination of already-collected information."[183] Professor Richards' comment suggests the aggregation problem can be addressed by using the intrusion tort at the observation stage to prevent an unnecessary accumulation of sensitive sensor data by IoT devices. Applying the intrusion tort at the observation stage can also address the unexpected discrimination problem, because by preventing the accumulation of personal sensor data, courts can preemptively foreclose any discrim-

179. *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, ¶ 142 (2015) (predicting that "it would not be surprising to see future privacy-related controversies give rise to more legal actions involving the tort of intrusion upon seclusion . . . .").

180. Bambauer, *supra* note 146, at 252.

181. *See id.* ("For unexposed data — data for which a user maintains a right to seclusion — the goals and designs of the Fair Information Practices are quite apt. When the personal data is used or disclosed for some purpose inconsistent with its original collection without advance notice and consent, an observation has occurred. This definition of automated observation is nearly identical to the 'respect for context' incorporated into President Obama's proposed Consumer Privacy Bill of Rights.").

182. *See infra* Part II.B.C.

183. Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 383 (2011).

inatory practices conducted by data analytics using sensor information.

IoT companies may defend their practices by pointing to privacy policies or notices that show the IoT device user consented to the challenged observation or data collection. However, courts could reject this argument because the consent waiver is limited in scope. For example, Professor Jessica Litman states that "when there is a restriction or it is implied from the terms of the consent or the circumstances, the consent may be regarded as conditioned upon the purpose, and it confers no privilege to do the same act for a different purpose."[184] Professor Litman's argument suggests that information privacy does not permit inappropriate, cross-contextual use for data that is not consented to in the original agreement.[185] Therefore, even if the privacy policy can insulate the defendant from contract claims, a tort claim still exists because tortious consent requires the "subject [to] appreciate the act that she consents to and be in fact willing that it occur."[186] Professor Litman argues that consent in tort law doesn't "depend on formalities like opt-in or opt-out" provisions and therefore maintains a distinct advantage from its common-law cousins, property and contract law.[187] By avoiding the need for contract formalities that are included in modern privacy policies, tort law possesses an adaptable characteristic that could be used to address modern privacy concerns. As a result, the intrusion tort is a possible remedy for the aggregation and unexpected discrimination problems that come with the IoT.

In the Internet context, notices and agreements, especially those found in privacy policies and End User Licensing Agreements, may "expand the scope of observation beyond what courts

184. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1310–11 (2000).

185. *See id.* at 1311 ("One important form of restriction is the limitation of the consent to acts done for a particular purpose. When there is a restriction or it is implied from the terms of the consent or the circumstances, the consent may be regarded as conditioned upon the purpose, and it confers no privilege to do the same act for a different purpose.").

186. *Id.* ("What counts or should count as effective consent has been one of the most contentious issues in the privacy debate. . . . Here, too, tort law has an edge over its common law cousin, property, because tort law has a finely developed jurisprudence of consent. The tort law version of consent doesn't depend on formalities like opt-in or opt-out. Rather it requires that the subject appreciate the act that she consents to and be in fact willing that it occur.").

187. *Id.*

would otherwise consider to be appropriate."[188] For this reason, courts may be in the best position to clarify the extent and effectiveness of IoT privacy policies before the technology industry creates a custom of intrusive observation.[189]

V. CONCLUSION

This Note explores the unique dangers the IoT poses, describes the current IoT regulatory framework, and advocates for the increased use of privacy torts as a potential remedy for IoT-induced consumer harms. The private facts and intrusion tort regulate different aspects of Internet interaction and can be applied in conjunction with privacy statutes and FTC enforcement. Applying the private facts tort poses a difficult challenge in that plaintiffs must overcome First Amendment concerns in the form of the newsworthiness test, and the intrusion tort leaves questions about how to define the circle of seclusion in which plaintiffs should be protected. Nevertheless, given the adaptable nature of tort law, courts should recognize the sensitive nature of sensor data as a distinct set of information deserving of judicial protection through increased use of privacy torts. To achieve this goal, this Note hopes to persuade the American Law Institute to consider emerging technologies — specifically, the IoT — when drafting the next Restatement of Torts, by including clear examples or commentary that address the sensitive nature of sensor data.

Society has reached a technological milestone requiring the special attention of the law, as we have entered a digital era where every device and every physical object surrounding us can be connected to the Internet. Soon, every human experience and physical sensation will be recorded and transmitted across the Internet for a variety of purposes. The growing presence of the

---

188. Bambauer, *supra* note 146, at 254 ("Today private industry places considerable faith in their privacy policies and End User Licensing Agreements ('EULAs') to define the scope of their duties. Boilerplate formalities of this sort might suffice to limit the scope of contract liability, but they are not sufficient to constitute consent to conduct that would otherwise be tortious. Consent is not assent. Consent requires acts that manifest an objective expectation that the would-be tort victim is willing for the tortious conduct to occur.").

189. For example, if IoT companies continue to add language into their contractual agreements that permits more intrusion, within the next decade, IoT companies may raise defenses in litigation by pointing to numerous examples of contractual language permitting their observation or unlawful conduct. In this way, IoT companies may create an "industry norm" and shift consumer expectations of privacy.

IoT should motivate the legal community to prepare for this exciting, yet frightening digital frontier and the privacy challenges that will accompany its arrival.