REGULATING THE INTERNET OF THINGS: FIRST STEPS TOWARDS MANAGING DISCRIMINATION, PRIVACY, SECURITY & CONSENT

By Scott R. Peppet*

Forthcoming Texas Law Review (2014)

The consumer "Internet of Things" is suddenly reality, not science fiction. Electronic sensors are now ubiquitous in our smart phones, cars, homes, electric systems, health care devices, fitness monitors, and workplaces. These connected sensor-based devices create new types and unprecedented quantities of detailed, high-quality information about our everyday actions, habits, personalities and preferences. Much of this undoubtedly increases social welfare. For example, insurers can price automobile coverage more accurately by using sensors to measure exactly how you drive (e.g., Progressive's SnapShot system), which should theoretically lower the overall cost of insurance. But the Internet of Things raises new and difficult questions as well. This Article shows that four inherent aspects of sensor-based technologies—the compounding effects of what computer scientists call "sensor fusion," the near impossibility of truly de-identifying sensor data, the likelihood that Internet of Things devices will be inherently prone to security flaws, and the difficulty of meaningful consumer consent in this context—create very real discrimination, privacy, security, and consent problems. As connected, sensor-based devices tell us more and more about ourselves and each other, what discrimination—racial, economic, or otherwise—will that permit, and how should we constrain socially-obnoxious manifestations? As the Internet of Things generates ever more massive and nuanced data sets about consumer behavior, how to protect privacy? How to deal with the reality that sensors are particularly vulnerable to security risks? And how should the law treat—and how much should policy depend upon—consumer consent in a context in which true informed choice may be impossible? This Article is the first legal work to describe the new connected world we are creating, address these four interrelated problems, and propose concrete first steps for a regulatory approach to the Internet of Things.

INTRODUCTION

I. THE INTERNET OF THINGS 12
A. Health & Fitness Sensors 13
i. Countertop Devices 13
ii. Wearable Sensors 15
iii. Intimate Contact Sensors 16
iv. Ingestible & Implantable Sensors 16
B. Automobile Sensors 17
i. Event Data Recorders (or "Black Boxes") 17

* Professor of Law, University of Colorado School of Law. I am grateful to the faculty of the University of Colorado Law School for their input, and particularly to Paul Ohm & Harry Surden for their thoughts. I also thank the participants at the Federal Trade Commission's Internet of Things Workshop (November 19, 2013), who gave helpful comments on many of these ideas. Finally, thank you to my research assistants Carey DeGenero and Brian Petz for their help.

Electronic copy available at: http://ssrn.com/abstract=2409074

ii. Consumer Automobile Sensors 18
iii. Auto Insurance Telematics Devices 19
C. Home & Electricity Sensors 20
i. The Smart Home 20
ii. The Smart Grid 21
D. Employee Sensors 23
E. Smart Phone Sensors 25

II. FOUR PROBLEMS 27
A. Discrimination 28
i. The Technical Problem: Sensor Fusion & Big Data Analytics May Mean that Everything Reveals Everything 28
ii. The Legal Problem: Antidiscrimination and Credit Reporting Law is Unprepared 34
B. Privacy 38
i. The Technical Problem: Sensor Data Are Particularly Difficult to De-Identify 38
ii. The Legal Problem: Privacy Law is Unprepared 41
C. Security 42
i. The Technical Problem: Internet of Things Devices May Be Inherently Prone to Security Flaws 43
ii. The Legal Problem: Data Security Law is Unprepared 45
D. Consent 48
i. The Technical Problem: Sensor Devices Confuse Notice and Choice 49
ii. The Legal Problem: Consumer Protection Law is Unprepared 54

III. FOUR (MESSY & IMPERFECT) FIRST STEPS 56
A. A Regulatory Blueprint for the Internet of Things 57
i. Dampening Discrimination With Use Constraints 57
ii. Protecting Privacy by Redefining Personally Identifiable Information in This Context 64
iii. Protecting Security by Expanding Data Breach Notification Laws 65
iv. Improving Consent by Guiding Internet of Things Disclosures 67
B. Seize the Moment: Why Public Choice Problems Demand Urgency 71

CONCLUSION

APPENDIX A: INTERNET OF THINGS PRIVACY POLICIES

Electronic copy available at: http://ssrn.com/abstract=2409074

> "Every animate and inanimate object on earth will soon be generating data, including our homes, our cars, and yes, even our bodies."[1]
>
> -- The Human Face of Big Data (2012)

> "Very soon, we will see inside ourselves like never before, with wearable, even internal, sensors that monitor even our most intimate biological processes. It is likely to happen even before we figure out the etiquette and laws around sharing this knowledge."[2]
>
> -- New York Times (2012)

> "[A]ll data is credit data, we just don't know how to use it yet. … Data matters. More data is always better."
>
> -- Douglas Merill, Google's former CIO & CEO of ZestFinance[3]

INTRODUCTION

The Breathometer is a small, black, plastic device that plugs into the headphone jack of an Android or iPhone smartphone.[4] Retailing for $49, the unit contains an ethanol sensor to estimate blood alcohol content from the breath. The company's web site advertises that the device will give you "the power to make smarter decisions when drinking."[5] The device works only in conjunction with the downloadable Breathometer application, which both displays the results of any given test and shows a user's longitudinal test history.

The Breathometer is representative of a huge array of new consumer devices that have exploded onto the market in the last twelve to eighteen months, promising to measure, record, and analyze different aspects of daily life.[6] For example, a Fitbit bracelet or Nike Fuel Band can track the steps you take in a day, calories burned, and minutes asleep. A Basis sports watch will track your heart rate, a Withings cuff will graph your blood pressure on your mobile phone or tablet, an iBGStar iPhone add-on will monitor your blood glucose levels, a Scanadu Scout will measure your temperature, heart rate, and hemoglobin levels, an Adidas Smart Ball will track your soccer performance, a UVeBand or June bracelet will monitor your daily exposure

---

[1] RICK SMOLAN & JENNIFER ERWITT, THE HUMAN FACE OF BIG DATA 3 (2012).
[2] Quentin Hardy, *Big Data in Your Blood*, N.Y. TIMES (Sep. 7, 2012).
[3] Quentin Hardy, *Just the Facts. Yes, All of Them.*, N.Y. TIMES (Mar. 24, 2012). *See also* ZESTFINANCE, http://www.zestfinance.com/how-we-do-it.html (touting the firm's philosophy that "All Data is Credit Data").
[4] *See* http://www.breathometer.com.
[5] *Id.*
[6] For description of each of these devices and citations to relevant product web sites, see Part I(A)-(E), *infra*.

to ultraviolet rays and notify your smartphone if you need to reapply sunscreen, a Smart Helmet by LifeBeam will track your heart rate, blood flow, and oxygen saturation as you cycle, a MimoBaby "onesie" shirt will monitor your baby's sleep habits, temperature and breathing patterns, a W/Me bracelet from Phyode will track changes in your autonomic nervous system to detect mental state (e.g., passive, excitable, pessimistic, anxious, balanced) and ability to cope with stress, and a Melon or Muse headband can measure brain activity to track your ability to focus. Other devices—such as the popular Nest Thermostat, SmartThings' home automation system, the Automatic Link driving and automobile monitor, GE's new line of connected ovens, refrigerators, and other appliances, and Belkin's WeMo home electricity and water usage tracker—can in combination measure your driving habits, kitchen appliance use, home electricity and water consumption, and even work productivity.[7]

Together these devices create the "Internet of Things,"[8] or what some have more recently called the "Internet of Everything."[9] Conservative estimates suggest that over 200 billion connected sensor devices will be in use by 2020,[10] with a market size of roughly $2.7-6.2 trillion per year.[11] These devices promise important efficiency, social and individual benefits through quantification and monitoring of previously immeasurable qualities. But the Internet of Things also raises a host of difficult questions. Who owns the data these sensors generate? How can such data be used? Are such devices, and the data they produce, secure? And are consumers aware of the legal implications that such data create—such as the possible use of such data by an adversary in court, an insurance company when denying a claim, an employer determining whether to hire, or a bank extending credit?

Return to the Breathometer example. When you purchase a Breathometer—as I did recently for purposes of researching this Article—it arrives in a small stylish black box featuring an image of the device and the motto "Drink Smart. Be Safe." Opening the packaging reveals both the device and a small user's manual that explains how to download the Breathometer app, create an account with the company through that app, and plug the Breathometer into one's smartphone. Nowhere in that manual's seventeen pages is there mention of a privacy policy that might apply to the

---

[7] *See* Part I(A)-(E) for discussion of these devices.

[8] The term is generally attributed to Kevin Ashton. *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (Jun. 22 2009) (claiming that the first use of the term was in a 1999 presentation by Ashton). *See also* NEIL GERSHENFELD, WHEN THINGS START TO THINK (1999). For a useful overview of the Internet of Things, see Melanie Swan, *Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, J. SENSOR & ACTUATOR NETWORKS 217 (2012).

[9] The phrase "Internet of Everything" seems to originate with Cisco's CEO John Chambers. *See* http://www.internetofeverything.cisco.com.

[10] *See* Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME (Jan. 13, 2014) (citing study by market researcher IDC).

[11] *See* MCKINSEY & COMPANY, DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 51 (May 2013).

data generated by the device. Nor is there explanation of what data the device generates (e.g., "just" blood alcohol content or also other sensor information?), where such data are stored (e.g., in one's phone or on the company's servers in the cloud?), whether such data can be deleted and how, or how the company might use such data (e.g., will the company sell it; could it be subpoenaed through a court process?). When installing the Breathometer app through the Apple App Store, no mention is made of any privacy policy. No pop-up with such a policy occurs when the user creates an account through the app or starts using the device. In short, the data-related aspects of the device are completely absent from the user experience. Only by visiting the company's web site, scrolling to the very bottom, and clicking the small link for "Privacy Policy" can one learn that one's blood alcohol test results are being stored indefinitely in the cloud, cannot be deleted by the user, may be disclosed in a court proceeding if necessary, and may be used to tailor advertisements at the company's discretion.[12]

Given the many potentially troubling uses for breathalyzer data—think employment decisions, criminal implications, and health, life, or car insurance ramifications—one might expect data-related disclosures to dominate the Breathometer user's purchasing and activation experience. Instead, the consumer is essentially led to the incorrect assumption that this small black device is merely a good like any other—akin to a stapler or ball point pen—rather than a data source and cloud-based data repository.[13]

Even Internet of Things devices far more innocuous than a Breathometer can generate data that present difficult issues. Sensor data capture incredibly rich nuance about who we are, how we behave, what our tastes are, and even our intentions. Once filtered through Big Data analytics,[14] these data are the grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities. I can tell a lot about you if I know that you often leave your oven on when you leave the house, fail to water your plants, don't exercise, or drive recklessly.[15] As Federal Trade Commission (FTC) Commissioner Julie Brill recently stated,

> "On the Internet of Things, consumers are going to start having devices, whether it's their car, or some other tool that they have, that's connected and sending information to a

[12] *See* http://www.breathometer.com/legal/privacy-policy.
[13] *See* ADRIAN MCEWEN & HAKIM CASSIMALLY, DESIGNING THE INTERNET OF THINGS 294 (2013) ("[M]any 'things' have little in their external form that suggests they are connected to the Internet. When you grab an Internet-connected scarf from the coat rack or sit on an Internet-connected chair, should you have some obvious sign that data will be transmitted or an action triggered?").
[14] For a discussion of Big Data practices, see Omer Tene & Jules Polonetsky, *Big Data For All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013) (providing overview).
[15] *See* Part I (describing Internet of Things devices for each of these functions).

> number of different entities, and the consumer may not even realize that they have a connected device or that the thing that they're using is collecting information about them."[16]

These are the real challenges of the Internet of Things: what information do these devices collect, how might that information be used, and what—if any—real choice do consumers have about such data?

To date, the law has left these questions unanswered. Consider a second preliminary example. Roughly ninety percent of automobiles in the United States contain an Event Data Recorder (EDR) or "black box."[17] By Federal law, such devices must store a vehicle's speed, how far the accelerator pedal is pressed, whether the brake is applied, whether the driver is using a seat belt, crash details, and other information, including, in some cases, the driver's steering input and occupant sizes and seat positions.[18] Such data can convict unsafe drivers[19] and help regulators improve safety.[20] But many policy questions remain unanswered or only partially addressed. Can an insurance company, for example, ex ante require an insured to grant access to EDR data in the insured's policy, or ex post condition claim payment on such access? The National Highway Traffic Safety Administration (NHTSA) has left who owns EDR data—the car owner, the manufacturer, the insurer—to the states, but only thirteen states have addressed the issue.[21] Four states currently forbid insurance companies from requiring that an insured consent to future disclosure of EDR data, or from requiring access to EDR data as a condition of settling an insurance claim.[22] One state—Virginia—also forbids an insurer from adjusting rates solely based on an insured's refusal to provide EDR data.[23] Should other states

[16] Speech by FTC Commissioner Julie Brill, Silicon Flatirons Conference, The New Frontiers of Privacy Harm (Jan. 17, 2014).
[17] National Highway Traffic Safety Administration. Final Regulatory Evaluation, Event Data Recorders, Table III-1 (July 2006).
[18] National Highway Traffic Safety Administration, Final Rule. Docket NHTSA-2006-25666. 49 CFR Part 563.
[19] Matos v. Florida, 899 So.2d 403 (2005).
[20] *See* H. CLAY GABLER, JOHN HINCH & JOHN STEINER, EVENT DATA RECORDERS: A DECADE OF INNOVATION (2008) (providing examples).
[21] *See* National Highway Traffic Safety Administration, Final Rule. Docket NHTSA-2006-25666. 49 CFR Part 563 ("This rule does not address certain other issues generally within the realm of State law, such as whether the vehicle owner owns the EDR data, how EDR data can be used/discovered in civil litigation, how EDR data may be used in criminal proceedings, whether EDR data may be obtained by the police without a warrant, whether EDR data may be developed into a driver-monitoring tool, and the nature and extent that private parties (including insurance companies, car rental companies, and automobile manufacturers) will have or may contract for access to EDR data. These issues are instead being addressed by State legislatures.").
[22] *See* Ark. Code § 23-112-107; N.D. Cent. Code § 51-07-28; Ore. Rev. Stat. §§ 105.925-.948; Va. Code § 38.2-2212(C)(s).
[23] Va. Code § 38.2-2213.1 ("No insurer … shall reduce coverage, increase the insured's premium, apply a surcharge, refuse to apply a discount …, place in a less favorable tier, refuse to place in the company's best tier … solely because a motor vehicle owner refuses to allow an insurer access to recorded data … from a recording device ….").

follow? Should Congress give Federal guidance on such uses of EDR data? Is such fine-grained information invasive of privacy—particularly given that consumers cannot easily turn off or "opt out" of its collection? And as more sophisticated car sensors reveal even more sensitive information—where we drive, when we drive, how we drive—that permits deeper inferences about us—how reckless, impulsive, or quick to anger we are—how will we regulate the use of such data? For example, should a bank be able to deny your mortgage application because your EDR data reveals you as an irresponsible driver and thus a bad credit risk? Should a potential employer be able to factor in a report based upon your driving data when deciding whether to hire you?

In beginning to answer these questions, this Article makes three claims about the Internet of Things—all new to the legal literature, all important, and all timely.

First, the sensor devices that together make up the Internet of Things are not a science fiction future but a present reality. Internet of Things devices have proliferated before we have had a chance to consider whether and how best to regulate them. Sales of fitness trackers such as FitBit and Nike FuelBand topped $300 million last year, and consumer sensor devices dominated the January 2014 International Consumer Electronics Show. The hype is real: such devices are revolutionizing personal health, home security and automation, business analytics, and many other fields of human activity. The scant legal work addressing such devices has largely assumed, however, that the Internet of Things is still in its infancy in a research laboratory, not yet ready for commercial deployment at scale.[24] To counter this misperception and lay the foundation for considering the current legal problems created by the Internet of Things, Part I presents a typology of types of consumer sensors and provides examples of the myriad ways in which existing Internet of Things devices generate data about our environment and our lives.

Second, the Internet of Things suffers from four unique technical challenges that in turn create four legal problems of discrimination, privacy, security and consent. This is the heart of the Article's argument, and it is the four-pronged focus of Part II.

First, Part II(A) explores the ways in which the Internet of Things may create new forms of discrimination—including both racial or protected class discrimination and economic discrimination—by revealing so much information about consumers. Computer scientists have long known that the phenomenon of "sensor fusion" dictates that the information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation. Just as two eyes generate

[24] *See e.g.,* Jerry Kang et al., *Self-Surveillance* Privacy, 97 IOWA L. REV. 809 (2012) (discussing sensors but largely focusing on early research examples rather than commercial).

depth of field that neither eye alone can perceive, two Internet of Things sensors may reveal unexpected inferences. For example, in combination a fitness monitor's separate measurements of heart rate and respiration can reveal not only a user's exercise routine, but also cocaine, heroin, tobacco, and alcohol use, each of which produces unique biometric signatures.[25] Sensor fusion means that on the Internet of Things, "every thing may reveal everything." By this I mean that each type of consumer sensor (e.g., personal health monitor, automobile black box, smart grid meter) can be used for many purposes beyond that particular sensor's original use or context, particularly in combination with data from other Internet of Things devices. Soon we may discover that we can infer whether you are a good credit risk or likely to be a good employee from driving data, fitness data, home energy use, or your smart phone's sensor data.

This makes each Internet of Things device—however seemingly small or inconsequential—important as a policy matter, because any device's data may be used in far-removed contexts to make decisions about insurance, employment, credit, housing, or other sensitive economic issues. Most troubling, this creates the possibility of new forms of racial, gender, or other discrimination against those in protected classes if Internet of Things data can be used as hidden proxies for such characteristics. In addition, such data may lead to new forms of economic discrimination as lenders, employers, insurers, and other economic actors use Internet of Things data to sort and treat differently unwary consumers. Part II(A) explores the problem of discrimination created by the Internet of Things, and the ways in which both traditional discrimination law and privacy statutes such as the Fair Credit Reporting Act (FCRA)[26] are currently unprepared to address these new challenges.

Part II(B) considers the privacy problems of these new technologies. The technical challenge here is that Internet of Things sensor data are particularly difficult to de-identify or anonymize. The sensors in Internet of Things devices often have entirely unique "fingerprints"—each digital camera, for example, has its own signature imperfections and irregularities.[27] Moreover, even when identifying characteristics such as name, address, or telephone number are removed from Internet of Things data sets, such sensor data are particularly vulnerable to re-identification. A recent MIT study showed, for example, that it is far easier than expected to re-identify "anonymized" cell phone users, and other computer science work has likewise shown that Internet of Things sensor devices are particularly prone to such attacks. Unfortunately, privacy law is not prepared to deal with this threat of easy re-identification of Internet of Things information, instead relying on the outdated assumption that one can usefully distinguish between "personally identifiable information" and de-identified sensor or

[25] *See* Part II(A).
[26] Fair Credit Reporting Act, 15 U.S.C. 1681 *et. Seq* (1970).
[27] *See* Part II(B).

biometric data. Part II(B) shows that this may no longer be viable on the Internet of Things.

Part II(C) then turns to the unique data security problems posed by the Internet of Things. The technical challenge is simple: many Internet of Things products have not been engineered to protect data security. These devices are often created by consumer goods manufacturers, not computer software or hardware firms. As a result, data security may not be top of mind for current Internet of Things manufacturers. In addition, the small form factor and low power and computational capacity of many of these Internet of Things devices makes adding encryption or other security measures difficult. Recent attacks—such as a November 2013 attack that took control of over one hundred thousand Internet of Things web cameras, appliances, and other devices—highlight the problem. Data security researchers have found vulnerabilities in Fitbit fitness trackers, Internet-connected insulin pumps, automobile sensors and other products.[28] Unfortunately, both current FTC enforcement practices and state data breach notification laws are unprepared to address Internet of Things security problems. In particular, were Fitbit, Nike, Nest Thermostat, or any other Internet of Things manufacturer to have users' sensitive sensor data stolen, *no* existing state data breach notification law would currently require public disclosure or remedy of such a breach.[29]

Next, Part II(D) considers the ways in which consumer protection law is also unprepared for the Internet of Things. In particular, I present the first survey in the legal literature of Internet of Things privacy policies, and show the ways in which such policies currently fail consumers.[30] Internet of Things devices generally have no screen or keyboard, and thus giving consumers data and privacy information and an opportunity to consent is particularly challenging. Current Internet of Things products often fail to notify consumers about how to find their relevant privacy policy, and once found such policies are often confusing, incomplete, and misleading. My review shows that such policies rarely clarify who owns sensor data, exactly what biometric or other sensor data a device collects, how such data are protected, and how such information can be sold or used. Both state and federal consumer protection law has not yet addressed these problems or the general issues that the Internet of Things creates for consumer consent.

Part II's focus on these four problems of discrimination, privacy, security, and consent concludes with a fairly dismal warning to regulators, legislators, privacy and consumer advocates, and corporate counsel: current discrimination, privacy, data security, and consumer protection law is unprepared for the Internet of Things, leaving consumers exposed in a host of ways as they begin to use these new devices. Absent regulatory action to

[28] *See* Part II(C) (discussing various security attacks).
[29] *See* Part II(C).
[30] *See* Part II(D) and Appendix A.

reassure and protect consumers, the potential benefits of the Internet of Things may be eclipsed by these four serious problems.

My third argument, therefore, is that state and federal legislators and regulators should take four preliminary steps to begin to guide the Internet of Things. This argument—in Part III—is the Article's most difficult. I could easily prescribe a comprehensive new Federal statute or the creation of a new oversight agency, but such approaches are simply implausible given current political realities. Vague prescriptions—such as calling for greater consumer procedural protections or due process—would also sound good without offering much immediate or practical progress. Yet real, operational prescriptions are challenging, in part because my goal in Part II is to provide a comprehensive map of the four major problems generated by the Internet of Things rather than focus on merely one aspect such as security or consent. Put simply, if Part II's description of the challenges we face is broad and accurate enough, proposing realistic prescriptions in Part III is necessarily daunting.

Nevertheless, Part III begins to lay out a regulatory blueprint for the Internet of Things. I take four prescriptive positions. First, new forms of discrimination will best be addressed through substantive restrictions on certain uses of data, not through promises to consumers of procedural due process. I therefore propose extending certain state laws that inhibit use of sensor data in certain contexts, such as statutes prohibiting insurers from conditioning insurance on access to automobile event data recorder data.[31] Although this approach is at odds with much information privacy scholarship, I argue that use constraints are necessary to prevent obnoxious discrimination on the Internet of Things. Second, biometric and other sensitive sensor data created by the Internet of Things should be considered potentially personally identifiable information, even in supposedly de-identified forms. I show how regulators and corporate counsel should therefore reconsider the collection, storage, and use of such data.[32] Third, we should at least protect sensor data security by broadening state data breach notification laws to include such data within their scope, and should create substantive security guidelines for Internet of Things devices. Although regulators may currently lack legislative authority to strictly enforce such guidelines, they can use their "soft" regulatory power to create industry consensus on best practices for Internet of Things security.[33] Finally, we should rigorously pursue Internet of Things firms for promulgating incomplete, confusing, and sometime deceptive privacy policies, and should provide regulatory guidance on best practices for securing meaningful consumer consent in this difficult context.[34] Having shown in Part II the many ways in which notice and choice is currently failing on the Internet of

[31] *See* Part III(A)(i).
[32] *See* Part III(A)(ii).
[33] *See* Part III(A)(iii).
[34] *See* Part III(A)(iv).

Things, I suggest several concrete privacy policy changes for regulators and corporate counsel to take up.

I do not pretend that these steps will solve every problem created by the Internet of Things. I aim to begin a conversation that is already overdue. Although some privacy scholarship has mentioned the proliferation of sensors,[35] none has systematically explored both the problems and opportunities the Internet of Things creates.[36] Some have explored particular contexts but not the complexity of the Internet of Things.[37] In a recent article, I highlighted the increase of such sensor data without offering analysis of how to address its proliferation.[38] Even computer science is just beginning to focus on the problems created by widespread use of consumer sensor devices,[39] as are regulators—the Federal Trade Commission (FTC) recently held its first workshop on the Internet of Things to solicit input on the privacy problems sensors create and how to address such issues.[40] This Article begins to fill this gap.

Before we begin, let me highlight four things I am *not* focused upon here. First, I am not talking about industrial or commercial sensors deployed

---

[35] *See e.g.,* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321 (2007) (focusing primarily on cameras and surveillance, rather than the commercial availability of many different types of sensors); A. Michael Froomkin, *The Death of Privacy?*, 52 STANFORD L. REV. 1461, 1493-96 (2000) (forecasting the rise of biometric, home, and vehicle tracking). Much scholarship focused on other privacy issues at least mentions sensors. *See e.g.,* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1940 (2013) (focusing on various types of government surveillance but noting that "the next fifteen [years] will likely herald the 'Internet of Things,' in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control.").

[36] *See e.g.,* Kang et al., *supra* note __; Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65 (focusing in part on sensors); Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93 (2005). Some forthcoming scholarship is beginning to focus on the Internet of Things. *See e.g.,* John Gudgel, *Objects of Concern? Risks, Rewards and Regulation in the 'Internet of Things'*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430780;

[37] *See e.g.,* Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHIC.-KENT L. REV. 161 (2013); Karin Mika, *The Benefit of Adopting Comprehensive Standards of Monitoring Employee Technology Use in the Workplace*, CORNELL HR REV. (2012); Kevin L. Doran, *Privacy and Smart Grid: When Progress and Privacy Collide,* 41 U. TOL. L. REV. 909 (2010); Patrick R. Mueller, Comment, *Every Time You Brake, Every Turn You Make—I'll be Watching You: Protecting Driver Privacy in Event Data Recorder Information*, 2006 WIS. L. REV. 135.

[38] See Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future*, 105 NW. UNIV. L. REV. 1153, 1167-1173 (2011).

[39] *See e.g.,* Andrew Raij et al., *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, ACM 11, 11 (2011) ("[L]ittle work has investigated the new privacy concerns that emerge from the disclosure of measurements collected by wearable sensors.").

[40] *See* FTC, Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013), available at http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

in factories, warehouses, ports, or other work spaces that are designed to keep track of machinery and production. This is an important part of the Internet of Things, but this Article focuses primarily on consumer devices. Second, I am not talking in general about ambient sensor devices used in an environment to capture information about the use of that space, such as temperature sensors. Such ambient informatics also creates difficult privacy and regulatory issues, but those are beyond our scope here. Third, I am not talking about the government's use of sensor data and the Constitutional issues that arise from such use. Future work will have to address how to deal with a governmental subpoena of FitBit or whether the National Security Agency (NSA) can or does track consumer sensor data.[41] Fourth, I am not talking about the privacy concerns that a sensor I am wearing might create for *you* as you interact with me. My sensor might sense and record your behavior, as when a cell phone's microphone records my speech but also yours, thus creating a privacy concern for you. Instead, here I focus on the issues raised for users themselves. Each of these other problems is a worthwhile topic for future work.

I. THE INTERNET OF THINGS

Microelectromechanical systems (MEMS) sensors translate physical phenomenon, such as movement, heat, pressure, or location, into digital information.[42] MEMS were developed in the 1980s, but in the last few years the cost of such sensors has dropped from twenty-five dollars to less than a dollar per unit.[43] These sensors are thus no longer the stuff of experimental laboratories; they are incorporated into consumer products available at scale. Some estimate that by 2025 over one *trillion* sensor-based devices will be connected to the Internet or each other.[44]

Part I aims to describe the Internet of Things technologies currently available to consumers. It overviews five types of Internet of Things devices: health and fitness sensors, automobile black boxes, home monitors

---

[41] *See e.g.,* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1940 (2013) ("[T]he next fifteen [years] will likely herald the 'Internet of Things,' in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control."); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012) (focusing on the constitutional problems of using facial recognition and other biometric technologies in law enforcement).

[42] A sensor is defined as "a device that receives a stimulus and responds with an electrical signal." JACOB FRADEN, HANDBOOK OF MODERN SENSORS: PHYSICS, DESIGNS, AND APPLICATIONS 2 (4th ed. 2010).

[43] *See* Alexander Wolfe, *Little MEMS Sensors Make Big Data Sing*, FORBES (Jun. 10, 2013) ("With the cost impediment overcome, deployment has caught fire.").

[44] *See* Bill Wasik, *Welcome to the Programmable World*, WIRED (May 14, 2013), http://www.wired.com/gadgetlab/2013/05/internet-of-things/.

and smart grid sensors, devices designed specifically for employee monitoring, and software applications that make use of the sensors within today's smart phones. Together, these consumer products change fundamentally our knowledge of self, other, and environment.

A. HEALTH & FITNESS SENSORS

There are five basic types of personal health monitors, in order from least physically invasive to most invasive: (1) countertop devices (such as a blood pressure monitor or weight scale); (2) wearable sensors (such as an arm or wrist band); (3) intimate contact sensors (such as a patch or electronic tattoo); (4) ingestible sensors (such as an electronic pill); and (5) implantable sensors (such as a heart or blood health monitor).[45] Each is already deployed commercially, and the market for health and wellness sensors has exploded in the last twelve to eighteen months. Mobile healthcare and medical app downloads are forecast to reach 142 million in 2016, up from 44 million in 2012,[46] creating a market worth $26 Billion by 2017.[47] Over 30 million wireless wearable health devices—such as FitBit or Nike FuelBand—were sold in 2012, and that figure was expected to increase to 48 million in 2013.[48]

i. Countertop Devices. Countertop devices include weight scales, blood pressure monitors, and other products meant to be used occasionally to track some aspect of health or fitness. The Aria[49] and Withings[50] scales, for example, are WiFi-enabled smart scales that can track weight, body fat percentage, and Body Mass Index (BMI). Each can email you your weight loss progress. Withings similarly manufactures a blood pressure cuff that synchronizes with a smartphone.[51] The software application accompanying the device graphs your blood pressure over time and can email results to you or your physician. Similarly, the iBGStar blood glucose monitor connects to an iPhone to track blood sugar levels over time,[52] and Johnson & Johnson's One Touch Verio sensor can upload such data to an iPhone wirelessly over

---

[45] *See* George Skidmore, *Ingestible, Implantable, or Intimate Contact: How Will You Take Your Microscale Body Sensors?*, http://singularityhub.com/2013/05/13/ingestible-implantable-or-intimate-contact-how-will-you-take-your-microscale-body-sensors/. For an overview, see D. Konstantas, *An Overview of Wearable and Implantable Medical Sensors*, IMIA YEARBOOK OF MED. INFORMATICS 66, 67-69 (2007) (describing sensor-filled clothing, patch sensors, and implantable sensors).

[46] *See* Partrick J. Skerrett, *The Potential of Remote Health Monitoring at Work*, HARVARD BUS. REV. (Dec. 9, 2009) *available at* http://blogs.hbr.org/health-and-well-being/2009/12/the-potential-of-remote-health.html.

[47] http://www.research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/

[48] http://www.abiresearch.com/press/sports-and-wellness-drive-mhealth-device-shipments

[49] *See* http://www.fitbit.com/aria.

[50] *See* http://www.withings.com/scales.

[51] *See* http://www.withings.com/en/bloodpressuremonitor.

[52] *See* http://www.ibgstar.us/.

BlueTooth.[53] Likewise, the Propeller Health sensor-based asthma inhaler tracks the time and place you use your asthma medication and wirelessly sends that information to your smartphone.[54] The accompanying application allows you to view your sensor data and create an asthma diary.

Countertop devices are a fast-growing and rapidly-advancing product sector. For example, the Scanadu Scout is a small countertop device that a user briefly holds up to the forehead to take measurements. It tracks vital signs such as heart rate, body temperature, oximetry (the oxygen in arterial blood), respiratory rate, blood pressure, electrocardiography (ECG), and emotional stress levels.[55] Such comprehensive home measurement was unthinkable even two years ago. Even more dramatic, Scanadu is developing a home uranalysis device—called the Scanadu Scanaflow—that measures glucose, protein, leukocytes, nitrates, blood, bilirubin, specific gravity, and pH in the urine.[56] It can also test for pregnancy. Again, such analysis is entirely novel for the home consumer market.

Sensor-laden countertop consumer products are becoming more diverse and creative as manufacturers invent new ways to capture data from the objects and environments with which we interact. Podimetrics makes a sensor-driven floor mat that helps diabetic patients detect foot ulcers.[57] AdhereTech makes an Internet-enabled pill bottle that tracks how many pills remain in a prescription and how often a pill is removed, allowing the company to remind patients to take a pill on schedule.[58] The HapiFork is a sensor-filled fork that monitors how much and how fast you eat. In addition to uploading its data to a computer or smartphone app, the fork's indicator lights will flash to warn you that you are eating too quickly.[59] Finally, after your meal you can brush with the Beam toothbrush, which wirelessly connects to a user's smartphone to record the date, time, and duration of "brushing events."[60]

ii. Wearable Sensors. Wearable sensors have also proliferated in the last eighteen months. As indicated, consumers have purchased tens of millions of these devices in the last few years.[61] Many—such as the FitBit,[62] Nike FuelBand,[63] and Body Media Fit arm band[64]—are electronic pedometers that track number of steps taken each day, distance walked, and calories burned.

---

[53] *See* http://www.onetouch.com/verio.
[54] *See* http://www.propellerhealth.com.
[55] *See* http://www.scanadu.com/scout.
[56] *See* http://www.scanadu.com/scanaflo.
[57] *See* http://www.podimetrics.com.
[58] *See* http://www.adheretech.com.
[59] *See* http://www.hapilabs.com.
[60] *See* http://www.beamtoothbrush.com.
[61] *See supra* note __ and accompanying text.
[62] *See* http://www.fitbit.com.
[63] *See* http://store.nike.com/us/en_us/pd/fuelband-se-gold/pid-1560508/pgid-1057887.
[64] *See* http://www.bodymedia.com.

Some wearable fitness devices also track other information, such as minutes asleep and quality of sleep,[65] heart rate, perspiration, or skin temperature.[66] The FINIS Swimsense tracks what swim stroke you are doing as well as distance swam, speed, and calories burned.[67] Not all inhabit the wrist or arm: the Valencell PerformTek fitness device packs a variety of sensors into a set of earbud headphones,[68] the Pulse is a finger ring that tracks heart rate,[69] and the LumoBack posture sensor is a strap worn around the lower back.[70]

Various companies have developed biotracking clothing with sensors embedded in the fabric.[71] Such sensor-laden clothing has both fitness and medical applications. Some is designed to measure athletic activity. The ElectricFoxy Move shirt, for example, contains four embedded stretch and bend sensors to monitor movement and provide realtime feedback about yoga poses, Pilates stretches, golf swings, or dance moves.[72] Nike+ sensor-filled shoes can measure running and walking data as well as the height achieved during a basketball dunk.[73] Other products have medical applications. The First Warning Systems Smart BSE (Breast Self Exam) bra, for example, contains integrated sensors in the bra's support cups that monitor slight variations in skin temperature that can provide very early indications of breast cancer.[74] Finally, Sensoria's Fitness smart socks can track not just how far or fast you run, but your running form and technique in order to avoid or diagnose injuries.[75]

Wearable fitness sensors are moving well beyond mere pedometry. The Amiigo wristband, for example, can detect different types of physical activity (e.g., jumping jacks, bicep curls, or jogging) and measure the number of repetitions performed or distances covered.[76] The LIT Tracker can measure paddles made in a canoe, jumps made during a basketball game, G-forces incurred during a ski jump, or effort expended surfing.[77] The Atlas tracker can measure heart rate and activity levels for almost any

---

[65] *See* http://www.fitbit.com/flex (tracking sleep duration and quality).
[66] *See* http://www.mybasis.com/basis-fitness-tracker-product-tour/ (touting that the basis wristwatch tracks heart rate, perspiration, and skin temperature as well as activity levels).
[67] *See* http://www.swimsense.finisinc.com.
[68] *See* http://www.performtek.com/ (tracking heart rate, respiration rate, energy expenditure, calories burned, metabolic rate, speed, steps taken, and recovery time).
[69] *See* http://www.electricfoxy.com/pulse.
[70] *See* http://lumoback.com/lumoback (tracking slouching and pelvic tilt and providing real time feedback on posture).
[71] *See* Elizabeth Woyke, *AT&T Plans to Sell Health-Tracking Clothing*, Forbes (Oct. 28 2011); http://www.aiqsmartclothing.com (offering BioMan smart clothing).
[72] *See* http://www.electricfoxy.com/move/.
[73] *See* http://www.nike.com/us/en_us/c/basketball/nike-basketball-hyperdunk-plus.
[74] *See* http://www.firstwarningsystems.com.
[75] *See* http://www.heapsylon.com/sensoria-fitness-more/.
[76] *See* http://www.amiigo.co.
[77] *See* http://www.nznlabs.com.

exercise, including swimming (it can distinguish between different strokes), running, weight lifting, pushups, situps, and rock climbing.[78]

iii. Intimate Contact Sensors. Related to wearables but sufficiently distinct to deserve special treatment, intimate contact sensors are devices embedded in bandages, medical tape, patches or tattoos worn on the skin. Sometimes called "epidermal electronics," these sensors are currently more medical in nature than fitness-oriented. For example, in November, 2012, the FDA approved the Raiing Wireless Thermometer, a peel-and-stick contact thermometer sensor that transmits real time body temperature to a user's smartphone.[79] Similarly, MC10's BioStamp is a tiny, flexible prototype device that can be worn like a small Band-Aid.[80] It measures and transmits heart rate, brain activity, body temperature, hydration levels, and exposure to ultraviolet radiation. Sano Intelligence is developing a patch to monitor the blood stream. This sensor-filled transdermal patch can record glucose levels, kidney function, potassium levels, and electrolyte balance.[81] The Metria patch by Avery Dennison is a remote medical monitoring device that measures temperature, sleep, heart rate, steps taken, and respiration rates.[82]

iv. Ingestible & Implantable Sensors. Although they may sound overly like science-fiction, ingestible and implantable sensors are also becoming a reality. Ingestible sensors include "smart pills," which contain tiny sensors designed to monitor inside the body. Given Imaging, for example, makes the PillCam—a pill-sized camera used to detect bleeding and other problems in the gastrointestinal tract—as well as SmartPill—an ingestible capsule that measures pressure, pH levels, and temperature as it travels through the body.[83] More bizarre, perhaps, in July, 2012, the Food and Drug Administration (FDA) approved the Proteus Feedback System, a pill containing a digestible computer chip.[84] The sensor is powered by the body's stomach fluids and thus needs no battery or antenna. A patch worn on the skin then captures data from the pill to track whether and when the pill was ingested, which it then sends on wirelessly to the user's smartphone. The goal is to embed such sensors into various types of medicines to monitor prescription compliance.

---

[78] *See* http://www.atlaswearables.com.
[79] *See* http://www.raiing.com.
[80] *See* http://www.mc10inc.com.
[81] *See* Ariel Schwartz, *No More Needles: A Crazy New Patch Will Constantly Monitor Your Blood*, available at http://www.fastcoexist.com/1680025/no-more-needles-a-crazy-new-patch-will-constantly-monitor-your-blood.
[82] *See* http://www.averydennison.com/en/home/technologies/creative-showcase/metria-wearable-sensor.html.
[83] *See* http://www.givenimaging.com.
[84] *See* http://www.proteusdigitalhealth.com.

Implantable medical sensors are already being prescribed to monitor blood glucose, blood pressure, and heart function,[85] and newer implantable sensors are being developed to detect organ transplant rejection.[86] One compelling example is a sensor that is implanted in a patient's tooth and that can differentiate between eating, speaking, coughing, smoking, drinking and breathing.[87] The device is fitted between two teeth or mounted on dentures or braces, and can transmit information wirelessly to one's dentist to assess dental disease or unhealthy habits.

Ingestible and implantable health and fitness sensors are at the cutting edge of current technology, but some estimate that within a decade up to a third of the U.S. population will have either a temporary or permanent implantable device inside their body.[88]

B. AUTOMOBILE SENSORS

Sensors have also become pervasive in the automotive context. Consider three types of automobile sensors that collect enormous amounts of data about drivers: event data records (or "black boxes"), consumer automobile sensor products, and auto insurance telematics devices.

i. Event Data Recorders (or "Black Boxes"). The National Highway Traffic Safety Administration (NHTSA) estimates that over 96 percent of 2013 vehicles—and most cars sold in the U.S. in the last twenty years—contain event data recorders (EDRs).[89] The NHTSA requires that EDRs collect fifteen types of sensor-based information about a car's condition, including braking status, vehicle speed, accelerator position, engine revolutions per minute, safety belt usage, air bag deployment, and number and timing of crash events.[90] The NHTSA requires that EDRs store such information for thirty seconds after a triggering impact, thus providing a composite picture of a car's status during any crash or incident. The NHTSA places no limits on the types of data that can be collected, nor does

---

[85] *See* http://www.medtronic.com.

[86] *See Transplant Rejection Sensor Paves Way for Body-Integrated Electronics*, http://www.theengineer.co.uk/medical-and-healthcare/news/transplant-rejection-sensor-paves-way-for-body-integrated-electronics/1016483.article (Jul. 22, 2014).

[87] *See* Ross Brooks, *Tooth-Embedded Sensor Relays Eating Habits to the Dentist* (July 30, 2013), available at http://www.psfk.com/2013/07/tooth-sensor-track-eating-habits.html?_escaped_fragment_=r3Fkm#!uz50L.

[88] *See* Cadie Thompson, *The Future of Medicine Means Part Human, Part Computer*, CNBC (Dec. 24, 2013), available at http://www.cnbc.com/id/101293979 (citing Eric Dishman of Intel Corporation).

[89] *See* Event Data Recorders, 69 Fed. Reg. 32,932, 32,933 (proposed June 14, 2004). On December 13, 2012, the National Highway Traffic Safety Administration (NHTSA) published a request for public comment on a proposed rule to mandate that all new cars sold after September 1, 2014 have an Event Data Recorder (EDR), or "black box." *See* 77 Fed. Reg. 74,144 (proposed Dec. 13, 2012).

[90] *See* 71 Fed. Reg. 50998-51048.

it specify who owns these data or whether such data can be retained and used by third parties.[91] A manufacturer can thus choose to include additional types of information, such as driver steering input, antilock brake activity, seat positions for driver and passenger, occupant size or position, vehicle location, phone or radio use, navigation system use, or other aspects of the car's condition.

ii. Consumer Automobile Sensors. In addition to EDRs, various consumer devices allow a driver to access her car's digital information via a smart phone. The leading example is the Automatic "Link"—a small Bluetooth device that connects to a car's OBD-II port.[92] Described as a "Fitbit for your car," the Link syncs information to a smart phone to monitor both the car's health and the user's driving habits. The Link tracks such variables as whether the driver brakes suddenly, is speeding, or accelerates rapidly—all in the name of helping the driver improve fuel efficiency. It also tracks and records location so as to provide feedback on how much driving you do per week, where, and when. All such information is stored in the cloud on Automatic's servers. The system can be set to automatically call for help in the event of a crash, and to email you when your engine needs maintenance.[93]

Much of the same functionality can be had just from the sensors already in a driver's smartphone. ZenDrive, for example, is an iPhone application that helps drivers track their driving, providing feedback on driving technique, tips to avoid traffic, and information on nearby attractions.[94] Likewise, DriveScribe is an app designed to help parents and insurers monitor teenage driving habits through the sensor data created by a driver's smartphone.[95] The app can be set to block texting and calling on the teenager's phone while driving, as well as to send an email or text message to a parent with updates on the teenager's driving performance. It records the time, length and location of every trip, average speed and speed at any point during the trip, and descriptions of any moving violations (e.g., speeding or other detectable infractions such as failing to obey a stop sign).

These consumer devices differ in important ways from the EDR already in most vehicles. First, an EDR typically can record and store only a few seconds of data—enough to assist with crash diagnostics, but not enough to track a vehicle's location or a driver's performance over time. Consumer smartphone-connected (or smartphone-based) apps record much more information and store it longitudinally. Second, an EDR stores its

[91] *See* Event Data Recorders, 69 Fed. Reg. 32,932, 32,933 (proposed June 14, 2004).
[92] www.automatic.com.
[93] The Dash is a similar device. *See* http://dash.by. Similarly, the Moj.io is a prototype Internet-connected car monitoring sensor that can alert a user if their car has been damaged, stolen, towed, or needs service. *See* http://www.moj.io.
[94] *See* http://www.zendrive.com.
[95] *See* http://www.drivescribe.com.

limited information in the car on the device itself. Consumer driving monitors and smartphone apps transmit such information to the device's manufacturer, and often store such information in the cloud. Third, obviously the notice involved to consumers differs. Many consumers may be unaware that their vehicle contains an EDR, which may be mentioned only in the owner's manual. Presumably consumers are aware, however, when they install a consumer sensor device in their car or a car tracking app on their smartphone.

iii. Auto Insurance Telematics Devices. Finally, a third type of automobile sensor device has become increasingly popular: insurance telematics devices. These products are given to consumers by automobile insurers to track consumer driving behavior and offer discounts on insurance premiums based on driving behavior.[96]

The most well-known telematics device in the United States is probably the Progressive Snapshot. Progressive provides the Snapshot device to insureds, who connect it to their vehicle. The Snapshot collects information on vehicle speed, time of day, miles driven, and rates of acceleration and braking. It does not collect information on location or driver identity. After thirty days of data collection, the data are used to calculate a "Snapshot score" for that vehicle (and/or driver), which is then used as one factor in determining the applicable insurance premium. Snapshot then continues to collect data for another five months to set the ongoing renewal discount for that policy. According to Progressive's Privacy Policy, Snapshot data are not used to resolve insurance claims without the user's consent.[97]

Snapshot and other usage-based devices have grown in popularity, but enrollment remains low as a percentage of the total insurance industry. Overall, roughly three percent of insureds use a telematics device, although roughly ten percent of Progressive's customer portfolio uses Snapshot.[98] Insurance executives continue to look for marketing approaches to reassure consumers about privacy concerns.[99] Some have expressed concern that manufacturers of consumer automobile telematics systems may not be disclosing sufficient information about the data collected or the ways such data are used.[100] Industry generally minimizes concerns about privacy,

---

[96] *See* Bill Kenealy, *Wireless Sensors Provide Underwriters with Expanded Data*, BUS. INS. (Jan. 13, 2013) ("[T]he Internet of Things … can furnish underwriters with a continuous data stream to better assess risk.").
[97] *See* http://www.progressive.com/auto/snapshot-privacy-statement/.
[98] *See* Becky Yerak, *Motorists Tap the Brakes on Installing Data Devices for Insurance Companies*, CHI. TRIB. (Sept. 15, 2013).
[99] *See id.*
[100] *See* Francesca Svarcas, *Turning a New Leaf: A Privacy Analysis of Carwings Electric Vehicle Data Collection and Transmission*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 165 (2013) (analyzing the consumer disclosures related to data collected by the Nissan LEAF electric vehicle).

equity, and discrimination, however. Instead, industry commentators tout the benefits of more accurate pricing[101]—and even of the changes that individuals might make to their behavior because of increased monitoring.[102] Insurance industry commentators speculate that the telematics revolution may spread from car insurance to health and life insurance.[103]

C. HOME & ELECTRICITY SENSORS

Internet of Things devices have entered the home as well. Consider two applications: the "smart home" of connected Internet of Things devices and the "smart grid" of sensor-based electricity monitors.

i. The Smart Home. The phrase "Internet of Things" often conjures up images of a home full of connected, sensor-laden devices. As discussed above, sensor devices go far beyond such "smart home" appliances. Nevertheless, such home electronics are indeed one aspect of the proliferation of sensors.

There are many new consumer sensor devices available for home use. The most well-known may be the Nest thermostat. The Nest thermostat—recently acquired by Google in the first major Internet of Things acquisition[104]—tracks your behavior at home to set temperature more efficiently.[105] The thermostat accepts and records direct user input (e.g., to increase or decrease temperature), but also contains sensors to sense motion in a room, ambient light, and room temperature and humidity. All such information is stored on Nest's cloud servers and can be accessed and controlled via a user's smartphone or other Internet-connected computer. Nest also makes a smoke and CO2 detector with similar features.[106]

---

[101] *See e.g.* Yuanshan Lee, *Applications of Sensing Technologies for the Insurance Industry*, in BUSINESS ASPECTS OF THE INTERNET OF THINGS (2008) (discussing how pay-as-you-drive auto insurance based on sensors helps overcome moral hazard and adverse selection); Lilia Filipova-Neumann & Peter Welzel, *Reducing Asymmetric Information in Insurance Markets: Cars With Black Boxes*, 27 Telematics & Informatics 394 (2010) (arguing that insurance contracts with post-accident monitoring of black box information are pareto efficient).

[102] *See id.* ("Doing whatever one feels may give one a sweet sense of freedom, but it's probably not a bad thing if I'm a little bit more conscious about how close I follow the other car, how frequently and suddenly I brake, or how much I exercise and how well I eat.").

[103] *See* Anthony O'Donnell, *Will Data Proliferation Foster Insurer/Customer Collaboration on Underwriting*, Ins. & Tech. (Nov. 19, 2010), available at http://www.insurancetech.com/business-intelligence/228300215 ("Perhaps life and health insurance customers may similarly be motivated to enter into a kind of information transparency partnership whereby they enjoy better rates for demonstrating less risky behavior.").

[104] *See* Rolfe Winkler & Daisuke Wakabayashi, *Google to Buy Nest Labs for $3.2 Billion*, WALL ST. J. (Jan. 13, 2014).

[105] *See* http://www.nest.com.

[106] *See id.*

Beyond thermostats and smoke detectors, a variety of home appliances are increasingly Internet-connected. The GE Brillion home oven, for example, reports its temperature, sends alerts, and can be turned on or controlled from a GE smartphone app.[107] More broadly, the DropTag sensor can detect if a package has been dropped or shaken during shipping,[108] a Twine sensor device can detect floods, leaks, opened doors, temperature, and other events in your home,[109] a WattVision will record home energy use patterns,[110] and a Wimoto Growth sensor will text you if your plants need watering.[111] Various firms are working to integrate such disparate sources of information onto software and hardware platforms. SmartThings, for example, consists of a processing hub that can connect to a variety of different home sensors, such as an open/shut sensor (to monitor doors and windows), a vibration sensor (to monitor knocking on the front door), a temperature sensor (to control a thermostat), a motion sensor, and a power outlet monitor (to turn outlets on and off remotely).[112] Similarly, Belkin is developing a network of home devices to monitor home electricity and water usage and allow consumer control over power outlets and home devices,[113] Sense has created the Mother line of motion and other sensors to track many aspects of daily life, including sleep, fitness, medication compliance, water usage, home temperature, and home security,[114] Revolv is a smart home hub designed to work with multiple brands of connected appliances,[115] and Quirky is a line of smart home products from GE and other manufacturers designed to work together.[116] All of these consumer products aim to provide users with information about and control over home appliances. Along the way, they generate, transmit, and store a great deal of information about both a home and those within it.

ii. The Smart Grid. The home is increasingly monitored via sensors in a second way as well: the "smart" electricity grid. According to the U.S. Energy Information Administration more than 36 million smart electricity meters were installed in the U.S. as of August, 2012, covering roughly 25 percent of the U.S. electric market.[117] The "smart grid" such meters create promises huge energy efficiencies.

At the same time, smart grid data provide an intimate look into one's home. Electricity usage can reveal when a person is or is not home,

---

[107] *See* http://www.geappliances.com/connected-home-smart-appliances.
[108] *See* http://www.cambridgeconsultants.com/news/pr/release/116/en.
[109] *See* http://www.supermechanical.com.
[110] *See* http://www.wattvision.com.
[111] *See* http://www.wimoto.com.
[112] *See* http://www.smartthings.com.
[113] *See* http://www.belkinbusiness.com/echo-water-0.
[114] *See* http://sen.se.
[115] *See* http://revolv.com.
[116] *See* http://quirky.com.
[117] *See Smart Meter Deployments Continue to Rise* (Nov. 1, 2012), available at http://www.eia.gov/todayinenergy/detail.cfm?id=8590.

how often they cook, clean, shower, or watch television, how often they go on vacation, and how much they use exercise equipment. Computer science research has even shown that one can determine—with 96 percent accuracy—exactly what program or movie someone is watching on television just by monitoring electrical signals emanating from the person's house.[118]

One can infer a great deal from such data, such as how affluent a person is, how diligent they are about cleanliness or exercise, and even how depressed or sleep-deprived they might be: "For example: the homeowner tends to arrive home shortly after the bars close; the individual is a restless sleeper and is sleep deprived; the occupant leaves late for work; the homeowner often leaves appliances on while at work; the occupant rarely washes his/her clothes; the person leaves their children home alone; the occupant exercises infrequently."[119] As with other forms of sensor data, such information could be of interest to insurance companies, employers, creditors, and law enforcement.[120] And it is very hard to opt out of the smart grid, because utility companies roll smart meters out to an entire geographic area.[121]

The European Data Protection Supervisor has warned that such monitors could lead to "massive collection of personal data" without much protection.[122] Similarly, the National Institute of Standards and Technology recently warned that "[p]ersonal energy consumption data … may reveal lifestyle information that could be of value to many entities, including vendors of a wide range of products and services. Vendors may purchase attribute lists for targeted sales and marketing campaigns that may not be welcomed … Such profiling could extend to … employment selection,

---

[118] *See* Miro Enev et al., *Inferring TV Content from Electrical Noise*, ACM CONFERENCE '10 1, 1 (2010) ("[W]e show that given a 5 minute recording of the electrical noise unintentionally produced by the TV it is possible to infer exactly what someone is watching (with an average accuracy of 96% …) by matching it to a database of content signatures.").

[119] Ann Cavoukian, Jules Polonetsky & Christopher Wolf, *SmartPrivacy for the Smart Grid: Embedding Privacy Into the Design of Electricity Conservation*, 3 IDENTITY IN THE INFORMATION SOCIETY 275, 284 (2010).

[120] *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 28 (Aug. 2010) ("Personal energy consumption data … may reveal lifestyle information that could be of value to many entities, including vendors of a wide range of products and services. … Such profiling could extend to … employment selection, rental applications, and other situations that may not be welcomed by those targets.").

[121] *See* Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161, 175 (2011) ("As electric utilities receive permission from their state public utility commissions to replace traditional meters with smart meters and expand their rollout, the utilities will cease servicing traditional meters and consumers will need to permit the installation of a smart meter in their homes if they want to continue to receive electricity.").

[122] Opinion of the European Data Protection Supervisor (Jun. 8, 2012), available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf ("[Smart meters that track electricity usage] enable[] massive collection of personal information ….").

rental applications, and other situations that may not be welcomed by those targets."[123] Nevertheless, only a few states have addressed how smart grid data can be used, how it should be secured, and what sorts of consent consumers should be required to provide for its use.[124] The California Public Utilities Commission and the National Institute of Standards and Technology collaborated on a report detailing the potential privacy problems with smart grid technology.[125] Two states have required utility companies to secure a homeowner's express consent before installing a smart grid device,[126] and six states have enacted legislation allowing consumers to opt out of using smart grid technology.[127] Several states have also limited a utility company's ability to sell or share smart grid data with third parties.[128] To date, however, such regulation of the smart grid is inconsistent and scattered.

D. EMPLOYEE SENSORS

Beyond the body, car, or home, sensors are also being deployed in the workplace, allowing new forms of employee monitoring and control. As in other contexts, workplace sensors create new streams of data about where employees are during the workday, what they are doing, how long their tasks take, and whether they comply with employment rules.

Consider a simple example. HyGreen is a hand hygiene monitoring system to record all hand hygiene events in a hospital and remind healthcare workers to wash their hands.[129] The system consists of sink-top sensors that detect soap dispensing and hand washing. When a hand hygiene event is recognized, the sensors read the employee's identification badge and wirelessly transmit a record of the employee's identity and the time and location of the hand washing event. If the employee has not washed her hands and approaches a patient's bed, another sensor on the bed registers that the employee is approaching and sends the employee's identification badge a warning signal, causing it to vibrate to remind the employee to wash. The system tracks and stores all hand washing by employees around the clock.[130]

---

[123] *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid* 28 (Aug. 2010) [hereinafter *Privacy and the Smart Grid*].
[124] Nat'l Inst. Of Standards and Tech., Smart Grid Cyber Security Strategy and Requirements, Draft 1 – Comment Resolution 123, at 103 According to NIST, "in general, state utility commissions currently lack formal privacy policies or standards related to the Smart Grid.".
[125] *See Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid* (Aug. 2010) [hereinafter *Privacy and the Smart Grid*].
[126] *See* Vermont; New Hampshire.
[127] *See* Michigan; New Hampshire, New York, Pennsylvania, Rhode Island, Vermont.
[128] *See* California (SB 674, 2011); Colorado (HB 1191, 2011); Oklahoma (HB 1079).
[129] *See* http://www.hygreen.com.
[130] Other handwashing systems exist as well. *See* http://www.intelligentM.com (offering hand washing system); http://www.generalsensing.com (offering MedSense system to track,

This is a direct and fairly obvious use of sensors to monitor employees and shape their behavior. Location and movement tracking is another relatively simple use. As one commentator recently noted, "[a]s Big Data becomes a fixture of office life, companies are turning to tracking devices to gather real-time information on how teams of employees work and interact. Sensors, worn on lanyards or placed on office furniture, record how often staffers get up from their desks, consult other teams and hold meetings."[131] The Bank of America, for example, has used sensor badges to record call center employees' movements and tone of voice throughout the day.[132]

Other examples of such relatively simple sensor systems include fleet tracking of company trucks or automobiles. For example, Cloud Your Car makes a small device that plugs into a car's cigarette lighter and contains a GPS tracker, cell connectivity, and a variety of accelerometer sensors.[133] It is designed to help business owners track their fleet of vehicles, as well as monitor employee driving behavior. An employer can, for example, monitor fleet status and locations in real time, review route histories, and track employees' driving rankings and scores. Similarly, Greenroad manufactures fleet-tracking sensors designed to reduce accident, fuel, insurance and maintenance costs by providing real-time driving and location information to employers.[134]

Sensors are being used to track more nuanced and abstract aspects of employee behavior as well. For example, Sociometric Solutions has deployed tracking devices for Bank of America, Steelcase, and Cubist Pharmaceuticals.[135] Employees wear a sensor-laden identification badge that contains a microphone, a Bluetooth transmitter, a motion sensor, and an infrared beam.[136] The microphone is not used to record the content of conversations, but instead to assess the tone of voice being used. The higher the pitch or the faster the speech, the more excited or passionate the speaker. Similarly, the infrared beam is used to determine how one user is positioned vis-à-vis another wearing a similar badge. Those who generally have others facing them when speaking are inferred to be more dominant personalities.

---

incentivize, and analyze hygiene compliance). *See generally* Anemona Hartocollis, *With Money at Risk, Hospitals Push Staff to Wash Hands*, N.Y.T. (May 28, 2013).

[131] *See* Rachel Emma Silverman, *Tracking Sensors Invade the Workplace*, WALL ST. J. (Mar. 7, 2013).

[132] *Id.*

[133] *See* http://www.cloudyourcar.com.

[134] *See* http://www.greenroad.com.

[135] *See* Vivian Giang, *Employees Tracked with "Productivity" Sensors*, BUSINESS INSIDER (Mar. 18, 2013).

[136] Hitachi has also developed a similar employee ID badge containing various sensors for nuanced monitoring of employee interactions and productivity. *See* H. James Wilson, *Wearable Gadgets Transform How Companies Do Business*, WALL ST. J. (Oct. 20, 2013) (describing the Hitachi Business Microscope).

Such sensors allow for some amazing inferences. Combined with email-traffic data and survey results, one company found that more socially-engaged employees performed better, as opposed to employees that spent more time alone in their offices. As a result, the employer set a daily afternoon coffee break—to encourage social interaction. This relatively benign example may not cause alarm. Such data, however, is extremely telling: the CEO of Sociometric Solutions says that he can "divine from a worker's patterns of movement whether that employee is likely to leave the company, or score a promotion."[137] As MIT Professor Alex Pentland put it, "[w]e've been able to foretell, for example, which teams will win a business plan contest, solely on the basis of data collected from team members wearing badges at a cocktail reception."[138]

There has been relatively little discussion in the legal or business literatures about such sensor-based employee monitoring.[139] Some fear that consent in the employment context is difficult to assess and rarely truly consensual.[140] This potentially becomes more problematic as employers demand access to more intimate information about their employees. The British grocery store chain Tesco, for example, has required employees to wear armbands that measure their productivity. These Motorola devices track how quickly employees unload and scan goods in Tesco's warehouse, as well has how often employees take breaks.[141]

E. SMART PHONE SENSORS

Finally, the most ubiquitous new sensor technologies are those embedded in smartphones. Such phones now generally contain a compass (to detect physical orientation), accelerometer (to track the phone's movement in space), ambient light monitor (to adjust screen brightness), proximity sensor (to detect whether the phone is near your face), and gyroscope (to detect the phone's orientation vertically or horizontally), as well as GPS, a sensitive microphone, and multiple cameras. Research is underway to further enhance smartphones to detect ultraviolet radiation

---

[137] *WSJ*, *supra*.

[138] Giang, *supra* note ___. *See also* Alex Pentland, *The New Science of Building Great Teams*, HARV. BUS. REV. (Apr. 2012).

[139] *See e.g.,* Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277 (2012) (analyzing the U.S. Supreme Court's decision in City v. Ontario v. Quon, and arguing that public sector employees should have greater privacy rights than private sector employees); Karin Mika, *The Benefit of Adopting Comprehensive Standards of Monitoring Employee Technology Use in the Workplace*, CORNELL H.R. REV. 1, 2 (2012) ("[A]n employer can monitor virtually everything and almost anything can be done with it.").

[140] *See e.g.,* Adam D. Moore, *Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy*, 10 BUS. ETHICS Q. 697, 701-702 (2000) (considering whether employee consent to tracking or surveillance is forced or truly consensual).

[141] *See* Claire Suddath, *Tesco Monitors Employees with Motorola Armbands*, Bloomberg Businessweek (Feb. 13, 2013).

levels (to help prevent skin cancer),[142] pollution levels (to help monitor one's environment),[143] and various indicators of health, activity and well-being,[144] including sensors that can monitor blood alcohol levels and body fat.[145]

A great deal of information can be gleaned from a typical smartphone. For example, the Run Keeper and Strava applications use an iPhone's sensors and GPS to track running and cycling routes, speeds, and history.[146] The Instant Heart Rate app uses a smartphone's camera to detect a user's fingertip pulse.[147] The Argus and Moves apps track a user's fitness by using a phone's sensors to monitor steps taken, cycling distances, and calories expended, just like a dedicated fitness monitor such as FitBit.[148]

More personal, perhaps, researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood,[149] stress levels,[150] personality type,[151] bipolar disorder,[152] demographics (e.g., gender, marital status, job status, age),[153] smoking habits,[154] overall wellbeing,[155] progression of Parkinson's disease,[156] sleep patterns,[157] happiness,[158] levels

---

[142] *See* http://mobile.mit.edu/research/new-sensors-smartphones (last visited May 14, 2012).
[143] *See* David Hasenfratz et al., *Participatory Air Pollution Monitoring Using Smartphones*, in Mobile Sensing (2012).
[144] *See e.g.,* Sean T. Doherty & Paul Oh, *A Multi-Sensor Monitoring System of Human Physiology and Daily Activities*, 18 TELEMEDICINE AND E-HEALTH 185 (2012) (using smartphone plus electrocardiogram and blood glucose monitor to track health and activity).
[145] *See* Andrew Ku, *Smartphones Spotted with Breathalyzer, Body Fat Sensors* (Mar. 2, 2012).
[146] *See* http://www.runkeeper.com; http://www.strava.com.
[147] *See* http://www.azumio.com.
[148] *See* http://www.moves-app.com.
[149] *See* Robert LiKamWa et al., *MoodScope: Building a Mood Sensor from Smartphone Usage Patterns*, MOBISYS 389 (2013); Robert LiKamWa et al., *Can Your Smartphone Infer Your Mood?*, PROC. PHONESENSE WORKSHOP 1 (2011);
[150] *See* Amir Muaremi et al., *Towards Measuring Stress with Smartphones and Wearable Devices During Workday and Sleep*, BIONANOSCI 1 (2013).
[151] *See* Gokul Chittaranjan et al., *Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones*, WEARABLE COMPUTERS 29, 35 (2011) (explaining methodology).
[152] *See* Agnes Grunerbl et al., *Towards Smart Phone Based Monitoring of Bipolar Disorder*, SENSYS '12 (2012) ("[D]ata gathered by a smart-phone can provide the necessary information to measure changes in the disease episodes.").
[153] *See* Erheng Zhong et al., *User Demographics Prediction Based on Mobile Data*, 9 PERV. & MOB. COMPUT. 823 (2013).
[154] *See* F. Joseph McClernon & Romit Roy Choudhury, *I Am Your Smartphone, and I Know You Are About to Smoke: The Application of Mobile Sensing and Computing Approaches to Smoking Research and Treatment*, 15 NICOTINE TOB. RES. 1651, 1652 (2013) ("[M]any of the conditions antecedent to smoking exhibit a 'fingerprint' on multiple sensing dimensions, and hence can be detected by smartphones.").
[155] *See* Nicholas D. Lane et al., *BeWell: A Smartphone Application to Monitor, Model and Promote Wellbeing*, 5TH INTL. ICST CONF. ON PERVASIVE COMPUT. TECH. FOR HEALTHCARE (2011).
[156] *See* Sinziana Mazilu et al., *Online Detection of Freezing of Gate with Smartphones and Machine Learning Techniques*, PERVASIVEHEALTH 123 (2012).

of exercise,[159] and types of physical activity or movement.[160] As evidence mounts of the many different inferences that smartphone sensors can support, researchers are beginning to imagine future phones that will be able to couple such sensor data with other information to understand even more about a user. One computer scientist has predicted that such next generation devices will be "cognitive phones."[161] Such a phone might be able to combine sensor-based indications of stress, for example, with information from one's calendar about what meeting or appointment caused the stress, information from other sensors about one's health, and location information about where you were at the time the stress occurred. Imagine that "the phone's calendar overlays a simple color code representing your stress levels so you can visually understand at a glance what events, people, and places in the past—and thus likely in the future—aren't good for your mental health."[162] As futuristic as this may sound, such devices are actually possible by combining different aspects of today's technology.

II. FOUR PROBLEMS

Part I provided a taxonomy of types of consumer devices—personal health monitors, automobile black boxes, home and appliance monitors, employee monitors, and smart phones—already contributing to the Internet of Things. These devices are currently generating reams of data about their users' activities, habits, preferences, personalities, and characteristics. Those data are intensely valuable. At the same time, the Internet of Things presents new and difficult issues. Put most simply, this much new, high-quality data cannot enter the economy without the potential for misuse. To reap the benefits of the Internet of Things we must deal proactively with its likely harms.

This Part explores four problems: (1) the reality that big data analysis of the Internet of Things will likely lead to unexpected inferences that cross contexts in potentially unacceptable and discriminatory ways; (2) the near impossibility of perfectly de-identifying Internet of Things data to protect privacy; (3) the vulnerability of these consumer devices to hacking and other security breaches; and (4) the weakness of consumer sensor privacy policies and of notice and choice in this context in which small,

---

[157] *See* Zhenyu Chen et al., *Unobtrusive Sleep Monitoring Using Smartphones*, PERVASIVEHEALTH 145 (2013).
[158] *See* Andrey Bogomolov et al., *Happiness Recognition from Mobile Phone Data*, SOCIALCOM 790 (2013).
[159] *See* Muhammad Shoaib et al., *Towards Physical Activity Recognition Using Smartphone Sensors*, UBIQUITOUS INTELL. & COMPUT. 80 (2013).
[160] *See* Alvina Anjum & Muhammad U. Ilyas, *Activity Recognition Using Smartphone Sensors*, CONSUMER COMMUN. & NETWORK. CONF. 914 (2013).
[161] *See* Andrew Campbell & Tanzeem Choudhury, *From Smart Phones to Cognitive Phones*, PERVASIVE COMPUTING 7, 11 (2012).
[162] *Id.*

often screen-less devices may generate a great deal of invisible data. For each issue—discrimination, privacy, security, and consent—I consider not only the technical problems inherent in the Internet of Things but the ways in which existing law is unprepared to address those problems.

A. DISCRIMINATION

The first Internet of Things problem is the Achille's Heel of widespread sensor deployment: Internet of Things data will allow us to sort consumers more precisely than ever before, but such sorting can easily turn from relatively benign differentiation into new and invidious types of unwanted discrimination. This section explores both the technical and legal problems of discrimination on the Internet of Things. The technical problem is simple: coupled with Big Data or machine learning analysis, massive amounts of sensor data from Internet of Things devices can give rise to unexpected inferences about individual consumers. Employers, insurers, lenders, and others may then make economically-important decisions based on those inferences, without consumers or regulators having much understanding of that process. This could lead to new forms of illegal discrimination against those in protected classes such as race, age, or gender. More likely, it may create troublesome but hidden forms of economic discrimination based on Internet of Things data. Currently, both traditional discrimination law and information privacy law such as the FCRA are unprepared for such new forms of discriminatory decision-making.

i. The Technical Problem: Sensor Fusion & Big Data Analytics May Mean That Everything Reveals Everything

Consider an example. Imagine that a consumer uses a Fitbit fitness tracking bracelet to monitor her fitness regime and overall health. In addition, she has an Internet-connected Aria scale—owned by Fitbit—that she uses to track her weight loss progress. She has used these devices for several months, storing and viewing her information on Fitbit's web site. Our hypothetical consumer now decides to apply for a job—or a mortgage, loan, or insurance policy. During the application process her prospective employer interviews her and runs her through various tests, simulations, and other exercises to discern her experience, knowledge base, and ability to work well with others. As a final step in the hiring process, the employer asks for access to our candidate's Fitbit records from the previous three months.

Although this may seem outrageous, employers increasingly analyze various data about potential employees to discern which will be most productive, effective, or congenial. As one commentator recently put

it, "[t]his … is the single biggest Big Data opportunity in business. If we can apply science to improving the selection, management, and alignment of people, the returns can be tremendous."[163] Such "talent analytics"[164] could increasingly incorporate sensor data from the Internet of Things. Employers have become more comfortable with using such devices as part of wellness programs.[165] Virgin Health Miles, for example, offers a turnkey "pay-for-prevention" program to employers that integrates incentives with electronic pedometers, heart rate monitors, and biometric tracking.[166] Some employers have also become more comfortable demanding such information from employees. 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.

Fitbit data could reveal a great deal to an employer. Impulsivity and the inability to delay gratification—both of which might be inferred from one's exercise habits—correlate with alcohol and drug abuse,[167] disordered eating behavior,[168] cigarette smoking,[169] higher credit card debt,[170] and lower credit scores.[171] Lack of sleep—which a Fitbit tracks—has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness and fear.[172] Such information could tip the scales for or against our hypothetical candidate.

The real issue, however, is not merely that an employer or other decision-maker might demand access to such data. The technical problem created by the Internet of Things is that sensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources. Put simply, in a world of connected sensors,

---

[163] *See* Josh Bersin, *Big Data in Human Resources: Talent Analytics Comes of Age*, FORBES (Feb. 17, 2013).
[164] www.evolvondemand.com .
[165] *See* Partrick J. Skerrett, *The Potential of Remote Health Monitoring at Work*, HARVARD BUS. REV. (Dec. 9, 2009) *available at* http://blogs.hbr.org/health-and-well-being/2009/12/the-potential-of-remote-health.html.
[166] *See* http://us.virginhealthmiles.com/solutions (last visited May 30, 2012).
[167] *See* C.W. Lejuez et al., *Behavioral and Biological Indicators of Impulsivity in the Development of Alcohol Use, Problems, and Disorders*, 34 ALCOHOLISM 1334 (2010).
[168] *See* Adrian Meule et al., *Enhanced Behavioral Inhibition in Restrained Eaters*, 12 EATING BEHAVIORS 152, 152-53 (2011).
[169] *See* Nathasha R. Moallem & Lara A. Ray, *Dimensions of Impulsivity Among Heavy Drinkers, Smokers, and Heavy Drinking Smokers: Singular and Combined Effects*, 37 ADDICTIVE BEHAVIORS 871, 872 (2012) ("There has been much evidence that heavy drinkers and smokers have increased delay reward discounting, that is, impulsively choosing a smaller, immediate reward over a larger, delayed reward.").
[170] *See* Stephan Meier & Charles Sprenger, *Present-Biased Preferences and Credit Card Borrowing*, 2 AMER. ECON. J. 193 (2010).
[171] *See* Sprenger, *supra* note __ at __.
[172] *See id*. at 917.

"everything may reveal everything." Sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a variety of—and perhaps all—other economic or information contexts.

Thus, an employer might not have to demand access to a candidate's Fitbit data. An individual's driving data—from their EDR, after-market consumer automobile monitor, or insurance telematics device—could likewise give rise to powerful inferences about their personality and habits. Her electricity usage might similarly reveal much about her daily life, how late she typically arrived at home, and other traits that could be of interest. Her smartphone data could also be extremely revealing. As just one example of a surprising inference, research has shown that conversational patterns—listening, speaking, and quiet states—can be inferred from various types of sensors, including respiratory rates[173] and accelerometer data like that generated by a smartphone.[174] As discussed in Part I(D), employers can learn a great deal about employees from such conversational information, even without recording audio of any kind.[175]

With so many potential data sources providing relevant information about a potential employee, an employer could turn to any number of commercial partners for information about that employee. One's mobile phone carrier, electric utility company, and auto insurer might have such useful information, as would the makers of the myriad Internet of Things products reviewed in Part I. The Internet has given rise to a massive infrastructure of data brokers that accumulate and track information about individuals. How long before they begin to incorporate the incredibly rich and revealing data from the Internet of Things?

The extent to which "everything reveals everything" is an empirical question, and one that I and my colleague Paul Ohm have begun to investigate experimentally.[176] It may be that some natural constraints remain between information types or uses, and that certain sensor data do *not* correlate with or predict certain economically-valuable traits. Fitness may not predict creditworthiness; driving habits may not predict employability. We don't know for sure. There is reason to expect, however, that everything may reveal everything *enough* to justify real concern. Consider two arguments for this prediction.

---

[173] *See* Mahbubur Rahman et al., *mConverse: Inferring Conversation Episodes from Respiratory Measurements Collected in the Field*, WIRELESS HEALTH '11 (2011) ("[T]his is the first work to show that inference of listening state is possible from respiration measurements.").

[174] *See* Aleksandar Matic et al., *Speech Activity Detection Using Accelerometer*, ENG. IN MED. & BIO. SOC. 2112, 2113-14 (2012) (using accelerometer to measure the vibrational activity of the vocal chords).

[175] *See id.*

[176] *See* Scott Peppet & Paul Ohm, *The Discriminatory Inferences Project*, available at http://www.scottpeppet.com.

First, computer scientists have long discussed the phenomenon of "sensor fusion." Sensor fusion is the combining of sensor data from different sources to create a resulting set of information that is better than if the information is used separately.[177] A classic example is the creation of stereoscopic vision—including depth information—by combining the images of two offset cameras. A new piece of information—about depth—can be inferred from the combination of two other pieces of data, neither of which independently contains that new information.

The principle of sensor fusion means that data gleaned from various small sensors can be combined to draw much more complex inferences than one might expect. Data from an accelerometer and a gyroscope—both of which measure simple movements—can be combined to infer a person's level of relaxation (based on whether their movements are steady and even or shaky and tense).[178] If one adds heart rate sensor data, one can readily infer stress levels and emotions, because research has shown that heart rate variations from physical exercise have a different pattern than increases due to excitation or emotion.[179] Similarly, one might infer emotion or mental state from a variety of other daily activities, such as the way a consumer holds a cell phone, how smoothly a person types a text message, or how shaky a person's hands are while holding their phone.[180] Again, sensor fusion allows such complex and unexpected inferences to be drawn from seemingly simple data sources. As consumers use devices with more and different types of sensors—from fitness trackers to automobiles, ovens to workplace ID badges—these sensor data will fuse to reveal more and different things about individuals' behaviors, habits, and future intentions.

Second, Internet of Things data are ripe for Big Data or machine learning analysis:

> "Networked body-worn sensors and those embedded in mobile devices we carry (e.g., smartphones) can collect a variety of measurements about physical and physiological states, such as acceleration, respiration, and ECG. By applying sophisticated machine learning algorithms to these data, rich inferences can be made about the physiological, psychological, and behavioral states and activities of people.

---

[177] *See generally* David L. Hall et al., *An Introduction to Multisensor Data Fusion*, 85 PROC. OF THE IEEE 6 (1997) (explaining sensor data fusion). Sensor fusion is a sub-set of the general idea of data fusion, by which data from different sources is combined to draw new, more powerful inferences. *See* Richard Beckwith, *Designing for Ubiquity: The Perception of Privacy*, PERVASIVE COMPUTING 40, 43 (Apr.-Jun. 2003) ("Data fusion raises a particularly insidious set of problems … It's difficult to imagine various uses for fused data when you don't even consider that a fusion could take place.").

[178] *See e.g.,* Kaivan Karimi*, The Role of Sensor Fusion and Remote Emotive Computing in the Internet of Things* (2013) (on file with author).

[179] *See id.* at 6.

[180] *Id.*

> Example inferences include dietary habits, psychosocial stress, addictive behaviors (e.g., drinking), exposures to pollutants, social context, and movement patterns. … Seemingly innocuous data shared for one purpose can be used to infer private activities and behaviors that the individual did not intend to share."[181]

Commercial firms are already applying Big Data techniques to Internet of Things data to produce such inferences.

Consider, for example, the credit industry. I have explored elsewhere the evolution of credit scoring into the Internet age,[182] but suffice to say that lenders continually expand the types of information they incorporate into credit assessments. Most recently, some lenders have included data from social networks, such as Facebook and LinkedIn, to gauge credit risk.[183] Neo Finance, for example, targets auto loan borrowers and uses social networks to gauge a borrower's credit risk,[184] as does Lenddo, a microlender in Hong Kong that uses social network density to make credit decisions.[185] Similarly, the startup Kreditech examines over eight thousand data points to create an alternative to FICO scores. These include location data, social data (likes, friends, locations, posts), e-commerce shopping behavior, and device data (apps installed, operating systems installed).[186] Kreditech focuses on consumers in emerging markets where traditional credit scores do not exist.[187]

In keeping with this search for more nuanced and predictive data sources, lenders are beginning to experiment with incorporating Internet of Things sensor data into such decisions. Cell phone data are an obvious first place to start. For example, Safaricom, Kenya's largest cell phone operator, studies its mobile phone users to establish their trustworthiness. Based on how often its customers top up their airtime, for example, it may then decide to extend them credit. Similarly, Cignifi uses the length, time of day, and location of cell calls to infer the lifestyle of smartphone users—and hence the reliability of those users—for loan applicants in the developing world.[188]

---

[181] Andrew Raij et al., *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, ACM 11, 11 (2011).
[182] *See* Peppet, *Unraveling Privacy*, *supra* note __ at ___.
[183] *See Bad Credit? Start Tweeting: Startups are Rethinking How to Measure Creditworthiness Beyond FICO*, WALL ST. J. (Apr. 1, 2013); Evgeny Morozov, *Your Social Networking Credit Score*, FUTURE TENSE (Jan. 30, 2013).
[184] *See* http://myneoloan.com.
[185] *See* http://www.lenddo.com.
[186] *See* http://www.kreditech.com.
[187] Similarly, Wonga, based in London, factors in the time of day and the way a potential borrower clicks through its web site to determine whether to grant a loan. *See* William Shaw, *Cash Machine: Could Wonga Transform Personal Finance?*, WIRED (May 5, 2011) (quoting the CEO of Wonga saying "we've built an engine that is dramatically more predictive for [the lending that] we do than FICO").
[188] *See* http://cignifi.com/en-us/.

Sensor fusion and Big Data analysis combine to create the possibility that everything reveals everything on the Internet of Things. Although a consumer may use a FitBit solely for wellness-related purposes, such data could easily help an insurer draw inferences about that consumer to set premiums more accurately (e.g., amount of exercise may influence health or life insurance, or amount and quality of sleep may influence auto insurance), aid a lender in assessing the consumer's creditworthiness (e.g., conscientious exercisers may be better credit risks), help an employer determine whom to hire (e.g., those with healthy personal habits may turn out to be more diligent employees), or even help a retailer price discriminate (e.g., those wearing a FitBit may have higher incomes than those without). To the extent that context-violative data use breaks privacy norms—as Helen Nissenbaum and others have argued—consumer sensors will disrupt consumers' expectations.[189] This is big data at an entirely new scale, brought about by the proliferation of little sensors.[190]

ii. The Legal Problem: Antidiscrimination and Credit Reporting Law is Unprepared

There are two main legal implications of the possibility that everything may begin to reveal everything. First, will the Internet of Things lead to new forms of discrimination against protected classes, such as race? Second, will the Internet of Things lead to troubling forms of economic discrimination or sorting?

(1) Racial & Other Protected Class Discrimination

If the Internet of Things creates many new data sources from which unexpected inferences can be drawn, and if those inferences are used by economic actors to make decisions, one can immediately see the possibility of seemingly innocuous data being used as a surrogate for racial or other forms of illegal discrimination. One might not know a credit applicant's race, but one might be able to guess that race based on where and how a person drives, where and how that person lives, or a variety of other habits, behaviors, and characteristics revealed by analysis of data from a myriad of Internet of Things devices. Similarly, it would not be surprising if various sensor devices—a FitBit, heart rate tracker, or driving sensor, for example—could easily discern a user's age, gender, or disabilities. If sensor fusion leads to a world in which "everything reveals everything," then many different types of devices may reveal sensitive personal characteristics. As a

---

[189] *See* Heather Patterson & Helen Nissenbaum, *Context-Dependent Expectations of Privacy in Self-Generated Mobile Health Data*, working draft on file with author (2013).

[190] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL CHANGE HOW WE LIVE, WORK AND THINK (2013).

result, the Internet of Things may make possible new forms of obnoxious discrimination.

This is a novel problem and one that legal scholars are just beginning to recognize.[191] I am not convinced that the most blatant and obnoxious forms of animus-based discrimination are likely to turn to Internet of Things data—if a decision-maker wants to discriminate based on race, age, or gender, they likely can do so without the aid of such Internet of Things informational proxies. Nevertheless, the problem is worth considering because traditional antidiscrimination law is in some ways unprepared for these new forms of data.

Racial and other forms of discrimination is obviously illegal under Title VII,[192] Title I of the Americans with Disabilities Act (ADA) forbids discrimination against those with disabilities,[193] and the Genetic Information Nondiscrimination Act (GINA) bars discrimination based on genetic inheritance.[194] These traditional antidiscrimination laws leave room, however, for new forms of discrimination based on Internet of Things data. For example, nothing prevents discrimination based on a potential employee's health status, so long as the employee does not suffer from what the ADA would consider a disability.[195] Similarly, antidiscrimination law does not prevent economic sorting based on our personalities, habits, and character traits.[196] Employers are free not to hire those with personality traits

---

[191] *See e.g.,* Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. TELECOMM. & HIGH TECH. L. 351, 358 (2013) (discussing discrimination and arguing that "it will be exceedingly difficult to detect such discrimination if it is based on a dozen factors that through big data analysis are found to be positively correlated with race"). Some have argued that increased information about consumers may *dampen* discrimination against those in protected classes. Lior Strahilevitz is most known for taking this optimistic view that increased data flows will *curb* racial discrimination by allowing individuals and firms to discriminate for economically-relevant reasons rather than using race, age, gender, etc., as a discriminatory proxy. *See* Lior Strahilevitz, *Towards a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013); Lior Strahilevitz, *Privacy versus Antidiscrimination*, 75 U. CHIC. L. REV. 363 (2008). *But see* Anita L. Allen, *Privacy Law: Postiive Theory and Normative Practice*, 126 HARV. L. REV. F. 241 (2013) (counterint Strahilevitz and arguing that even if increased information benefits some African Americans, such heavy surveillance it might also create disproportionate burdens for African Americans as a group).

[192] *See* 42 U.S.C. § 2000e(b).

[193] *See* 42 U.S.C. § 12112(a)(2006 & Supp. V 2011).

[194] *See* 42 U.S.C. § 2000ff(4)(A) (2011).

[195] *See* Jessica L. Roberts, *Healthism and the Law of Employment Discrimination*, 99 IOWA L. REV. 571, 595-97 (2014) (analyzing antidiscrimination law to consider discrimination based on health).

[196] *See* Strahilevitz, *Postive Theory*, *supra* note __ at 2024 ("Maybe the law's tolerance for personality discrimination ought to be questioned, but American antidiscrimination law presently does not regard that kind of question as close."). There is some debate about whether an employer conducting a personality test on a potential employee triggers the Americans with Disabilities Act (ADA)'s prohibition on pre-job offer medical examinations. *See* Gregory Vetter, *Is a Personality Test a Pre-Job-Offer Medical Examination Under the ADA?*, 93 NORTHWESTERN UNIV. L. REV. 597 (1998-99).

they don't like; insurers are free to avoid insuring—or charge more to—those with risk preferences they find too expensive to insure; lenders are free to differentiate between borrowers with traits that suggest trustworthiness versus questionable character.[197]

As analysis reveals more and more correlations between Internet of Things data, however, this exception or loophole in antidiscrimination law may collapse under its own weight. A decision at least facially based on conduct—such as not to hire a particular employee because of her lack of exercise discipline—may systematically bias an employer against a certain group if that group does not or can not engage in that conduct as much as others. Moreover, seemingly voluntary "conduct" may shade into immutable trait depending on our understanding of genetic predisposition. Nicotine addiction and obesity, for example, may be less voluntary than biologically determined.[198] The level of detail provided by Internet of Things data will allow such fine-grained differentiation that it may easily begin to resemble illegal forms of discrimination. Currently, traditional antidiscrimination law has not yet considered these problems.

(2) Economic Discrimination

Even without the problem of race, age, or gender discrimination, using Internet of Things data to discriminate between—or "sort"—consumers is also potentially controversial. If widespread consumer sensor use leads to a world in which everything reveals everything, this will permit insurers, employers, lenders, and other economic actors to more finely distinguish between potential insureds, employees, and borrowers. From the perspective of economics, this may be beneficial. Put simply, more data will allow firms to separate pooling equilibria in insurance, lending, and employment markets, leading to efficiencies and increased social welfare.[199] From a legal or policy perspective, however, economic sorting is just not that simple. The public and its legislators tend to react strongly to forms of economic discrimination that economists view as relatively benign. For example, price discrimination—charging one consumer more for a good than another because of inferences about the first person's willingness or ability to pay—may be economically neutral or even efficient, but consumers react strongly against it.[200]

As indicated, traditional antidiscrimination law does not forbid differentiating between individuals on the basis of their behavior, personality, or conduct. That said, some constraints do exist on the use of Internet of Things data streams for such inferences and purposes. Most

---

[197] *See* Roberts, *Healthism*, *supra* note __ at 604-605 (discussing trait-based versus conduct-based discrimination).
[198] *See id.* at 614.
[199] *See* Strahilevitz, *Positive Theory*, *supra* note __ at 2021.
[200] [INSERT CITATIONS]

important, the Fair Credit Reporting Act[201] establishes consumers' rights vis-à-vis credit reports. Under FCRA, "consumer reporting agencies" (CRAs) are entities that engage in "assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[202] A consumer report is any report bearing on a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used … for the purpose of serving as a factor in establishing a consumer's eligibility for (A) credit or insurance …; [or] (B) employment purposes."[203]

The FTC has warned mobile application developers that if they provide information to employers about an individual's criminal history, for example, they may be providing consumer reports and thus regulated by FCRA.[204] By analogy, if a consumer sensor company such as FitBit began to sell their data to prospective employers or insurance companies, the FTC could take the position that Fitbit had become a CRA under FCRA. If a company such as Fitbit were classified as a CRA, consumers would have the right to dispute the accuracy of any information provided by such a CRA.[205] If Internet of Things manufacturers were *not* deemed CRAs, but instead deemed to be providing information *to* CRAs—such as established credit reporting firms or data aggregators—FCRA would forbid Internet of Things firms from knowingly reporting inaccurate information and would require that such firms correct and update incomplete or incorrect information.[206]

Although this somewhat constrains the use of Internet of Things data streams, FCRA's reach is limited. First and foremost, a lender, insurer, or employer doing their *own* analysis of sensor data would not trigger FCRA's CRA-related requirements.[207] Thus, Internet of Things data could be requested from applicants or gathered by such firms with impunity, as in the introductory example to this Section.

---

[201] Fair Credit Reporting Act, 15 U.S.C. 1681 *et. Seq* (1970).
[202] 15 U.S.C. 1681 a(f).
[203] 15 U.S.C. 1681b.
[204] On January 25, 2012, the FTC sent warning letters to three marketers of mobile applications (Everfy, InfoPay, and Intelligator) that provided criminal background checks to employers. Copies of the three letters are available on the FTC's website at http://www.ftc.gov/opa/2012/02/mobileapps.shtm.
[205] *See* 15 U.S.C. 1681i(a)(1)(A).
[206] 15 U.S.C. 1681s-2(1)(A-B).
[207] *See* Commissioner Julie Brill, *Reclaim Your Name*, keynote address at FTC Privacy Conference (Jun. 26, 2013), on file with author (describing "new-fangled lending institutions that forgo traditional credit reports in favor of their own big-data-driven analysis" as "right on—or just beyond—the boundaries of FCRA and other laws"). *See also* Nate Cullerton, Note, *Behavioral Credit Scoring*, 101 GEORGETOWN L.J. 807, 827 (2013) ("[T]he FCRA appears not to apply at all to credit determinations made 'in house' by credit issuers if they are not based on a credit report.").

Further, FCRA does not apply if data are used to tailor *offers* made through sophisticated electronic marketing techniques. For example, if a data aggregator sells a consumer's profile—including a profile based on Internet of Things sensor data—to a credit card company at the moment that the consumer accesses the credit card company's website, and that profile is used to tailor what the consumer sees on the web site (e.g., displaying one or another credit card based on assumptions about that consumer), that tailored offer does not trigger the FCRA's provisions.[208]

Finally, FCRA is designed to ensure *accuracy* in credit reports. FCRA gives consumers the right to check and challenge the accuracy of information found in such reports, so that credit, insurance and employment determinations are fair. Accuracy, however, is really not the problem with Internet of Things sensor data. One's Fitbit, driving, or smart home sensor data are inherently accurate—there is little to challenge. What is more questionable are the inferences *drawn* from such data. FCRA does not reach those inferences, however. It applies to the underlying "inputs" into a credit, insurance, or employment determination, not the reasoning that a bank, insurer, or employer then makes based on those inputs. Thus, FCRA provides consumers with little remedy if Internet of Things data were to be incorporated into credit reporting processes.

In summary, both traditional antidiscrimination law and data use-related legislation such as FCRA are unprepared to address the problem that on the Internet of Things everything may reveal everything.

B. PRIVACY

Discrimination based on sensor data is a potential problem so long as individualized inferences can be drawn from sensor data: if *your* FitBit or automotive or smartphone data are used to draw inferences about *you*. One solution would be to simply aggregate and anonymize all such data, refusing to release information about particular individuals. Many manufacturers of consumer sensor devices take this approach, promising users that their data will only be shared with others in de-identified, anonymous ways.[209] Does this solve the problem of discrimination and protect consumers' privacy?

i. The Technical Problem: Sensor Data Are Particularly Difficult to De-Identify

[208] *See* Brill, *supra* note __ at 4 (arguing that such marketing does not "fall under FCRA because they are used for marketing and not for determinations on ultimate eligibility"); Cullerton, *supra* note __ at 827 (arguing that such offers do not trigger the FCRA so long as "that data is not used to make the actual lending decision").

[209] *See infra* notes __-__ (exploring such policies). *See also* Appendix A.

Unfortunately not. Return to our Fitbit example. Even were Fitbit to de-identify its information by removing a user's name, address, and other obviously identifying information from the data set before it shared that information with others, it would be relatively easy to *re*-identify that data set. The reason is straightforward: each of us has a unique gait. This means that if I knew something about an individual Fitbit user's gait or style of walking, I could use that information to identify that individual among the millions of anonymized Fitbit users' data. I would then have access to all of that user's *other* Fitbit data, which would now be re-associated with her. As Ira Hunt, Chief Technology Officer of the Central Intelligence Agency, put it: "[S]imply by looking at the data [from a FitBit] we can find out … with pretty good accuracy, what your gender is, whether you're tall or you're short, whether you're heavy or light, … [and] you can be one hundred percent … identified by simply your gait—how you walk."[210]

In the last five years, legal scholars have become increasingly wary of the extent to which large data sets can ever be truly anonymized. My colleague Paul Ohm has argued that advances in computer science increasingly make it possible to attack and re-identify supposedly "anonymized" databases, rendering futile many attempts to protect privacy with anonymity.[211] Without delving into the burgeoning literature on de-identification generally, the point here is that *sensor* data sets are particularly vulnerable.[212]

Anonymization or de-identification becomes exceedingly difficult in sparse data sets: data sets in which an individual can be distinguished from other individuals by only a few attributes.[213] Sensor data sets are particularly prone to sparsity.[214] The reason is simple: sensor data captures such a rich picture of an individual, with so many related activities, that each individual in a sensor-based data set is reasonably unique.[215] For example, if

---

[210] Mathew Ingram, *Even the CIA is Struggling to Deal with the Volume of Real-Time Social Data*, GigaOm (Mar. 20, 2013).

[211] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 U.C.L.A. L. REV. 1701 (2010). *But see* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J. L. & TECH. 1 (2011) (arguing that Ohm's fears are misplaced and that anonymity can and should remain a central part of privacy law).

[212] *See* Andrew Raij et al., *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, ACM 11, 13 (2011) ("[E]xisting anonymization techniques alone cannot be used to protect individuals sharing personal sensor data.").

[213] *See* Lane et al., *supra* note __ at 13 ("Within this research community, the term sparsity refers to datasets in which an individual user or identity can be distinguished from others in a dataset by only a few select rarely occurring user attributes.).

[214] Lane et al., *supra* note __ at 13 (arguing, for example, that "shared mobile sensor data … is likely prone to sparsity").

[215] In addition to the fact that sensor data tend to be sparse, sensors themselves are also unique. An individual sensor may produce a unique fingerprint of "noise" that can then identify that sensor. For example, digital cameras can be individually identified from the patterns of sensor noise that they generate. *See* Jan Lukas, Jessica Fridrich, and Miroslav

a health sensor captures an individual's movements throughout the day, it is quite easy to infer what types of transportation that individual used (e.g., car, bike, subway). That unique pattern of transportation uses, however, means that if I have access to that anonymized data set containing your complete sensor information, and if I simultaneously know a few specific dates and times that you rode the subway or a bike, for example, I can probably determine which of the many users in that data set you are—and therefore know *all* of your movement information for all dates and times.[216]

Preliminary research suggests that robust anonymization of Internet of Things data is extremely difficult to achieve, or, put differently, that de-identification is far easier than expected:

> "[R]esearchers are discovering location-oriented sensors are not the only source of concern and finding other sensors modalities can also introduce a variety of new privacy threats. … [S]ensors, such as accelerometers, gyroscopes, magnetometers, or barometers, which at first glance may appear innocuous, can lead to significant new challenges to user anonymization."[217]

For example, researchers at MIT recently analyzed data on 1.5 million cellphone users in Europe over fifteen months and found that it was relatively easy to extract complete location information about a single person from an anonymized data set containing more than a million people.[218] In a stunning illustration of the problem, they showed that to do so required only locating that single user within several hundred yards of a cellphone transmitter sometime over the course of an hour four times in one year. With four such known data points, the researchers could identify ninety-five percent of the users in the data set. As one commentator on this

---

Goljan, *Digital Camera Identification from Sensor Pattern Noise*, 1 INFO. FORENSICS & SECUR. 205 (2006).

[216] *See* Lane et al., *supra* note __ at 13 (explaining that sensor data is particularly difficult to anonymize for this reason).

[217] *See* Nicholas D. Lane, Junyuan Xie, Thomas Moscibroda & Feng Zhao, *On the Feasibility of User De-Anonymization from Shared Mobile Sensor Data*, PHONESENSE 12, 12 (Nov. 6, 2012). *See also* Mudhakar Srivatsa & Mike Hicks, *Deanonymizing Mobility Traces: Using Social Networks as a Side-Channel*, CCS'12 (Oct. 2012).

[218] *See* Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCIENTIFIC REPORTS 1 (2013) ("[L]ittle outside information is needed to re-identify the trace of a targeted individual even in a sparse, large-scale, and coarse mobility dataset."). *See also* Sebastien Gambs, Marc-Olivier Killijian & Miguel Nunez del Prado, *De-anonymization Attack on Geolocated Datasets*, ACM (Jul. 18, 2012) ("[G]eolocated datasets gathering the movements of individuals are particularly vulnerable to a form of inference attack called the de-anonymization attack, and this even if the mobility traces have been anonymized prior to release.").

landmark study put it, for sensor-based data sets "it's very hard to preserve anonymity."[219]

Consider another example. Many smartphone owners are concerned about the misuse of their location data, which is often considered quite sensitive. In addition to GPS location sensors, however, most smartphones contain an accelerometer that measures the ways in which the smartphone is moving through space. Research shows that the data emitted by an accelerometer from one smartphone can often be correlated with similar data from a second phone to reveal that the two phones are producing sufficiently similar motion signatures to support the inference that they are in the same location.[220] In addition, if a smartphone user is driving her car, the patterns of acceleration and motion created by the car moving over the roadway are unique as to any other location. As the authors of the study revealing this finding put it, "the idiosyncrasies of roadways create globally unique constraints. … [T]he accelerometer can be used to infer a location with no initial location information."[221] So long as one phone (with a known location) has travelled the same roads as the previously "hidden" phone (with unknown location), the latter can be located.

ii. The Legal Problem: Privacy Law is Unprepared

The inherent sparsity of Internet of Things data means that protecting privacy through anonymization is particularly unlikely to succeed. The legal implications are dramatic. Ohm has catalogued the huge number of privacy laws that rely on anonymization.[222] Many distinguish "personally identifiable information" (PII)—usually defined as name, address, social security number, or telephone number—from other data that is presumed not to reveal identity.[223] The threat of de-identification of sparse sensor-based data sets makes questionable this distinction between PII and other data.

Information privacy scholarship has begun to debate how to address the threat of re-identification. Ohm proposes abandoning the idea of PII completely;[224] Paul Schwartz and Daniel Solove have recently resisted this

---

[219] Larry Hardesty, *How Hard Is It to "De-Anonymize" Cellphone Data?*, MIT NEWS (Mar. 27, 2013).
[220] *See* Jun Han et al., *ACComplice: Location Inference Using Accelerometers on Smartphones*, IEEE 1 (Jan. 2012)
[221] *Id.*
[222] *See* Ohm, *Broken Promises*, *supra* note __ at 1740 ("[A]lmost every single privacy statute and regulation ever written in the U.S. and the EU embraces … the assumption that anonymization protects privacy, most often by extending safe harbors from penalty to those who anonymize their data.").
[223] *See id.* at 1740-41 (cataloging such laws).
[224] *See id.* at 1742 ("At the very least, we must abandon the pervasively held idea that we can protect privacy by simply removing personally identifiable information (PII).").

approach, arguing instead that we should redefine PII along a continuum between identified information, identifiable information, and non-identifiable information.[225] The "identified" category pertains to information that is clearly associated with an individual. The "non-identifiable" pertains to information that carries only a very remote risk of connection to an individual.[226] In the middle are data streams for which there is a non-trivial possibility of future re-identification. Schwartz and Solove argue that the law should treat differently information in these three categories. For merely identifiable information that has not yet been associated with an individual, "[f]ull notice, access, and correction rights should *not* be granted …."[227] In addition, "limits on information use, data minimalization, and restrictions on information disclosure should not be applied across the board to identifiable information."[228] Data security, however, should be protected when dealing with identifiable information.[229]

Others have adopted a similar approach.[230] According to the FTC, three considerations are most relevant: "as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the [FTC's proposed] framework."[231] The FTC's is trying to distinguish, in short, between data that is "reasonably identifiable" and data that is not, as well as between firms that are taking reasonable steps to prevent re-identification.

Although Schwartz and Solove—and the FTC—are trying to use this new, third category of identifiable information to prevent the complete conceptual collapse of all data into the category of PII, that collapse may be inevitable in the Internet of Things context. If sensor data sets are so sparse that easy re-identification is the norm, then *most* Internet of Things data may be "reasonably identifiable." The FTC's standard—and the Schwartz and Solove solution—may mean that in the end all biometric and sensor-based Internet of Things data needs to be treated as PII. That, however, would require a radical re-working of current law and practice. As we will see below, Internet of Things firms currently try to treat sensor data as "nonpersonal." Corporate counsel, regulators, and legislators have not yet faced the reality that Internet of Things sensor data may all be identifiable. In short, privacy law—both on the books and on the ground—is unprepared for the threats created by the Internet of Things.

---

[225] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1877 (2011).
[226] *See id.* at 1878.
[227] *Id.* at 1880.
[228] *Id.*
[229] *See id.* at 1881.
[230] *See* Tene & Polonetsky, *supra* note __ at 46 (adopting Schwartz & Solove's continuum rather than a dichotomy between identifiable and non-identifiable data).
[231] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 22 (2012).

C. SECURITY

Internet of Things devices suffer from a third problem: they are prone to security vulnerabilities for reasons that may not be simple to remedy. More importantly, data security laws—particularly state data breach notification statutes—are unprepared for and don't apply to such security problems. To return to our example, if Fitbit's servers were hacked today, the company would have no legal obligation to inform the public and no legal consequence would likely attach.

i. The Technical Problem: Internet of Things Devices May Be Inherently Prone to Security Flaws

The Internet of Things has recently begun to attract negative attention because of increasing concerns over data security. In November 2013, security firm Symantec discovered a new Internet worm that targeted small Internet of Things devices—particularly home routers, smart televisions, and Internet-connected security cameras—in addition to traditional computers.[232] In the first large-scale Internet of Things security breach, experts estimate that the attack compromised over one hundred thousand devices—including smart televisions, wireless speaker systems, and refrigerators—and used them to send out malicious emails.[233]

Although attention to such issues is on the rise, computer security experts have known for years that small, sensor-based Internet of Things devices are prone to security problems.[234] A team from Florida International University showed that the Fitbit fitness tracker could be vulnerable to a variety of security attacks, and that simple tools could capture data from any Fitbit within 15 feet.[235] The device simply was not engineered with data security in mind.

More dire, insulin pumps have been shown to be vulnerable to hacking. Jay Radcliffe, a security researcher with diabetes, has demonstrated that these medical devices can be remotely accessed and controlled by a

---

[232] *See* Kaoru Hayashi, *Linux Worm Targeting Hidden Devices*, available at http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices (Nov. 27, 2013) (describing the Linux.Darlloz worm).

[233] *See* Elise Hu, *What Do You Do If Your Refrigerator Begins Sending Malicious Emails?*, available at http://www.npr.org (Jan. 16, 2014).

[234] For a useful interview related to this question, see https://soundcloud.com/gigaom-internet-of-things/securing-the-internet-of. *See also* Daniela Hernandez, *World's Health Data Patiently Awaits Inevitable Hack*, Wired (Mar. 25, 2013).

[235] *See* Mahmudur Rahman, Bogdan Carbunar & Madhusudan Banik, *Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device*, arXiv:1304.5672 (Apr. 20, 2013).

hacker nearby to the device's user.[236] Similarly, many insulin pumps communicate wirelessly to a small monitor that patients use to check insulin levels. Radcliffe has shown that these monitors are also easily accessed, leading to the possibility that a malicious hacker could cause a monitor to display inaccurate information, causing a diabetic patient to mis-administer insulin doses.[237]

As a final example, in August, 2013, a Houston couple heard the voice of a strange man cursing in their two year old daughter's bedroom.[238] When they entered the room, the voice started cursing them instead. The expletives were coming from their Internet-connected and camera-equipped baby monitor, which had been hacked. Many other webcam devices have also been found vulnerable: in September, 2013, the FTC took its first action against an Internet of Things firm when it penalized TRENDnet—a web-enabled camera manufacturer—for promising customers that its cameras were secure when they were not.[239]

These examples illustrate the larger technical problem: Internet of Things devices may be inherently vulnerable for several reasons. First, these products are often manufactured by traditional consumer goods makers rather than computer hardware or software firms. The engineers involved may therefore be relatively inexperienced with data security issues, and the firms involved may place insufficient priority on security concerns.[240]

Second, consumer sensor devices often have a very compact form factor. The goal is to make a small health monitor that fits on your wrist, or a health monitor that resides in the sole of your shoe. Small form factors, however, do not necessarily lend themselves to adding the processing power needed for robust security measures such as encryption.[241] In addition, small devices may not have sufficient battery life to support the extra processing required for more robust data security.

Finally, these devices are often not designed to be re-tooled once released into the market. A computer or smart phone contains a complex operating system that can be constantly updated to fix security problems, therefore providing a manufacturer with ongoing opportunities to secure the

---

[236] *See* Jordan Robertson, *Insulin Pumps, Monitors Vulnerable to Hacking*, available at http://news.yahoo.com/insulin-pumps-monitors-vulnerable-hacking-100605899.html.

[237] *See id.*

[238] *See* http://abcnews.go.com/blogs/headlines/2013/08/baby-monitor-hacking-alarms-houston-parents/.

[239] *See* FTC Complaint 1223090 (Sep. 4, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf.

[240] *See* Brian Fung, *Here's the Scariest Part About the Internet of Things*, WASH. POST (Nov. 19, 2013) ("Although the folks who make dishwashers may be fantastic engineers, or even great computer programmers, it doesn't necessarily imply they're equipped to protect Internet users from the outset.").

[241] *See* Stacey Higginbotham, *The Internet of Things Needs a New Security Model. Which One Will Win?*, available at www.gigaom.com (Jan. 22, 2014).

device against new threats. A consumer sensor device, however, is often less malleable and robust. Internet of Things products may thus not be patchable or easy to update.[242]

For all of these reasons, the Internet of Things may be inherently prone to security flaws. The risks go beyond spam. In addition to using these devices as remote servers, there are also endless possibilities for hacking into sensor-based devices for malicious purposes. As computer security expert Ross Anderson recently asked, "[w]hat happens if someone writes some malware that takes over air conditioners, and then turns them on and off remotely? You could bring down the power grid if you wanted to."[243] One could also, of course, spy on an individual's sensor devices, steal their data, or otherwise compromise an individual's privacy. These problems have led some computer security experts to conclude that "without strong security foundations, attacks and malfunctions in the [Internet of Things] will outweigh any of its benefits."[244]

ii. The Legal Problem: Data Security Law is Unprepared

Data security law is unprepared for these Internet of Things security problems. Data security in the U.S. is generally regulated through one of two mechanisms: FTC enforcement or state data breach notification laws. Neither is clearly applicable to breaches of Internet of Things data. Put differently, if your biometric data were stolen from a company's servers, it is contestable whether any state or Federal regulator would have the authority to respond.

First consider the FTC's authority. Because there is no general Federal data security statute,[245] the FTC has used its general authority under the Federal Trade Commission Act (FTC Act)[246] to penalize companies for security lapses. The FTC Act states that "unfair or deceptive acts or practices in or affecting commerce" are unlawful.[247] The FTC has used both the unfair and deceptive prongs of the FTC Act to regulate privacy and security, generally through consent orders with offending firms.[248] In "deception" cases—such as the 2013 TRENDnet webcam action described

---

[242] *See* Bruce Schneier, *The Internet of Things is Wildly Insecure—And Often Unpatchable*, WIRED (Jan. 6, 2014) ("These embedded computers are riddled with vulnerabilities, and there's no good way to patch them.").
[243] *See Spam in the Fridge: When the Internet of Things Misbehaves*, ECONOMIST (Jan. 25, 2014) (discussing Internet of Things security issues).
[244] Rodrigo Roman et al., *Securing the Internet of Things*, 44 COMPUTER 51, 51 (Sept. 2011)).
[245] Certain information types, such as health and financial data, are subject to heightened Federal data security requirements, but no statute sets forth general data security measures.
[246] 15 U.S.C. §§ 41-58.
[247] 15 U.S.C. § 45(a)(1) (2006).
[248] *See e.g.,* FTC v. Accusearch Inc., 570 F.3d 1187, 1194 (10th Cir. 2009) (alleging violating of FTC Act); GeoCities, 127 F.T.C. 94, 96 (1999) (claiming deceptive practices).

above[249]—the FTC demonstrates that a company violated its own statements to consumers. This is a powerful but somewhat limited grounds for enforcement in security cases, because it depends on the company having made overly strong security-related promises to the public.

The FTC has therefore also brought "unfairness" cases to attack poor security practices.[250] In "unfairness" cases, the FTC must show that a firm injured consumers in ways that violate public policy.[251] This is most easy in contexts with Federal statutory requirements about data security, such as finance and healthcare. Outside of those delimited contexts, the FTC's authority is on somewhat shaky ground. Both commentators and firms have increasingly questioned the scope of the FTC's jurisdiction in such cases.[252] Most recently, the Wyndham Hotel Group is litigating that jurisdiction after the FTC alleged that Wyndham had unreasonably exposed consumer information through lax security measures.[253] Although the challenge is pending and the FTC may yet prevail, there is no question that its authority in this area would be considerably strengthened by legislative action to establish data security requirements. I will not rule out that the FTC currently could (and should) try to enforce against an Internet of Things manufacturer for lax security practices in the design or engineering of a consumer device, but it is not absolutely clear that it would prevail.

As a second option, therefore, consider the possible treatment of Internet of Things security violations under state data breach notification statutes. At the very least, one might assume that breaches of potentially sensitive—and difficult to anonymize—sensor data would be made public under such laws, just as theft of credit card data or other personal information requires public disclosure. At the moment, however, that is not the case. Forty-six states have enacted data breach notification laws.[254] All

---

[249] *See supra* notes __-__ and accompanying text.

[250] *See e.g.,* BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467-69 (2005); DSW Inc., 141 F.T.C. 117, 119-20 (2006).

[251] *See* 15 U.S.C. § 45(n) (2006).

[252] *See generally* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673 (2013) (arguing that the FTC's practices may violate the fair notice principle); Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809 (2011) (providing overview of FTC privacy and security enforcement actions and reviewing controversy).

[253] *See* Stegmaier & Bartnick, *supra* note __ (reviewing Wyndham litigation).

[254] *See* Alaska Stat. § 45.48.010 et seq.; Ariz. Rev. Stat. § 44-7501 (2006); Ark. Code § 4-110-101 et seq. (2005); Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82 (2003); Colo. Rev. Stat. § 6-1-716 (2006), as amended (2010); Conn. Gen Stat. 36a-701b (2005), as amended (2012); Del. Code tit. 6, § 12B-101 et seq. (2005); Fla. Stat. § 817.5681 (2005); Ga. Code §§ 10-1-910-912 (2005), as amended (2007); Haw. Rev. Stat. § 487N- 1-4 (2006); Idaho Stat. §§ 28-51-104-107 (2006); 815 ILCS 530/1 et seq. (2006); Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq. (2006), as amended (2009); Ia. Code Ann. §§ 715C.1 et seq. (2008); Kan. Stat. Ann. §§ 50-7a01, 50-7a02 (2006); La. Rev. Stat. § 51:3071 et seq. (2005) Me. Rev. Stat. tit. 10, §§ 1346 et seq. (2005), as amended (2006); Md. Code, Com. Law § 14-3501 et seq. (2007); Mass. Gen. Laws § 93H-1 et seq. (2007); Mich. Comp. Laws § 445.63 et seq. (2006);

of those cover "personal information,"[255] which is generally defined in such statutes as an individual's first and last name plus one or more of their Social Security number, driver's license number, or bank or credit card account information.[256] Thus, for the vast majority of states, a security breach that resulted in the theft of records containing users' names and associated biometric or sensor data would *not* trigger state data breach notification requirements. A breach that only stole sensor data without users' names would also fail to trigger such laws.

A few anomalous states have enacted data breach notification laws that could be interpreted broadly to protect sensor data, but only with some creativity. Two groups of states differ somewhat from the norm described above. The first group includes Arkansas, California, Missouri and Puerto Rico, which all include "medical information" in their definition of "personal information."[257] Missouri defines "medical information" to mean "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional."[258] Thus, if breached sensor data related to "mental or physical condition"—for example, personal fitness tracking data—Missouri's statute might reach the breach. Arkansas, California, and Puerto Rico define "medical information" more narrowly to mean only information "regarding the individual's medical history or medical treatment or diagnosis by a health care professional."[259] These three state statutes seem to have followed the definitions included in HIPAA, which defines "health information" as

---

Minn. Stat. §§ 325E.61, 325E.64 (2005); Miss. Code Ann. § 75-24-29 (2010); Mo. Rev. Stat. § 407.1500 (2009); Mont. Code §§ 30-14-1701-04, 2-6-504 (2005); Neb. Rev. Stat. §§ 87-801-07 (2006); Nev. Rev. Stat. §§ 603A.010 et seq. (2005) N.H. Rev. Stat. §§ 359-C:19-C:21 (2006); N.J. Stat. 56:8-163-66 (2005); N.Y. Gen. Bus. Law § 899-aa (2005); N.C. Gen. Stat §§ 75-65 (2005), as amended (2009); N.D. Cent. Code §§ 51-30-01 et seq. (2005);Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191-192 (2007); Okla. Stat. § 74-3113.1 (2006), § 24-161 et seq. (2008); Oregon Rev. Stat. §§ 646A.600 et seq. (2011); 73 Pa. Stat. §§ 2301-2308, 2329 (2006); R.I. Gen. Laws §§ 11-49.2-1 et seq. (2005); S.C. Code § 39-1-90 (2009); Tenn. Code §§ 47-18-2107, 2010 S.B. 2793 (2005); Tex. Bus. & Com. Code § 521.03 (2007), Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224); Utah Code §§ 13-44-101, et seq. (2006); Vt. Stat. tit. 9 § 2430 et seq. (2006); Va. Code § 18.2-186.6 (2008), § 32.1-127.1:05 (2011); Wash. Rev. Code §§ 19.255.010, 19.255.020, 42.56.590 (2005); W.V. Code §§ 46A-2A-101 et seq. (2008); Wis. Stat. § 134.98 et seq. (2008); Wyo. Stat. §§ 40-12-501, 40-12-502 (2010); D.C. Code § 28- 3851 et seq. (2007); 9 Guam Code Ann. Tit. IX, § 48-10 et seq. (2009); 10 L.P.R.A. §§ 4051 et. seq. (2005), as amended (2008); V.I. Code § 2208, et seq. (2005).

[255] New York's statute covers "private information." *See* McKinney's Gen. Bus. L. § 899-aa(b). Vermont's covers "personally identifiable information." *See* Vt. Stat. Ann. Tit. 9 § 2430(5)(A). The Texas statute covers "sensitive personal information." *See* Tex. Bus. & Comm. Code § 521.002.

[256] *See e.g.,* the state data breach statute standardized form, available at http://www.dataprivacymonitor.com/.

[257] *See* Ark. Code § 4-110-101 et seq. (2005); Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82 (2003); Mo. Rev. Stat. § 407.1500 (2009); 10 L.P.R.A. §§ 4051 et. seq. (2005), as amended (2008).

[258] *See e.g.,* Mo. Rev. Stat. § 407.1500 (2009).

[259] Ark. Code Ann. § 4-110-103(5) (2005); Cal. Civ. Code § 1798.81.5(d)(2) (2004); L.P.R.A. §§ 4051(a) (2005).

"any information, including genetic information, … that is … created or received by a health care provider, health plan, … and … relates to the … physical or mental health or condition of an individual …."[260] HIPAA's definition would most likely *not* encompass fitness or health related—let alone other—potentially sensitive sensor data.

The second group that differs from the norm includes Iowa, Nebraska, Texas and Wisconsin, all of which include an individual's "unique biometric data" in their definitions of "personal information."[261] Both Nebraska and Wisconsin define "unique biometric data" to include fingerprint, voice print, and retina or iris image, as well as any "other unique physical representation."[262] This phrase might be interpreted to include at least some fitness or health-related sensor data. Texas goes further. Its statute is triggered by any breach of "sensitive personal information," which includes information that identifies the individual and relates to the physical or mental health or condition of the individual.[263] This quite clearly would protect at least fitness-related sensor data.

Thus, in a small minority of states, health or fitness-related sensor data—such as data produced by a Breathometer, FitBit, Nike FuelBand, blood glucose monitor, blood pressure monitor, or other device—could arguably be protected by the state's data breach notification law. In most, theft or breach of such data would not trigger public notification. Moreover, *none* of these state statutes would be triggered by data security breaches into data sets containing other types of sensor data discussed in Part I. Driving-related data, for example, would nowhere be covered; location, accelerometer, or other data from a smartphone would nowhere be covered; smart grid data or data streaming out of Internet of Things home appliances would nowhere be covered. Put most simply, current data security breach notification laws are ill prepared to alert the public of security problems on the Internet of Things.

D. CONSENT

Discrimination, privacy, and security concerns about the Internet of Things underscore the new and unique ways in which connected sensor devices could harm consumer welfare. At the same time, the quick and massive growth in this market shows consumer desire for these technologies. Consumer consent offers one way to reconcile these competing realities: if consumers understand and consent to the data flows generated by their FitBits, car monitors, smart home devices, and smart

[260] 45 C.F.R. § 160.103.
[261] *See* Ia. Code Ann. §§ 715C.1 et seq. (2008); Neb. Rev. Stat. §§ 87-801-07 (2006); Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224); Wis. Stat. § 134.98 et seq. (2008).
[262] *See* Neb. Rev. Stat. §§ 87-802(5) (2006); Wis. Stat. § 134.98. (2008).
[263] Tex. Bus. & Com. Code § 521.002(a)(2) (2007) (emphasis added).

phones, perhaps there is no reason to worry. Unfortunately, consent is unlikely to provide such reassurance. Internet of Things devices complicate consent just as they complicate discrimination, privacy, and security. Moreover, consumer protection law related to privacy policy disclosures is currently unprepared to deal with these issues.

i. The Technical Problem: Sensor Devices Confuse Notice and Choice

Notice and choice—in other words, consumer consent—has been the dominant approach to regulating the Internet for the last decade. Regulators, legislators, and scholars have largely depended on the assumption that so long as firms provide accurate information to consumers and consumers have an opportunity to choose or reject those firms' web services, most data-related issues can be self-regulated. Unfortunately, these already stretched assumptions apply uncomfortably in the context of the consumer goods at the heart of the Internet of Things.

Internet of Things devices are often small, screen-less, and lacking an input mechanism such as a keyboard or touchscreen. A fitness tracker, for example, may have small lights and perhaps a tiny display, but no means to confront a user with a privacy policy or secure consent. Likewise, a home electricity or water sensor, connected oven or other appliance, automobile tracking device, or other Internet of Things object will not have input and output capabilities. The basic mechanism of notice and choice—to display and seek agreement to a privacy policy—can therefore be awkward in this context because the devices in question do not facilitate consent.

This inherently complicates notice and choice for the Internet of Things. If an Internet user visits a web page, the privacy policy is available on that page. Although this does not perfectly protect consumer welfare, it at least provides a consumer with the option to review privacy and data-related terms at the locus and time of use. Internet of Things devices, however, are currently betwixt and between. A device most likely has no means to display a privacy notice. As a result, such information must be conveyed to consumers elsewhere: in the box with the device, on the manufacturer's web site, or in an associated mobile application.

At the moment, Internet of Things manufacturers overwhelmingly seem to prefer to only provide privacy and data-related information in web site privacy policies. Appendix A shows the results of my survey of twenty popular Internet of Things consumer devices, including FitBit and Nike Fuelband fitness trackers, the Nest Thermostat, the Breathometer, and

others.[264] For many of the surveyed devices I actually purchased the object in order to inspect the packaging and examine the consumer's experience of opening and activating the device. For others I was able to download or secure from the manufacturer the relevant material included in the device packaging—generally the consumer user or "quick start" guides.

As indicated in Appendix A, *none* of the twenty devices included privacy or data-related information in the box. None even referred in the packaging materials or user guides to the existence of a privacy policy on the manufacturer's web site. This is reasonably surprising, given that many of these devices are for sale in traditional brick and mortar stores and not only through the manufacturer's web site, making it possible for a consumer to purchase such a device with no notice that it is subject to a privacy policy.

Internet of Things manufacturers may currently depend on web site posting of privacy policies for at least two reasons. First, they may be accustomed to including such information on a web site and may not have considered that a consumer purchasing an object experiences that purchase somewhat differently than a user browsing the Internet. Second, they may believe that because Internet of Things devices generally require pairing with a smartphone app or Internet account through the manufacturer's web service, the consumer will receive adequate notice and provide adequate consent when downloading that app or activating their online account.

This belief would be unjustified. Appendix A shows that for several of the products reviewed it was extremely difficult to even locate a relevant privacy policy. Consider just one example. iHealth manufacturers various health and fitness devices, including an activity and sleep tracker, a pulse oximeter, a blood pressure wrist monitor, and a wireless body analysis scale. All of these work together through the iHealth smartphone or tablet application.[265] The privacy policy on the iHealth web site, however, applies only to use of that web site—not to use of iHealth products or the iHealth mobile app.[266] This suggests that iHealth assumes users will confront a second product-related privacy notice when activating the mobile app to use their products. At installation, that app presents users with a software license agreement, which states that by using the app users may upload personal information, including vital signs and other biometric data.[267] The agreement also states that "[o]ur use of Personal Data [and] VITALS [biometric data] is outlined in our Privacy Policy."[268] At no point, however, is a user confronted with that product-related policy, nor told where it can be located. Were a user to look on the iHealth web site, she would find only the policy posted there that applies to use of the site, not to use of iHealth products.

---

[264] *See* Appendix A.
[265] *See* http://www.ihealthlabs.com.
[266] *See id.*
[267] *See* iHealth Software License Agreement (on file with author).
[268] *Id.*

Within the mobile iHealth app, the only mention of privacy is found under the Settings function in a tab labeled "Copyright." That Copyright tab actually includes the application's Terms of Use, which again references a privacy policy that governs product use and sensor data but provides no information on where to find that policy. In short, even an interested consumer seeking privacy information about iHealth products and sensor data is led in an unending circle of confusion. This is a horrendous example of how not to provide consumers with clear notice and choice about privacy information.

Appendix A lists other examples nearly as confusing. Some policies seem to apply to both web site use and sensor device use. Other policies limit their application to web site use, not sensor device use, but provide no means to locate a device-related privacy policy. This leaves unanswered whether *any* privacy-related policy applies to the data generated by these devices.[269] In still other cases, two privacy policies vie for users' attention: one for web site use, one for sensor device use. In some ways this is a better approach, because it provides clear notice that the sensor device comes with a unique set of data-related and privacy issues. At the same time, this doubles the cognitive and attentional load on consumers, who already fail to read even one privacy policy. This approach may also create confusion if consumers see the web site policy and fail to realize that a second policy exists related to their sensor data.

In addition to the problem of *finding* a relevant privacy policy, Appendix A shows that even when one locates a policy that applies to use of these products and the sensor data they generate, many current Internet of Things privacy policies provide little real guidance to consumers. My review of these twenty products and their privacy policies reveals two major problems.

First, these policies are often confusing about whether sensor or biometric data count as "personal information," and thus unclear about how such data can be shared with or sold to third parties.[270] Some of these policies define "personal information" (or "personally identifiable information") in a very traditional manner, as including only name, address,

[269] In at least one case, the web site privacy policy stated that a second sensor device policy existed, but the policy was not actually available anywhere online. *See* http://www.propellerhealth.com/privacy/ ("This privacy policy is for users of the website only, the product-related privacy policy is different, and can be reviewed in our User Agreement.").

[270] This problem extends beyond Internet of Things policies. *See* Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 458 (2013) (providing an empirical review of terms of service and privacy policies for cloud computing services and concluding—as with my review here in the Internet of Everything context—that such policies rarely provide much detail on firms' obligations to consumers).

email address, or telephone number.[271] For such policies, sensor data would not be given the heightened protections afforded to personally identifiable information.

Other policies are significantly less clear. Some include language that might be interpreted to include sensor data. Breathometer's privacy policy, for example, defines "personal information" as "information that directly identifies you, or that can directly identify you, such as your name, shipping and/or billing address, e-mail address, phone number, and/or credit card information."[272] Although this would generally suggest that sensor data are not included, a computer scientist or regulator that understands the problem of re-identification might interpret this to mean that test results *were* included as personal information. The Breathometer privacy policy adds to the confusion. In a section titled "Personal information we affirmative collect from you," the policy states that "[u]ser-generated content (such as BAC Test results) may include Personal Information."[273] This further confuses whether the company will treat sensor readings from a Breathometer as personal information under the policy.

Similarly, the Nest Thermostat's privacy policy defines "personally identifiable information" as "data that can be reasonably linked to a specific individual or household."[274] Given the threat of re-identification of Internet of Things sensor data, it is entirely unclear whether the policy's drafters consider Nest Thermostat data to be personally identifiable. This same issue arises in the Belkin WeMo home automation system privacy policy. That policy defines personal information as "any information that can be used to identify you." One might therefore believe this to include sensor data if such data is easily re-identified. The policy then goes on, however, to state that "non-personal information" includes "usage data relating to … Belkin Products …."[275] In other words, the policy creates conflict between its definition of "personal information" and "non-personal information."

This definitional wrangling matters. Most privacy policies permit manufacturers to share or sell non-personal information far more broadly than personal information. The LifeBeam Smart Helmet privacy policy, for example, allows non-personal information to be collected, used, transferred, and disclosed for any purpose, but states that "LifeBeam does not disclose personally-identifying information."[276] In addition, certain other terms in these privacy policies apply only to personal information. For example, the Breathometer policy contractually provides for user notification in the event of a security breach that compromises personal information. Because the

[271] *See* Appendix A.
[272] http://www.breathometer.com/lega/privacy-policy.
[273] http://www.breathometer.com/legal/privacy-policy.
[274] https://nest.com/legal/privacy-statement/.
[275] http://www.belkin.com/us/privacypolicy/.
[276] *See* http://www.life-beam.com/privacy.

policy leaves unclear whether sensor data are personal information, it is unclear whether a user should expect notification in the event that sensor data were breached. Similarly, the MimoBaby Onesie policy gives broad access, correction, and deletion rights to users for "personal information" but makes no mention of how such rights apply to other information.[277]

In short, these Internet of Things privacy policies are often quite unclear about whether collected sensor data count as "personal information"—and therefore ambiguous as to what rights and obligations apply to such data.

Second, the privacy policies for these devices often do not address several important issues relevant to consumers. For example, privacy policies for consumer sensor devices often do not mention ownership of sensor data. Of the twenty products covered by Appendix A, only three discussed data ownership explicitly. Of those that did clarify ownership of sensor data, all three indicated that the *manufacturer*, not the consumer, owned the sensor data in question.[278] The BodyMedia Armband's policy, for example, states that "[a]ll data collected including, but not limited to, food-logs, weight, body-fat-percentage, sensor-data, time recordings, and physiological data … are and shall remain the sole and exclusive property of BodyMedia."[279] The MyBasis Sports Watch policy similarly states that "[a]ll Biometric Data shall remain the sole and exclusive property of BASIS Science, Inc."[280] It is only some consolation that at least ownership is clear in these few cases.

Similarly, these policies often do not specify exactly what data the device collects or which types of sensors the device employs. Of the twenty products reviewed, only three provided clear information on exactly what sensors the product included or what sensor data the product collected.[281] A few more provided some information on data collected without complete detail. For example, the privacy policy relevant to the Automatic Link automobile monitor describes that the device collects location information, information on "how you drive," error codes from the car's computer, and information from both the car's sensors and the device's sensors.[282] The policy does not give detail about what car or device sensors are used or what exactly the device records about "how you drive." Moreover, Appendix A shows that many of these Internet of Things privacy policies provided *no* information on what sensor data their device generated.

---

[277] *See* http://mimobaby.com/terms/.
[278] *See* Appendix A.
[279] http://www.bodymedia.com/Support-Help/Policies/Privacy-Policy.
[280] http://www.mybasis.com/legal/privacy.
[281] *See* Appendix A (Basis Sports Watch, MimoBaby Onesie monitor, Nest Thermostat or Smoke Detector).
[282] *See* http://www.automatic.com/legal/.

These policies are likewise inconsistent in the access, modification, and deletion rights they give consumers. Most of the twenty policies I reviewed said nothing about such rights. None provided an easy mechanism for *exportation* of raw sensor data. And many were quite confusing about what access, modification, and deletion rights a consumer had. These privacy policies sometimes gave users such rights for personal information but not for other (non-personal) information. As discussed,[283] it is often unclear whether sensor or biometric data count as "personal information," and therefore unclear whether users have modification and deletion rights vis-à-vis those data.

Finally, none of these policies explained how much sensor data were processed on the device itself versus transmitted to and processed on the company's servers remotely. Only three detailed whether encryption techniques were used or what techniques were specifically employed. (The Basis Sports Watch and MimoBaby Onesie monitor privacy policies state that biometric data are not encrypted; the Nest Thermostat states that data are encrypted.) None detailed the security measures built into the device itself to prevent security breach.

In short, these policies seem to have been shaped by the needs and expectations relevant to the normal Internet, not the Internet of Things. Not surprisingly, at the dawn of the Internet of Things, there may not yet have been much real consideration of the special issues that Internet of Things privacy policies should address.[284]

ii. The Legal Problem: Consumer Protection Law is Unprepared

As discussed above, the FTC's mandate is to police deceptive and unfair trade practices.[285] In the privacy policy context, this includes taking action against firms that violate their posted privacy policies[286] as well as providing soft guidance to firms on what constitutes adequate notice in a privacy policy.[287] Although the FTC held its first public workshop on the Internet of Things in November, 2013, it has yet to release guidelines or

---

[283] *See supra* notes __-__ and accompanying text.

[284] There has been some academic work on Internet of Things privacy policies, but nothing in mainstream legal scholarship. *See e.g.,* Sebastian Speiser et al., *Web Technologies and Privacy Policies for the Smart Grid*, INDUST. ELECT. SOC. 4809 (2013); R.I. Singh et al., *Evaluating the Readability of Privacy Policies in Mobile Environments*, 3 INTL. J. OF MOB. HUM. COMP. INTERACTION (2011).

[285] *See supra* notes __-__ and accompanying text.

[286] *See e.g., In the Matter of GeoCities, Inc.*, FTC Docket No. C-3850 (Feb. 5, 1999) (first FTC privacy policy action).

[287] *See* FTC, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.htm (2007). Various commentators have called for more substantive or legislative guidance on what terms should be included in online privacy policies. *See* Kesan, Hayes & Bashir, *supra* note __ at 459 (calling for substantive regulatory steps to provide baseline terms in privacy policies).

policy recommendations specifically related to privacy policies on the Internet of Things. Manufacturers therefore have no tailored guidance from the FTC about what constitutes adequate notice in Internet of Things privacy policies.

California's Office of Privacy Protection has taken the lead among states in setting out recommended practices on privacy policies.[288] California's Online Privacy Protection Act (COPPA)[289] requires a firm operating a "commercial web site or online service" that collects personally identifiable information to post a privacy policy, either on the web site or, in the case of an "online service," through "any other reasonably accessible means of making the privacy policy available to consumers of the online service."[290] The policy must identify the categories of PII collected and types of third parties with whom the company shares information.[291] If the firm provides consumers a mechanism to access or correct PII, the policy must explain that process.[292] In 2008, the California Office of Privacy Protection issued non-binding guidelines for compliance with these requirements. These guidelines urge firms to include in their privacy policies information on how they collect personal information, what kinds of personal information they collect, how they use and share such information with others, and how they protect data security.[293] In addition, California has recently promulgated guidelines for how best to adapt privacy policies to the smaller screens of mobile phones.[294]

Internet of Things firms clearly trigger COPPA's requirement to have a privacy policy, either because they maintain a web site or because they operate an "online service." They must thus disclose the types of PII collected and the categories of third parties with whom they share that PII. This is precisely what we see in existing policies, as discussed above. Because neither the FTC nor California—nor any other relevant legislative or regulatory actor—has set forth requirements specifically applicable to the Internet of Things context, firms are undoubtedly using these baseline web site requirements as a minimal safe harbor. They are promulgating privacy policies that meet legal requirements created for the Internet, not the Internet of Things.

---

[288] *See* CALIFORNIA OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON CALIFORNIA INFORMATION-SHARING DISCLOSURES AND PRIVACY POLICY STATEMENTS (2008).
[289] *See* Calif. Bus. & Prof. Code §§ 22575-22578.
[290] Calif. Bus. & Prof. Code § 22577(b)(5).
[291] *See* Calif. Bus. & Prof. Code § 22575(b).
[292] *See id.*
[293] *See* CALIFORNIA OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON CALIFORNIA INFORMATION-SHARING DISCLOSURES AND PRIVACY POLICY STATEMENTS 12-14 (2008).
[294] *See* CALIFORNIA ATTORNEY GENERAL, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013).

In short, consumer protection law is essentially unprepared for the Internet of Things. Clearly firms cannot post deceptive privacy policies for Internet of Things devices, but that is relatively little comfort. Neither the FTC nor California has provided substantive guidance on information disclosure for Internet of Things devices. California's privacy policy law has not been revised since 2008, long before the Internet of Things began to take shape. Not surprisingly, then, notice and choice is off to a rocky start in the Internet of Things context.

III. FOUR (MESSY & IMPERFECT) FIRST STEPS

Let us review the argument to this point. The Internet of Things is developing rapidly as connected sensor-based consumer devices proliferate. Millions of health and fitness, automotive, home, employment, and smart phone devices are now in use and collecting data on consumers' behaviors. These sensor-based data are so granular and high quality that they permit often profound and unexpected inferences about personality, character, preferences, and even intentions. The Internet of Things thus gives rise to difficult discrimination problems, both because seemingly innocuous sensor data might be used as proxies in illegal racial, age, or gender discrimination and because highly tailored economic sorting is itself controversial. In addition, Internet of Things data are difficult to anonymize, creating privacy problems, and difficult to secure. Finally, notice and choice is an ill fitting solution to these problems, both because Internet of Things devices may not provide consumers with inherent notice that data rights are implicated in their use and because sensor device firms seem stuck in a notice paradigm designed for web sites rather than connected consumer goods. Currently, discrimination, privacy, security, and consumer welfare law are all unprepared to handle the legal implications of these new technologies.

This Part does not propose a grand solution to these problems. I do not call for a new Federal statute or urge the creation of a new regulatory agency. Such solutions would be elegant but implausible, at least at the moment. Scholars have argued for such comprehensive privacy reforms for the last decade,[295] and Congress has ignored them. The futility of such large scale projects thus leads me to suggest smaller and more eclectic first steps that have some chance of actual effect.

I do not attempt to impose a theoretically consistent approach on these four first steps. One might, for example, demand procedural due process for consumers[296] or argue for state (as opposed to Federal) or

[295] *See e.g.,* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006).

[296] *See* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 126-127 (2014) (calling for procedural due process to protect information privacy).

Federal (as opposed to state) intervention. I walk a different line, making use of both procedural and more substantive solutions as well as both Federal and state reforms. My purpose is not to propose a course that is perfectly consistent, but instead one that can be realistic and pragmatic. I therefore suggest four messy and imperfect first steps towards regulating the Internet of Things: (1) broadening existing use constraints—such as some state law on automobile event data records—to dampen discrimination; (2) redefining "personally identifiable information" to include biometric and other forms of sensor data; (3) protecting security by expanding state data breach notification laws to include security violations related to the Internet of Things; and (4) improving consent by providing guidance on how notice and choice should function in the context of the Internet of Things.

My goal is to provoke regulatory and scholarly discussion, as well as to provide initial guidance to corporate counsel advising Internet of Things firms at this early stage. In this I borrow from recent work by Bamberger and Mulligan, who have argued persuasively that chief privacy officers and corporate counsel need such guidance on how to uphold consumer expectations.[297] If privacy regulation focuses exclusively on procedural mechanisms for ensuring notice and choice, corporate decision-makers will likewise focus on such procedural moves. They will tweak their privacy policies, enlarge their fonts, and add more bells and whistles to such policies to try to satisfy regulators. But such hoop-jumping may have little real impact on consumer welfare. Providing substantive guidance to corporations, however, may lead corporate decision-makers down a different path. If legislators, regulators, and the privacy community make clear their substantive expectations for the Internet of Things, corporations will likely use such norms as guidance for what consumers expect and demand. This is the "privacy-protective power of substantive consumer expectations overlaid onto procedural protections …."[298]

My goal in this Part is to suggest ways in which regulators, legislators, and privacy advocates can begin to provide such substantive guidance to the firms creating the Internet of Things. The Part concludes with a public choice argument for urgency—suggesting that we can and must move quickly to set guidelines and ground rules before economic interests in the Internet of Things ecosystem become overly entrenched and immovable.

A. A REGULATORY BLUEPRINT FOR THE INTERNET OF THINGS

i. Dampening Discrimination With Use Constraints

[297] *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 298 (2011) ("Most simply, decisions at the corporate level might provide the best way to avoid privacy harms.").
[298] *Id.* at 300.

Use constraints—or "don't use" rules[299]—are common across the law. Fifth Amendment jurisprudence prohibits a jury from drawing negative inferences from a defendant's failure to testify; the FCRA bars creditors from denying credit on the basis of bankruptcies more than ten years old; and the Genetic Information Nondiscrimination Act (GINA) bars the use of genetic information by health insurers.[300] Such rules "rest on a social judgment that even if transacting parties both wish to reveal and use a particular piece of information, its use should be forbidden because of some social harm, such as discriminating against those with genetic disorders, that is greater than the social benefits, such as the allocative and contractual efficiency created by allowing freedom of contract."[301]

As a first regulatory step, we should constrain certain uses of Internet of Things data if it threatens consumer expectations. This approach is substantive rather than procedural, and sectoral rather than comprehensive.[302] The advantages of such an approach include that one can tailor such constraints to each particular context and prioritize those contexts that present the most risk of consumer harm. In addition, one can sometimes mobilize legislators and regulators that become concerned about discriminatory uses of information in a particular context and galvanized about that type of use, but who might not adopt more widespread, systemic reforms.

Consider two broad categories of—and justifications for—use constraints: constraints on cross-context use of data and constraints on forced data revelation even within a given context.

(1) Cross-Context Use Constraints

First, borrowing from Helen Nissenbaum's work on the importance of restraining cross-context data flows to protect consumer privacy,[303] privacy advocates should focus on keeping Internet of Things data use from violating contextual boundaries. Some choices will be easy. Racial, gender, age, and other forms of already illegal discrimination are likely to generate immediate and sympathetic responses. If an employer, insurer, or other economic actor were to begin using Internet of Things data as a proxy for race or other protected characteristics, legislators and regulators are sure to react.

---

[299] *See* Peppet, *Unraveling Privacy*, *supra* note __ at 1199 (discussing don't use rules).
[300] *See id.* at 1199-1200 (providing citations).
[301] *Id.* at 1200.
[302] In contrast, for example, consider a recent proposal by Tene & Polonetsky calling for increased decisional transparency—requiring organizations that *use* data to disclose how they do so and for what purposes. *See* Tene & Polonetsky, *supra* note __ at 85-86 ("[W]e propose that organizations reveal not only the existence of their databases but also the *criteria* used in their decisionmaking processes ….").
[303] *See* Nissenbaum, *supra* note __.

Beyond racial and other forms of illegal discrimination, there is some reason for optimism, however, that use constraints are possible to dampen economic discrimination based on cross-context use of Internet of Things data. State legislatures—far more so than Congress—have enacted a variety of use constraints that protect consumers' information. For example, although relatively little attention has been paid in the legal literature to the use of diverse sources of information in credit scoring,[304] there has been some debate over whether lenders should be permitted to access social media—Facebook, LinkedIn, Twitter—to factor one's social context into credit determinations.[305] Similarly, controversy erupted a few years ago when it was publicized that auto insurers were factoring FICO credit scores into auto insurance rate-setting. Consumer groups protested that this cross-context use of information was unfair and opaque to consumers.[306] Finally, several states, including California, Connecticut, Hawaii, Illinois, Maryland, Oregon, and Washington, have passed laws limiting employers' consideration of credit reports,[307] even though research has shown that credit scores correlate with traits such as impulsivity, self-control or impatience, and trustworthiness.[308] Such traits are relevant to employers—but inferences drawn from one context can be disturbing if used in another.[309]

Similarly, state legislators may be galvanized to take action on the use of data emerging from the many Internet of Things devices that track and measure two of our most privacy-sensitive contexts: the body and the home. Although fitness, health, appliance use, and home habit data may be economically valuable in employment, insurance, and credit decisions, it is also likely that the public will react strongly to discrimination based on such sensitive information.

---

[304] *See e.g.,* Nate Cullerton, Note, *Behavioral Credit Scoring*, 101 GEO. L.J. 807, 808 (2013) ("Although much scholarly attention has been paid to the privacy implications of online data mining and aggregation … for use in targeted behavioral advertising, relatively little attention has been focused on the adotion of these techniques by lenders."); Lea Shepard, *Toward a Stronger Financial History Antidiscrimination Norm*, 53 B.C. L. REV. 1695 (2012) (exploring the use by employers of credit reports and financial histories in the hiring process).

[305] *See e.g. Stat Oil: Lenders Are Turning to Social Media to Assess Borrowers*, THE ECONOMIST (Feb. 9, 2013).

[306] *See* Herb Weisbaum, *Insurance Firms Blasted for Credit Score Rules*, NBC NEWS.COM (Jan. 27, 2010).

[307] *See* Cal. Lab. Code § 1024.5 (West Supp. 2012); Conn. Gen. Ann. § 31-51 (West Supp. 2012); Haw. Rev. Stat. Ann. § 378-2(a)(8) (2011); 820 Ill. Comp. Stat. 70/10 (2010); (Md. Code Ann., Lab. & Empl. § 3-711 (2011); Or. Rev. Stat. § 659A.320 (2011); Wash. Rev. Code § 19.182.020 (2007).

[308] *See* Shweta Arya, Catherine Eckel & Colin Wichman, *Anatomy of the Credit Score*, 95 J. ECON. BEHAV. & ORG. 175 (2013); Stephan Meier & Charles Sprenger, *Time Discounting Predicts Creditworthiness*, 23 PSYCH. SCI. 56 (2012).

[309] *See e.g.,* Ruth Desmond, Comment, *Consumer Credit Reports and Privacy in the Employment Context: The Fair Credit Reporting Act and the Equal Employment for All Act*, 44 U.S.F. L. REV. 907 (2010).

Advocates, regulators, and legislators might therefore consider these two domains as worthy candidates for cross-context use constraints. First, the explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging. At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decision-making. A woman tracking her fertility should not fear that a potential employer could access such information and deny her employment; a senior employee monitoring his fitness regime should not worry that his irregular heart rate or lack of exercise will lead to demotion or termination; a potential homeowner seeking a new mortgage should not be concerned that in order to apply for a loan she will have to reveal her fitness data to a bank as an indicator of character, diligence, or personality.

Second, Internet of Things devices in the home should be similarly protected. As indicated,[310] it is relatively easy to draw powerful inferences about a person's character from the intimate details of her home life. Whether and how often a person comes home late at night, how regularly she cooks for herself, how often she uses her vacuum to clean her home, with what frequency she leaves her oven on or her garage door open as she leaves the house, whether she turns on her security system at night—all of these intimate facts could be the basis for unending inference. Currently there is little to prevent a lender, employer, insurer, or other economic actor from seeking or demanding access to such information. Given the personal nature of such data, however, this seems like a ripe area for cross-context use constraints to prevent such invasive practices.

Some will undoubtedly object to this call for cross-context use constraints, arguing that the economic benefits of using such data to tailor economic decisions outweigh any social costs. I disagree. Just because everything may reveal everything on the Internet of Things, it does not follow that all uses of all data necessarily benefit social welfare. If any contexts demand respect and autonomy, the body and the home seem likely candidates. Moreover, for the Internet of Things to flourish, consumers must be reassured that overly aggressive, cross-context uses of data will be controlled. Early research suggests, for example, that consumers have been slow to adopt car insurance telematics devices out of fear that their driving data will leak into other contexts such as employment.[311] Research on

---

[310] *See* Part I(B).

[311] *See* Johannes Paefgen et al., *Resolving the Misalignment Between Consumer Privacy Concerns and Ubiquitous IS Design: The Case of Usage-Based Insurance*, 33RD INTL. CONF.

personal fitness monitors reveals similar fears.[312] Reasonable constraints on cross-context data use will likely facilitate, not inhibit, the development of the Internet of Things.

(2) Constraints on Forced Disclosure Even Within a Given Context

As a second category, legislators should consider use constraints *within* a given context to prevent forced disclosure of sensitive Internet of Things data. Whereas cross-context use constraints derive their legitimacy from privacy theory that shows that context-violating data use threatens consumer expectations and welfare, this second type of within-context use constraints is grounded in the assumption that consumers should not be forced to reveal certain information through economic or other pressure.

To understand this second type of use constraint and how it differs from cross-context constraints, return to the example of automobile event data recorders. Privacy advocacy groups have argued for use constraints in this context. The Electronic Privacy Information Center (EPIC), for example, has urged the NHTSA to limit use of EDR data.[313] In particular, EPIC has argued that insurers should be forbidden from requiring access to EDR data as a condition of insurability, using EDR data for premium assessment, or conditioning the payment of a claim on the use of such data.[314] Likewise, several states have passed laws limiting EDR data use.[315] Four states currently forbid insurance companies from requiring that an insured consent to future disclosure of EDR data, or from requiring access to EDR data as a condition of settling an insurance claim.[316] One state—Virginia—also forbids an insurer from adjusting rates solely based on an insured's refusal to provide EDR data.[317]

These statutes illustrate how use constraints can substantively limit data use *within* a given context. They enact the judgment that insurers

---

ON INFO. SYS. 1, 2 (2012) ("[T]he slow diffusion rate of [usage based insurance] has been attributed to [privacy concerns] among potential customers.").

[312] *See* Part III(A)(iv) (discussing research on consumer expectations).

[313] Electronic Privacy Information Center, Comments to the National Highway Traffic Safety Administration (Feb. 11, 2013) (on file with author).

[314] *Id.*

[315] Thirteen states have passed laws related to EDR data. *See* Ark. Code § 23-112-107; Calif. Veh. Code § 9951; Colo. Rev. Stat. § 12-6-401-403; Conn. Gen. Stat. § 14-164aa; Me. Rev. Stat. Ann. Tit. 29-1 § 1971-1973; Nev. Rev. Stat. § 484D.485; N.H. Rev. Stat. § 357-G:1; N.Y. Veh. & Traffic Code § 416-b; N.D. Cent. Code § 51-07-28; Ore. Rev. Stat. §§ 105.925-.948; Tex. Trans. Code § 547.615; Va. Code § 38.2-2212(C)(s), § 38.2-2213.1, § 46.2-1088.6, § 46.2-1532.2; Wash. Code § 46.35.010-.050.

[316] *See* Ark. Code § 23-112-107; N.D. Cent. Code § 51-07-28; Ore. Rev. Stat. §§ 105.925-.948; Va. Code § 38.2-2212(C)(s).

[317] Va. Code § 38.2-2213.1 ("No insurer … shall reduce coverage, increase the insured's premium, apply a surcharge, refuse to apply a discount …, place in a less favorable tier, refuse to place in the company's best tier … solely because a motor vehicle owner refuses to allow an insurer access to recorded data … from a recording device ….").

should not use economic pressure to force consumers to reveal automobile sensor data. Other states should consider enacting these restrictions on EDR data.

In addition, however, state legislatures should broaden these statutes. Most of these state statutes currently would not cover the data generated by consumer driving and automobile monitors, such as the Automatic Link sensor device described in Part I. Several states, including Arkansas,[318] California,[319] Colorado,[320] Nevada,[321] New Hampshire,[322] and Texas,[323] limit their EDR statutes to factory or manufacturer-installed data recorders. These statutes thus do not apply to a consumer-installed after market device. Other states, including Oregon,[324] Connecticut,[325] and Utah,[326] limit their statutory protections only to devices that record vehicle data just prior to or after a crash event. Again, this would—somewhat ironically—exclude Internet of Things devices such as the Automatic Link that record far *more* information around-the-clock.

Two states—Virginia and Washington—have enacted broader EDR statutes that would protect Internet of Things data from compelled use by an insurer. Virginia and Washington define a "recording device" broadly as "an electronic system … that primarily … preserves or records … data collected by sensors … within the vehicle."[327] If other states adopt new EDR statutes—or states with existing but limited EDR statutes consider revision—they should extend their statutory protections to data collected by after-market consumer Internet of Things devices, not merely manufacturer-installed crash-related EDRs. Doing so will ensure that consumers can experiment with the Internet of Things without fear that an insurance company will compel revelation of their data.

In addition, however, states considering new or revised EDR statutes should take seriously the threat that everything reveals everything. Use constraints could restrict the use of automobile and driving data for employment, credit, and housing decisions, as well as for insurance decisions outside of the car insurance context (e.g., health or life insurance, for example), when the decision in question does not directly relate to driving. Thus, if an employer wanted access to driving data from its fleet of

---

[318] *See* Ark. Code § 23-112-107(a)(2).
[319] *See* Calif. Veh. Code § 9951(b).
[320] *See* Colo. Rev. Stat. § 12-6-401(2).
[321] *See* Nev. Rev. Stat. § 484D.485(6).
[322] *See* N.H. Rev. Stat. § 357-G:1(II).
[323] *See* Tex. Trans. Code. § 547.615(a)(2).
[324] *See* Ore. Rev. Stat. § 105.925(1) (borrowing definition from Federal statute 49 C.F.R. § 563.5(b)).
[325] *See* Conn. Gen. Stat. § 14-164aa(1).
[326] *See* Utah Rev. Code § 41-1a-1502(2) (borrowing definition from Federal statute 49 C.F.R. § 563.5(b)).
[327] Va. Code § 46.2-1088.6(A); Wash. Code § 46.35.010(2).

vehicles in order to improve fleet efficiency or oversee its drivers' safety, such directly-related uses should be permitted. But if an employer sought access to an employee's personal Internet of Things data to make hiring or other employment decisions, a state EDR statute should prevent forced revelation of such information.

By this point it might seem overly detailed to consider this one example—automobile EDR data—so carefully. I predict, however, that the control of Internet of Things data will have to happen in this fine-grained way. Each context, device, or type of data will need to be considered. The opportunities and risks of discrimination based on that data will have to be weighed. And legislators will have to decide whether allowing such sensor data to leak into unexpected and sensitive contexts harms consumer welfare.

Various contexts are ripe for consideration. One can easily imagine health and life insurers demanding or seeking access to fitness and health sensor data or home insurers demanding access to home monitoring system data. As such data become more detailed, sensitive, and revealing, states might consider prohibiting insurers from conditioning coverage on their revelation. The Nest Smoke Detector, for example, not only alerts a consumer about smoke alarms, but also contains motion sensors that track how and when users inhabit different parts of their homes.[328] Although such information might be useful to a home insurer to investigate a fire or casualty claim, it seems invasive to permit insurers to demand such detailed information as a condition of insurance.

Similarly, legislators might consider within-context constraints on employers who demand disclosure of personal Internet of Things data streams. The LumoBack posture sensor, for example, is a strap that one wears around one's mid-section.[329] It constantly monitors one's posture and can aid in recovery for back injuries. One can imagine an employer becoming quite interested in such data if it were prosecuting a worker's compensation claim or investigating an employee's work habits in a factory or warehouse. Forcing disclosure of such information, however, will likely kill consumer interest in such devices over time. Reasonable within-context use constraints might dampen these problems.

Some will no doubt object that within-context use constraints are overly paternalistic and will prevent certain consumers from making use of their Internet of Things data to distinguish themselves in the market as good, trustworthy, diligent economic actors. I have argued elsewhere that forced disclosure is and will likely become increasingly problematic as biometric and other sensors proliferate.[330] There is no reason to repeat that long and somewhat complex argument here. For now, I will simply conclude that

[328] *See* http://www.nest.com.
[329] *See* http://www.lumoback.com.
[330] *See* Peppet, *Unraveling Privacy*, *supra* note __.

Internet of Things devices are likely to create a variety of within-context forced disclosure examples that may provoke legislative reaction.

Of course, in the end my judgment is irrelevant: legislators—particularly state legislators—will have to weigh consumer welfare and determine whether such use constraints seem justified. At the moment these issues of discrimination are not even on the regulatory radar screen. Hopefully this proposal to employ use constraints to dampen discrimination based on the Internet of Things will begin that conversation.

ii. Protecting Privacy by Redefining Personally Identifiable Information in This Context

A second plausible first step is to focus attention on how the terms "personal information" or "personally identifiable information" are used in relation to Internet of Things data. As indicated in Part II, both academic commentators and the FTC have already begun to move from a binary definition—where information is or is not PII—to a more nuanced approach in which regulation becomes more strict as information becomes more *likely* to identify or be identified with an individual. Neither scholars nor regulators, however, have focused on the particular issues for PII raised by the Internet of Things.[331] This has left the door open for Internet of Things firms to define "personal information" and "personally identifiable information" in a variety of ways in privacy policies and terms of use, as indicated by the privacy policy survey discussed in Part II.[332]

As a first step, regulators should issue guidance to Internet of Things firms about how to define and treat personally identifiable information in their privacy policies, on their web sites generally, and in their security practices. Part II asserted that sensor data are particularly difficult to anonymize successfully, and at least the computer science research to date seems to support this conclusion. If every person's gait can be uniquely identified by their FitBit data, then FitBit data are essentially impossible to de-identify.[333] If every road is unique and therefore a smartphone traveling in a vehicle over any given road emits a unique accelerometer data stream, then accelerometer data are essentially impossible to de-identify.[334] If one can be picked out from 1.5 million anonymized cellphone location streams based on just a very small number of known locations over a year-long period, then cellphone location data are essentially impossible to de-identify.[335] If electricity usage can reveal not

[331] *See* Part II(B)(ii).
[332] *See* Part II(D)(ii) and Appendix A.
[333] *See* Part II(B)(ii).
[334] *Id.*
[335] *See id.*

only that you are watching television but what movie you are viewing, then electricity data are essentially impossible to de-identify.[336]

Internet of Things firms currently act—particularly in their privacy policies—as if "personal information" includes only fields such as name, address, and telephone number. This allows them to use less stringent security to protect sensor data from attack, as well as to release aggregated de-identified sensor data streams to partners or other third parties under the assumption that such information cannot be easily re-identified. But if Internet of Things sensor data are so sparse as to make re-identification fairly simple, such practices are exposing very sensitive consumer information.

At the very least, corporate and privacy counsel for Internet of Things firms should focus on these definitions of PII and consider seriously the possibility that they are currently misleading the public. Several of the privacy policies surveyed, for example, make statements that the firm takes steps to make re-identification of aggregated consumer data impossible.[337] Counsel should investigate whether such promises can actually be upheld given the ways in which computer science research has shown sensor data are vulnerable to re-identification.

In addition, regulators—particularly the FTC and California's Office of Privacy Protection—should convene discussions with corporate counsel, computer scientists, academics, and privacy advocates to come up with guidance for the definition of PII in the Internet of Things context. For some types of Internet of Things devices it may remain plausible to distinguish "personal information" from sensor information. Whether an Internet-connected lightbulb is on or off may not reveal much about a user's identity. But for many—perhaps most—Internet of Things firms, the current approach to defining the concept of PII seems ill-conceived.

iii. Protecting Security by Expanding Data Breach Notification Laws

Third, regulators, corporate counsel, privacy advocates and others should focus on data security for the Internet of Things. At the very least, regulators can promulgate soft guidelines on best practices for securing these devices. California already issues such non-binding guidelines for Internet data generally[338]—it and other states should extend such guidance to the Internet of Things context. Data should be encrypted whenever possible, firmware should be updatable to allow for future measures to address security flaws, and data should be collected, transmitted, and stored

---

[336] *See id.*
[337] *See* Part II(D)(ii) and Appendix A.
[338] *See* CAL. DEP'T OF CONSUMER AFF., OFF. OF PRIVACY PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 8 (2006).

only as necessary to make the device function.[339] By giving guidance to Internet of Things firms, regulators can generate interest in and discussion of what constitutes industry standard in this new area.

Beyond that, however, states should extend their data breach notification laws to reach Internet of Things sensor data. Public disclosure of data breaches serves a reputational sanction function as well as allows the public to mitigate the harm from data theft.[340] It is essentially a market mechanism to address data security,[341] rather than an administrative one.[342] Coupled with substantive guidance from regulators on data security best practices for the Internet of Things, data breach notification can play a powerful role in disciplining device manufacturers.[343] Research has shown that data breach notification requirements are important to firms and corporate counsel, who take the reputational consequences of such notice seriously.[344]

To extend data breach notification law to the Internet of Things will require revision of the definitions in existing state statutes. As indicated in Part II, only a few such statutes even arguably apply currently to breach of Internet of Things sensor data.[345] To remedy this, states can take one of two approaches.

First, a state could simply alter the definition of "personal information" in their data breach statute to include name plus biometric or other sensor-based data such as, but not necessarily limited to, information from fitness and health sensor devices, automobile sensors, home appliance, electricity, and other sensors, and smartphone sensors. This approach would continue current practice of applying data breach notification statutes only to *already identified* data sets—in other words, data sets that include name

---

[339] For example, in response to certain security flaws identified in November, 2013, Belkin issued a firmware update for its WeMo home automation devices. The patch prevented XML injection attacks, added SSL encryption and validation to the WeMo system, and password protected certain port interfaces to prevent malicious firmware attacks. Belkin distributed these updates through its smartphone apps. *See* http://www.belkin.com/us/support-article?articlenum=80322 (describing security flaws and firmware patch).

[340] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007).

[341] *See* Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 66 (2011) (discussing market mechanism).

[342] *See* Nathan Alexander Sales, *Regulating Cyber Security*, 107 NW. U. L. REV. 1503, 1545 (2013) (calling for an administrative law approach to cyber security, wherein regulators would proactively monitor malicious code, harden vulnerable targets, and respond in the aftermath of attacks).

[343] *See* Burdon, *supra* note __ at 126-128 (calling for use of data breach notification laws in conjunction with substantive regulation of security practices).

[344] *See* Bamberger & Mulligan, *supra* note __ at 275 ("[E]very single respondent mentioned … the enactment of state data breach notification statutes as an important driver of privacy in corporations.").

[345] *See* Part II(C)(ii).

or other clearly identifying information. As this is the dominant current approach to state data breach notification laws, it seems likely that were states to consider extending such laws to Internet of Things sensor data, they would continue to require theft of name plus sensitive sensor information.

A second approach would abandon the "name plus" formula, instead triggering data breach notification if even de-identified data sets were breached. As indicated, most state laws do not currently extend to de-identified data sets. If a state legislature is going to take up revision of their data breach notification law, however, they might consider the continued wisdom of this limitation. As discussed in the previous Section, easy re-identification of Internet of Things data suggests that even de-identified sensor data sets should be protected by data breach notification statutes. Thus, a state could abandon the "name plus" approach and trigger notification if de-identified sensor data were stolen.

Either reform would significantly improve on the status quo. Currently, consumers have no way to know whether Internet of Things firms are under attack or if their potentially sensitive information has been stolen. As consumers behavior is increasingly measured, quantified, analyzed, and stored by the Internet of Things, it is reasonable that if one's weight, heart rate, fertility cycles, driving abilities, and personal habits at home should be protected as much as one's credit card or social security number. Such statutory amendment would bring the Internet of Things on par with the way in which we treat other types of sensitive information.

iv. Improving Consent by Guiding Internet of Things Consumer Disclosures

Finally, a fourth initial step would be to provide guidance on how to secure consumer consent to privacy practices on the Internet of Things. Such guidance must come, again, from the FTC, California's Office of Privacy Protection, similar state regulatory bodies, and privacy advocacy groups.

As an initial caveat, I do not want to place too much emphasis on consent as a solution to discrimination, privacy, and security problems. Most regulatory approaches to information privacy suffer from the delusion that consent can sanitize questionable privacy practices. Daniel Solove has called this the "privacy self-management" approach—the belief that providing consumers with sufficient information and control will allow them to "decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information."[346] Unfortunately, privacy self-management fails for a variety of reasons, as Solove and others have

[346] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013).

shown.[347] Consumers are uninformed, cognitively overwhelmed, and structurally ill-equipped to manage the vast information and myriad decisions that privacy self-management requires.[348]

With that caveat in place, however, focusing on Internet of Things privacy policies is still worthwhile for two reasons. First, consumers and consumer advocates should at least have some *chance* of using privacy policies to assess the implications of product choices. Acknowledging the limitations of consumer use of notice and choice does not justify allowing firms to confuse consumers with poor privacy policies. Second, privacy policies are one of the few regulatory tools currently available.[349] As discussed, the FTC's authority to constrain deceptive practices is a relatively stable ground for regulatory action. Thus, it is worth focusing at least some attention on the ways in which consumer protection law can address Internet of Things privacy policies.

Regulatory guidance must be grounded in protecting consumer expectations in this context. Relatively little empirical research has been done to date exploring those expectations for the Internet of Things.[350] Preliminary research about this new class of devices, however, does reveal certain basic consumer concerns. For example, Klasnja et al. studied twenty-four subjects using fitness trackers over several months.[351] They found that study participants' privacy concerns varied depending on (1) what types of sensors the tracker employed (e.g., accelerometers versus GPS versus audio recordings); (2) the length of time data were retained (e.g., kept indefinitely or discarded quickly); (3) the contexts in which the participants used the sensors (e.g., work or home); (4) the perceived value to the participants of the sensor-enabled applications; and (5) whether data were stored on the users device or on a website/in the cloud.[352] Similarly, in a recent study of FitBit, Withings scales, and other health related sensor devices, Barua et al. found that users want to be able to have a copy of the data such devices produce.[353] This is the simplest level of control over one's data—the ability to inspect, manipulate, and store your own information.[354] As the authors

---

[347] *See generally* Ryan Calo, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773, 788-789 (2014) (reviewing critiques of privacy notice).
[348] *See id.*
[349] *See* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere),* 87 NOTRE DAME L. REV. 1027, 1028 (2012) ("In the context of digital privacy, notice is among the only affirmative obligations websites face.").
[350] *See e.g.,* Debjanee Barua et al., *Viewing and Controlling Personal Sensor Data: What Do Users Want?*, PERVASIVE 15, 15 (2013) ("There has been little work on the issues of capture and management of the data associated with these [sensor devices] ….").
[351] *See* Predrag Klasnja et al., *Exploring Privacy Concerns about Personal Sensing*, PERVASIVE 176 (2009).
[352] *See id.* at 179-181 (describing study results).
[353] *See id.* at 22 (finding that only 16 percent of survey respondents say no need for a copy).
[354] *See* Tene & Polonetsky, *supra* note __ at 64 (arguing that firms should provide "individuals with access to their data in a 'usable' format and allow[] them to take advantage of third party applications to analyze their own data and draw useful conclusions ….").

note, however, even this basic level of control is not supported by current consumer products:

> "With the state of present sensors, this is a problem. Typically, each sensor, and its associated data, is under the control of its manufacturer. … [T]his does not make it feasible for most people to get a copy of their own data."[355]

Finally, in one of the most interesting studies to date, Heather Patterson and well-known privacy scholar Helen Nissenbaum focused on user expectations of privacy regarding FitBit and other fitness data.[356] Their study builds on the basic finding that Americans are generally concerned about health-related data being used outside of the medical context: 77 percent are concerned about such information being used for marketing, 56 percent are concerned about employer access, and 55 percent worry about insurer access.[357] Patterson and Nissenbaum found that participants were concerned about the potential for discrimination in hiring[358] and insurance,[359] overly personal marketing efforts based on FitBit data,[360] and data security.[361] Patterson and Nissenbaum conclude that "[s]elf-tracking services should … be concrete about information disclosures, explaining to users the conditions under which *particular* third parties, including employers, insurance companies, and commercial researchers, may obtain access to their data, and giving users the explicit right to opt out of these disclosures."[362]

Together, these studies suggest that Internet of Things consumers want answers to such seemingly basic questions as:

1. What exact information does the device collect about itself or its user, using what sorts of sensors?
2. Is that information stored on the device itself, on the user's smartphone (assuming the device interacts with the user's phone), on the manufacturer's servers in the cloud, or all of the above?
3. Is that information encrypted and how?
4. If the information is stored in a de-identified form, does the manufacturer maintain the ability to re-identify the information (for example, in response to a subpoena)?

---

[355] *Id.* at 24-25.
[356] *See* Patterson & Nissenbaum, *supra* note __.
[357] *See* Patterson & Nissenbaum, *supra* note __ at 11 (citing Center for Democracy and Technology, *Comments submitted to the Presidential Commission for the Study of Bioethical issues*).
[358] *See id*. at 27.
[359] *See id*. at 41.
[360] *See id*. at 28.
[361] *See id.*
[362] *Id.* at 46.

5. Can the user gain access to the raw sensor data in order to export it to another service or device?
6. Can the user view, edit, or delete sensor data from the manufacturer's servers, if it is kept there?
7. According to the device manufacturer, who owns the data in question?
8. Who exactly will the manufacturer or service share the data with and will the user have any right to opt out of such disclosures?

Such information would provide consumers with the information needed to make informed choices about such connected devices. Unfortunately, Part II(D) showed that current industry practice provides nothing near this level of disclosure.[363] Instead, existing Internet of Things privacy policies tend to leave unanswered most or all of these basic questions.

I suggest four basic reforms to current practice, beyond the re-definition of "personally identifiable information" already discussed above.[364] First, regulators should seek industry consensus on best practices for *where* and *when* to give consumers notice about privacy and data issues. Firms should either include the relevant product-related privacy policy in the box with a consumer Internet of Things device, or should provide clear information with the product about how a user can find that policy. In addition, firms should clarify whether web site policies apply only to web site use or also to data generated by product use. If the latter, that merged policy should clearly and directly address the sensor data generated by an Internet of Things device and clarify any distinctions in how such data are handled (as compared to data generated by web site use).

Second, Internet of Things privacy policies should commit firms to the principle that consumers own the sensor data generated by their bodies, cars, homes, smartphones, and other devices. As a corollary to this commitment, firms should be encouraged to give users clear access, modification, and deletion rights vis-à-vis sensor data. As indicated in Part II, none of the surveyed privacy policies provided for user ownership of sensor data, and only a very few even addressed access rights to sensor data specifically. Although firms currently sometimes give consumers the right to change "personal information," lack of clarity about whether sensor data qualifies as personal information currently makes those rights relatively weak vis-à-vis sensor data.

Third, Internet of Things privacy policies should specify what sensors are used in a device, exactly what data those sensors create, for what purposes those data are used, and how (and for how long) those data are stored. Consumers should be told whether sensor data are kept on the device

[363] *See* Part II(D) and Appendix A.
[364] *See* Part III(A)(ii).

or in the cloud, and should be given clear notice that cloud storage means that the data is both more vulnerable to security breach and available for subpoena or other discovery. If sensor data are stored in the cloud, firms should disclose whether such data are stored in encrypted or de-identified form.

Finally, Internet of Things firms should commit to not sharing even aggregated, de-identified sensor data that poses reasonable risk of re-identification. This is a corollary of my argument in Part III(A)(ii) for re-defining personally identifiable information in this context, but deserves separate mention. Sensor data are so sensitive and revealing that consumers should be reassured that they will not leak into the public sphere. I would urge regulators and privacy advocates to encourage Internet of Things firms to adopt a simple principle: when in doubt, assume that sensor data can be re-identified. Such firms would do well to build their business models around the assumption that they cannot share even aggregated, de-identified sensor data without significant reputational, market, and regulatory risk.

These basic reforms to Internet of Things privacy policies are meant to begin a conversation between regulators, consumer advocates, privacy scholars, and corporate counsel. This is a new and evolving field full of new and evolving products. My review of the status quo reveals that reform is necessary to minimize consumer confusion and make Internet of Things privacy policies at least plausibly useful. But this conversation will take time and consensus-building between regulators and market players. As the next and final section shows, however, the conversation must begin with some urgency.

B. SEIZE THE MOMENT: WHY PUBLIC CHOICE PROBLEMS DEMAND URGENCY

This brings us to our final topic: the public choice problems inherent in addressing the Internet of Things and the resulting need for urgency. The informational privacy field has long lamented the difficulties of enacting legislative privacy reforms.[365] Congress has largely ignored academic and even regulatory proposals over the last decade. What chance, then, is there for managing these problems of discrimination, privacy, security and consent in the Internet of Things context?

There are two reasons for hope. First, sensor-based tracking tends to garner strong responses from the public and its representatives. Various states raced to forbid employers from requiring employees to implant subcutaneous RFID tags even before employers tried to so.[366] Several states

[365] *See e.g.,* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).
[366] *See* Peppet, *Unraveling Privacy*, *supra* note __ at __.

have addressed GPS locational tracking, which galvanizes public reaction.[367] And, as indicated, some states have focused on automobile EDR data and various cross-context use constraints to control sensor data use. In short, sensors tend to scare people—the potential harms they present are perhaps more salient than the more vague or generalized harms of Internet tracking generally. As a result, reformers may find it easier to mobilize support for shaping the Internet of Things than for cabining Internet or web data generally.

Second, the Internet of Things is relatively new, and therefore industry has perhaps not yet hardened its views on how these data streams should be managed. Lior Strahilevitz has recently noted the importance of identifying winners and losers in privacy contests, and of analyzing the public choice issues that thus arise.[368] I have likewise tried to focus informational privacy scholars on these issues.[369] As firms find ways to profit from Internet of Things information, those firms will increasingly push for sparse regulation of such data uses. As the Internet of Things moves from startups to large established Internet players—witness Google's recent acquisition of the Nest Thermostat—those players will have more power to resist shaping of the industry. For now, however, most of the consumer products reviewed in this Article are the work of small, relatively new entrants to this emerging market. Advocates, regulators, and corporate counsel have an opportunity to guide such firms towards best practices. And even as larger firms create Internet of Things products or acquire such devices from startups, the newness of this field is likely to temporarily permit some collaboration between those seeking increased regulation and those building the Internet of Things.

This suggests a need for urgency. Not only are consumers currently vulnerable to the discrimination, privacy, security and consent problems outlined here, but it may become harder over time to address such issues. In technological and political circles it may be convenient to prescribe a "wait and see—let the market evolve" stance, but the reality is that as time passes it will likely become harder, not easier, for consumer advocates, regulators, and legislators to act. The Internet of Things is here. It would be wise to respond as quickly as possible to its inherent challenges.

CONCLUSION

This Article has mapped the sensor devices at the heart of the consumer Internet of Things, explored the four main problems such devices

---

[367] *See* Peppet, *Unraveling Privacy*, *supra* note __ at 1169-70 (discussing examples).
[368] *See* Lior Strahilevitz, *Towards a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013).
[369] *See* Peppet, *Unraveling Privacy*, *supra* note __ (discussing public choice problems inherent in regulating privacy).

create, and put forth plausible first steps towards constraining those problems. Although my argument's scope is broad, I have tried to show detailed examples of regulatory solutions that have a chance of succeeding in this new arena. As with many such efforts, I am humble in my expectations, hoping mostly to provoke debate and serious consideration of how best to regulate the emerging Internet of Things.

APPENDIX A:
INTERNET OF THINGS PRIVACY POLICIES

Product	Does Product Manual or Quick Start Guide in Packaging Discuss Data, Privacy or Security?	Privacy Policy							
		Does Policy Apply to Web Site Use, Sensor Product Use & Data, or Both?	Does Policy Discuss Sensor Data Ownership?	Does Policy Disclose Sensor Types or Exactly What Sensor Data Are Collected?	Does Policy Explain Whether Data Are Stored on Device, Smart Phone, or Cloud?	Does Policy Explain Whether Sensor Data Are Encrypted?	Does Policy Explain Whether Sensor Data are Stored in De-Identified State, and Whether Firm Has Ability to Re-Identify?	Does Policy Limit Sensor Data Use or Resale?	Does Policy Provide for User to Change or Delete Sensor Data?
Health & Fitness									
FitBit fitness monitors and Aria Wi-Fi Smart Scale[370]	No	Both	No	No. Sensor information is available on various different pages of web site, including on specifications pages and under help or support.	No. One can infer cloud storage but it is not described.	Policy mention that "encryption techniques" are used for security purposes but does not describe	No. Policy explains that only aggregated data can be shared with third parties, but does not discuss whether data are stored anonymized.	Unclear whether sensor data are "personal information" under the policy. Personal information can be shared for only limited reasons; Other information can be shared if aggregated and "non-personally identifiable"	Unclear: user can delete personal information. Sensor data remain in "de-identified and anonymized historical" form.
Nike FuelBand[371]	No	Both	No	No. Sensor information is available on various different pages of web site, including on specifications	No	Policy mentions that encryption is used for security purposes but seems to imply that only credit	No	No	Yes, but Nike has the right to keep a copy

				pages and under help or support.		card information is encrypted			
Body Media Armband[372]	No	Confusing. Policy states that it applies to web site use, but also includes provisions related to sensor data.	Yes: Body Media owns all sensor data	Somewhat: privacy policy explains that armband data does *not* include location, medical vital signs, or voice data. Does not explain what data are collected. Web site includes a page detailing four types of sensor measurements (accelerometer, galvanic skin response, skin temperature, heat flux)[373]	No.	Credit card information is encrypted	Yes. Policy states that armband data is anonymized	Limits sale or sharing of personal information; May sell "non-personally identifiable" information	No
Withings Blood Pressure Cuff & Weight Scale[374]	No	Both	No	Somewhat: privacy policy explains that arterial pressure or weight data are collected; does not detail sensor types	No.	No.	No.	Limits sale or sharing of personal information, which is defined to include sensor data	Yes
iHealth Blood Pressure monitor[375]	No[376]	Two separate policies: one for web site and one for products. The	Yes: iHealth owns all sensor data (according to mobile app	N/A	No, but web site indicates data is stored in the cloud.	N/A	N/A	N/A	N/A

[372] *See* http://www.bodymedia.com/Support-Help/Policies/Privacy-Policy.
[373] *See* http://www.bodymedia.com/the_science.html.
[374] *See* http://www.withings.com/index/privacy.
[375] *See* http://www.ihealthlabs.com/blood-pressure-dock-feature_31.htm.
[376] *See* http://www.ihealthlabs.com/ihealth_support_Downloads_14.htm (providing user manuals and quick start guides).

		latter is referenced in the mobile app Terms of Use, but currently unavailable.	Terms of Use)						
Wahoo BlueHR Heart Rate Monitor[377]	N/A	Privacy policy only seems to apply to data collected through web site.							
Basis Sports Watch[378]		Both	Yes: Basis owns all biometric data	Yes. Privacy policy defines heart rate, skin temperature, ambient temperature, galvanic skin response, and accelerometer data as "biometric data"	No, but web site indicates data is stored in the cloud	Yes: Policy states that data are not encrypted	No	Yes: Basis may sell or share data for any use so long as "your individual identity is not readily discernible"; may sell or share de-identified aggregated biometric data	User can delete personal information but not biometric data. User cannot export raw biometric data.
Breathometer[379]	No	Both	No	No	No	No	No	Limits sharing somewhat but permits marketing	Yes: can review but not correct or delete
June UV Monitor Bracelet[380]	N/A	Both	No	No. Sensor information is available on various different pages of web site, including on specifications pages and under help or support.	No	No	No	Limits sharing somewhat; permits marketing and broadly permits sharing of de-identified data	Yes: User has access, correction and deletion rights under French law
LifeBeam Smart Cycling Helmet[381]	No	Both	No	No. Sensor information is available on	No	No	No	Limits sharing somewhat; broadly permits	No

[377] *See* http://www.wahoofitness.com/privacy.asp.
[378] *See* http://www.mybasis.com/legal/privacy.
[379] *See* http://www.breathometer.com/legal/privacy-policy.
[380] *See* http://www.netatmo.com/en-US/site/terms#div_privacy1.

				various different pages of web site, including on specifications pages and under help or support.				sharing of de-identified data	
MimoBaby Onesie Sleep & Breathing Monitor[382]	N/A	Website and smartphone app. Unclear whether it applies to product data	No	Policy states that sensors collect biometric information including skin temperature, body position, breathing rate, audio, and ambient temperature	Terms of service explains data are transferred to firm's servers	Policy states explicitly that sensor data are not encrypted	No	Limits sharing to aggregate information	Unclear: user has access, correction and deletion rights for "personal information"
Phyode W/Me Bracelet to Monitor Mental States[383]	No[384]	No privacy policy available (although web site indicates that one exists).							
Muse Headband to Monitor Stress and Mental States[385]	No	Both	Yes. User owns biometric or sensor data.	No – policy refers to owner's manual and specifications.	Yes. Policy explains that some data are stored on phone or device.	No	Yes. Policy explains that sensor data are stored in an anonymized form.	Unclear. Policy states that sensor data are highly sensitive and implies it will not be shared.	Yes. User can remove or delete biometric or sensor data.
Propeller Asthma Inhaler Sensor[386]	N/A	Web site only; indicates that a second policy exists for product-related privacy							

[381] *See* http://mysmarthelmet.com/privacy-policy/.
[382] *See* http://mimobaby.com/terms/.
[383] *See* http://www.phyode.com.
[384] *See* http://www.phyode.com/images/WMe%20Wristband%20User%20Guide.pdf (providing user guide for W/Me bracelet).
[385] *See* http://www.choosemuse.com/pages/privacy.
[386] *See* http://www.propellerhealth.com/faqs/.

		issues, but it is not on web site							
Automobile									
CarChip[387]	No	Both	No	No	User manual explains that data are stored on user's computer	No	No	Unclear whether sensor data are personal information; limits sharing of personal information; allows broad sharing of non-personal information	No. Users can access and correct personal information but no mention of sensor data.
Automatic Link[388] driving monitor	N/A	Both	No	Somewhat. It explains that it collects location, how you drive, error codes from the car's computer, and sensor information from both the car's sensors and the device's sensors. It does not specify which sensors exactly.	Yes. Policy states that data is stored in the device, in the app, and in its "cloud servers"	No	No	Limits sharing of personal information but not of sensor data	Yes: User has deletion rights for all data including sensor data
BMW iPhone Power Meter App[389]	No policy readily available on iTunes app store or BMW web site								

[387] *See* http://www.davisnet.com/about/index.asp.
[388] *See* http://www.automatic.com/legal/.
[389] *See* http://www.bmw.com/com/en/newvehicles/mseries/x5m/2009/g_meter.html (for description of app).

Home & Electric Grid									
Nest Thermostat or Smoke Detector[390]		Two separate policies: one for web site, one for products	No	Yes. Policy explains types of information and provides examples.	Yes. Policy states that data are both stored on device and regularly uploaded to Nest "cloud servers"	Yes. Policy states that all data are encrypted	No	Limits sharing of personally identifiable information; allows sharing of aggregated and anonymous information.	Somewhat: allows deletion of personally identifiable information but unclear as to sensor data
SmartThings home automation sensor system[391]	No, although available at time of signup for account on mobile app	Both	No. However, the separate Terms of Service document clarifies that users own sensor data.	Somewhat. Policy provides an example that a home temperature unit would automatically report temperature and location.	Yes. Policy explains that data are automatically stored on servers.	No	No.	Allows sharing of sensor data in de-identified and/or aggregated form only.	Somewhat. User can access and change device information and location, as well as name, etc.
Belkin Wemo Home Automation system[392]	No	Both	No.	Somewhat. Policy does not describe sensor types, but indicates that usage data, data about devices connected to Belkin devices, data about when and how Belkin devices are used, and utility settings, temperature and light readings, motion detection, and alarm events	Policy indicates that data may be stored in the cloud.	No.	Somewhat. Policy states that usage data are generally anonymized, although it does not indicate whether Belkin stores usage data in an identified form as well.	Limits sale or sharing of Personal Information but defines usage/sensor data as non-personal information. Permits sharing of aggregated, anonymized non-personal information. Forbids downstream partners to re-identify data.	Somewhat: allows access to and deletion of personal information but silent as to sensor data (which it defines as non-personal)

[390] *See* http://www.nest.com/legal/privacy-statement/.
[391] *See* http://www.smartthings.com/privacy/.
[392] *See* http://www.belkin.com/us/privacypolicy/.