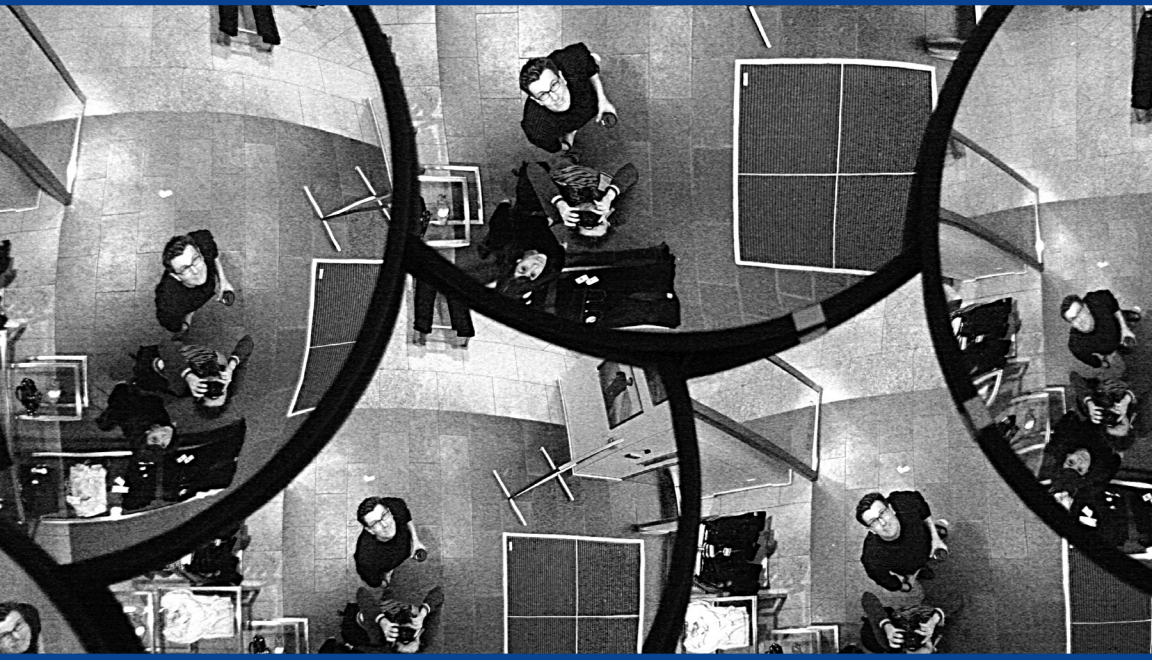
O'REILLY®

Privacy and the Internet of Things



Gilad Rosner

Privacy and the Internet of Things

Gilad Rosner

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Privacy and the Internet of Things
by Gilad Rosner

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editors: Susan Conant and Jeff Bleiel
Production Editor: Shiny Kalapurakkel
Copyeditor: Octal Publishing, Inc.
Proofreader: Charles Roumeliotis
Interior Designer: David Futato
Cover Designer: Randy Comer
Illustrator: Rebecca Panzer

October 2016: First Edition

Revision History for the First Edition
2016-10-05: First Release

978-1-491-93282-7

[LSI]

Table of Contents

Introduction

The "Internet of Things," or IoT, is the latest term to describe the evolutionary trend of devices becoming "smarter": more aware of their environment, more computationally powerful, more able to react to context, and more communicative. There are many reports, articles, and books on the technical and economic potential of the IoT, but in-depth explorations of its privacy challenges for a general audience are limited. This report addresses that gap by surveying privacy concepts, values, and methods so as to place the IoT in a wider social and policy context.

How many devices in your home are connected to the Internet? How about devices on your person? How many microphones are in listening distance? How many cameras can see you? To whom is your car revealing your location? As the future occurs all around us and technology advances in scale and scope, the answers to these questions will change and grow. Vint Cerf, described as one of the "fathers of the Internet" and chief Internet evangelist for Google, said in 2014, "Continuous monitoring is likely to be a powerful element in our lives."[1] Indeed, monitoring of the human environment by powerful actors may be a core characteristic of modern society.

Regarding the IoT, a narrative of "promise or peril" has emerged in the popular press, academic journals, and in policy-making dis-

1 Anderson, J. and Ranie, L. 2014. *The Internet of Things Will Thrive by 2025: The Gurus Speak*. Pew Research Center. Available at *http://pewrsr.ch/2cFqMLJ*.

course.[2] This narrative focuses on either the tremendous opportunity for these new technologies to improve humanity, or the terrible potential for them to destroy what remains of privacy. This is quite unhelpful, fueling alarmism and hindering thoughtful discussion about what role these new technologies play. As with all new technical and social developments, the IoT is a multilayered phenomenon with valuable, harmful, and neutral properties. The IoT is *evolutionary* not *revolutionary*; and as with many technologies of the information age, it can have a direct effect on people's privacy. This report examines what's at stake and the frameworks emerging to address IoT privacy risks to help businesses, policy-makers, funders, and the public engage in constructive dialogue.

What This Report Is and Is Not About

This report does the following:

- Draws together definitions of the IoT
- Explores what is meant by "privacy" and surveys its mechanics and methods from American and European perspectives
- Briefly explains the differences between privacy and security in the IoT
- Examines major privacy risks implied by connected devices in the human environment
- Reviews existing and emerging frameworks to address these privacy risks
- Provides a foundation for further reading and research into IoT privacy

2 For example, see Howard, P. 2015. *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up*. New Haven: Yale University Press; Cunningham, M. 2014. Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm. *Groningen Journal of International Law*, 2(2):115-144; Bradbury, D. 2015. How can privacy survive in the era of the internet of things? *The Guardian*. Available at *http://bit.ly/2dwaPcb*; Opening Statement of the Hon. Michael C. Burgess, Subcommittee on Commerce, Manufacturing, and Trade Hearing on "The Internet of Things: Exploring the Next Technology Frontier," March 24, 2015. Available at *http://bit.ly/2ddQU1b*.

This report is not about:

- Trust—in the sense of people's comfort with and confidence in the IoT
- The potential benefits or values of the IoT—this is covered exhaustively in other places[3]
- The "industrial IoT"—technologies that function in industrial contexts rather than consumer ones (though the boundary between those two might be fuzzier than we like to think[4])
- Issues of fully autonomous device behavior—for example, self-driving cars and their particular challenges

We can divide IoT privacy challenges into three categories:

- IoT privacy problems as classic, historical privacy problems
- IoT privacy problems as Big Data problems
- IoT privacy problems relating to the specific technologies, characteristics, and market sectors of connected devices

This report examines this division but mainly focuses on the third category: privacy challenges particular to connected devices and the specific governance they imply.

Discussions of privacy can sometimes be too general to be impactful. Worse, there is a danger for them to be shrill: the "peril" part of the "promise or peril" narrative. This report attempts to avoid both of these pitfalls. In 1967, Alan Westin, a central figure in American privacy scholarship, succinctly described a way to treat emergent privacy risks:

3 E.g., see Manyika, J. et. al. 2015. *Unlocking the Potential of the Internet of Things*. Available at *http://bit.ly/2dtCp7f*; UK Government Office for Science. 2014. *The Internet of Things: making the most of the Second Digital Revolution*. Available at *http://bit.ly/2ddS4tI*; O'Reilly, T. and Doctorow, C. 2015. *Opportunities and Challenges in the IoT*. Sebastopol: O'Reilly Media.

4 For example, the US National Security Telecommunications Advisory Committee Report to the President on the Internet of Things observes, "the IoT's broad proliferation into the consumer domain and its penetration into traditionally separate industrial environments will progress in parallel and become inseparable." See *http://bit.ly/2d3HJ1r*.

> The real need is to move from public awareness of the problem to a sensitive discussion of what can be done to protect privacy in an age when so many forces of science, technology, environment, and society press against it from all sides.[5]

Historically, large technological changes have been accompanied by social discussions about privacy and vulnerability. In the 1960s, the advent of databases and their use by governments spurred a far-ranging debate about their potential for social harms such as an appetite for limitless collection and impersonal machine-based choices about people's lives. The birth of the commercial Internet in the 1990s prompted further dialogue. Now, in this "next wave" of technology development, a collective sense of vulnerability and an awareness that our methods for protecting privacy might be out of step propel these conversations forward. It's an excellent time to stop, reflect, and discuss.

5 Westin, A. 1967. *Privacy and Freedom*. New York: Atheneum.

What Is the IoT?

So, what is the IoT? There's no single agreed-upon definition, but the term goes back to at least 1999, when Kevin Ashton, then-director of the Auto-ID Center at MIT, coined the phrase.[6] However, the idea of networked noncomputer devices far predates Ashton's term. In the late 1970s, caffeine-fixated computer programmers at Carnegie Mellon University connected the local Coca Cola machine to the Arpanet, the predecessor to the Internet.[7] In the decades since, several overlapping concepts emerged to describe a world of devices that talk among themselves, quietly, monitoring machines and human beings alike: ambient intelligence, contextual computing, ubiquitous computing, machine-to-machine (M2M), and most recently, cyber-physical systems.

The IoT encompasses several converging trends, such as widespread and inexpensive telecommunications and local network access, cheap sensors and computing power, miniaturization, location positioning technology (like GPS), inexpensive prototyping, and the ubiquity of smartphones as a platform for device interfaces. The US National Security Telecommunications Advisory Committee wrote in late 2014:[8] "the IoT differs from previous technological advances because it has surpassed the confines of computer networks and is connecting directly to the physical world."

6 Ashton, K. 2009. That "Internet of Things" Thing. *RFID Journal*. Available at *http://bit.ly/18XhbHO*.

7 The "Only" Coke Machine on the Internet. Available at *https://www.cs.cmu.edu/~coke/history_long.txt*.

8 See footnote 4.

One term that seems interchangeable with the IoT is *connected devices*, because the focus is on purpose-built devices rather than more generic computers. Your laptop, your desktop, and even your phone are generic computing platforms—they can do many, many things, most of which were not imagined by their original creators. "Devices" in this sense refers to objects that are not intended to be full-fledged computers. Fitness and medical wearables, cars, drones, televisions, and toys are built for a relatively narrow set of functions. Certainly, they have computing power—and this will only increase over time—but they are "Things" first and computers second.

As to the size of the IoT, there are many numbers thrown around, a popular one being Cisco's assertion that there will be 50 billion devices on the 'net in 2020.[9] This is a guess—one of several, as shown in Figure 2-1.

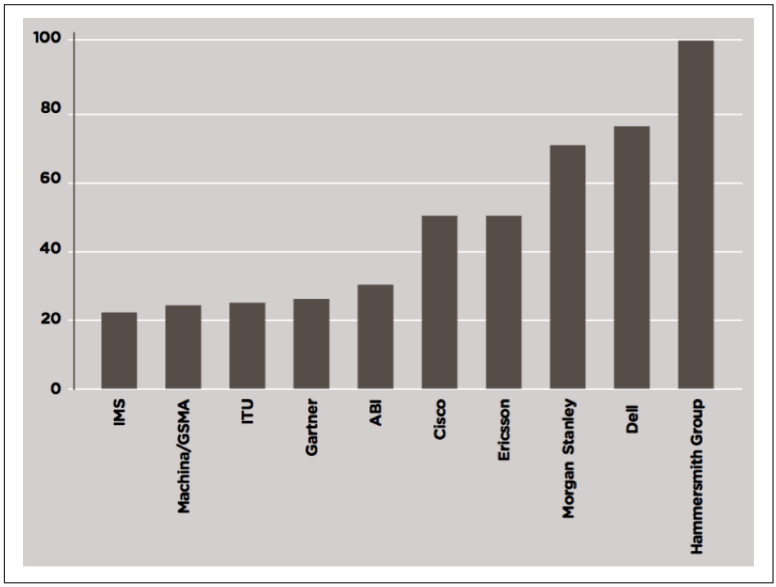


Figure 2-1. Industry estimates for connected devices (billions) in 2020 (source: The Internet of Things: making the most of the Second Digital Revolution, UK Government Office for Science, 2014)

9 Evans, D. 2011. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Available at *http://bit.ly/2ddRdZS*.

Segmenting the IoT into categories, industries, verticals, or technologies assists in examining its privacy risks. One categorization is consumer versus industrial applications, for example, products in the home versus oil and gas drilling. Separating into categories can at least make a coarse division between technologies that deal directly in personal data (when are you home, who is in the home, what are you watching or eating or saying) and those that do not. For privacy analysis, it's also valuable to separate the IoT into product sectors, like wearables, medical/health/fitness devices, consumer goods, and the connected car. Similarly useful are verticals like cities, health, home, and transport. The smart city context, for example, implicates different privacy, governance, and technology issues than the health context.

The IoT is a banner for a variety of definitions, descriptions, technologies, contexts, and trends. It's imprecise and messy, but a few key characteristics emerge: sensing, networking, data gathering on humans and their environment, bridging the physical world with the electronic one, and unobtrusiveness. And although the concept of connected devices is decades old, policy-makers, journalists, and the public are tuning in to the topic now because these devices are noticeably beginning to proliferate and encroach upon personal spaces in ways that staid desktops and laptops did not. Ultimately, the term will vanish, like "mobile computing" did, as the fusion of networking, computation, and sensing with formerly deaf and dumb objects becomes commonplace and unremarkable.

What Do We Mean by Privacy?

Much like the problem of saying "the Internet of Things" and then assuming that everyone knows what you are talking about, the term "privacy" means *very* different things to people. This is as true among experts, practitioners, and scholars as it is among general society. "Privacy is a concept in disarray," observes Dan Solove, one of America's leading privacy law scholars; it is "too complicated a concept to be boiled down to a single essence."[10] Privacy is an economic, political, legal, social, and cultural phenomenon, and is particular to countries, regions, societies, cultures, and legal traditions. This report briefly surveys American and European privacy ideas and mechanisms.

The Concept of Privacy in America and Europe

In 1890, two American legal theorists, Warren and Brandeis, conceived of the "right to be let alone" as a critical civil principle,[11] a right to be protected. This begins the privacy legal discussion in the United States and is often referenced in European discussions of privacy, as well. Later, in 1967, privacy scholar Alan Westin identified "four basic states of privacy":

10 Solove, D. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154(3): 477-560. Available at *http://bit.ly/2d3ucsk*.

11 Brandeis, L. and Warren, S. 1890. The Right to Privacy. *Harvard Law Review* 4(5): 193-220. Available at *http://bit.ly/2d3HVxI*.

Solitude
: Physical separation from others

Intimacy
: A "close, relaxed, and frank relationship between two or more individuals" that can arise from seclusion

Anonymity
: Freedom from identification and surveillance in public places

Reserve
: "The creation of a psychological barrier against unwanted intrusion"[12]

Westin wrote that privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[13] This view appears also in European conceptions of privacy. In 1983, a German Constitutional Court articulated a "right of informational self-determination," which included "the authority of the individual to decide [for] himself...when and within what limits information about his private life should be communicated to others."[14] In Europe, privacy is conceived as a "fundamental right" that people are born with. European policies mainly use the term "data protection" rather than "privacy." It's a narrower concept, applied specifically to policies and rights that relate to organizations' fair treatment of personal data and to good data governance. Privacy covers a broader array of topic areas and is concerned with interests beyond fairness, such as dignity, inappropriate surveillance, intrusions by the press, and others.

In 1960, American law scholar William Prosser distilled four types of harmful activities that privacy rights addressed:

12 See footnote 5.

13 See footnote 5.

14 Quoted in Rouvroy, A. and Poullet, Y. 2009. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & S. Nouwt (eds.), *Reinventing Data Protection?* (pp. 45-76). Dordrecht: Springer.

- Intrusion upon someone's seclusion or solitude, or into her private affairs
- Public disclosure of embarrassing private facts
- Publicity which places someone in a false light
- Appropriation of someone's name or likeness for gain without her permission[15]

This conception of privacy is, by design, focused on *harms* that can befall someone, thereby giving courts a basis from which to redress them. But, as the preceding descriptions show, conceiving of privacy exclusively from the perspective of harms is too narrow.

Thinking of privacy harms tends to focus discussion on *individuals*. Privacy, however, must also be discussed in terms of *society*. Privacy and data protection, it is argued, are vital for the functioning of society and democracy. Two German academics, Hornung and Schnabel, assert:

> ...data protection is... a precondition for citizens' unbiased participation in the political processes of the democratic constitutional state. [T]he right to informational self-determination is not only granted for the sake of the individual, but also in the interest of the public, to guarantee a free and democratic communication order.[16]

Similarly, Israeli law scholar Ruth Gavison wrote in 1980: "Privacy is...essential to democratic government because it fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy."[17]

In this way, privacy is "constitutive" of society,[18] integrally tied to its health. Put another way, privacy laws can be seen as social policy,

---

15 Prosser, W. 1960. Privacy. *California Law Review* 48(3):383-423. Available at *http://bit.ly/2d3I6ZU*.

16 Hornung, G. and Schnabel, C. 2009. Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination. *Computer Law & Security Report* 25(1): 84-88.

17 Gavison, R. 1980. Privacy and the Limits of the Law. *Yale Law Journal* 89(3):421-471. Available at *http://bit.ly/2cWTFD1*.

18 Schwartz, P. 2000. Internet Privacy and the State. *Connecticut Law Review* 32(3): 815-860. Available at *http://bit.ly/2dm8yxe*; Simitis, S. 1987. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review* 135(3):707-746. Available at *http://bit.ly/2dtDxYB*.

encouraging beneficial societal qualities and discouraging harmful ones.[19]

In trying to synthesize all of these views, Professor Solove created a taxonomy of privacy that yields four groups of potentially harmful activities:[20]

- Information collection
  - — Surveillance: watching, listening to, or recording an individual's activities
  - — Interrogation: questioning or probing for information
- Information processing
  - — Aggregation: combining various pieces of data about a person
  - — Identification: linking information to particular individuals
  - — Insecurity: carelessness in protecting stored information
  - — Secondary use: use of information for a purpose other than what it was originally collected for without a person's consent
  - — Exclusion: failure to allow someone to know about data others have about him, and to participate in its handling and use
- Information dissemination
  - — Breach of confidentiality: breaking a promise to keep a person's information confidential
  - — Disclosure: revelation of information that affects how others judge someone
  - — Exposure: revealing another's nudity, grief, or bodily functions
  - — Increased accessibility: amplifying the accessibility of information
  - — Blackmail: the threat to disclose personal information
  - — Appropriation: the use of someone's identity to serve someone else's interests

19 See Part 1 of Bennett, C. and Raab, C. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Burlington: Ashgate Publishing.

20 See footnote 10.

- Distortion: disseminating false or misleading information about someone
- Invasion
  - Intrusion: invading someone's tranquillity or solitude
  - Decisional interference: incursion into someone's decisions regarding her private affairs

Although this taxonomy is focused around the individual, it should be understood that personal losses of privacy add up to societal harms. One of these is commonly called *chilling effects*: if people feel like they are being surveilled, or that what they imagine to be private, intimate conversations or expressions are being monitored, recorded, or disseminated, they are less likely to say things that could be seen as deviating from established norms.[21] This homogenization of speech and thought is contrary to liberty and democratic discourse, which relies upon a diversity of views. **Dissent, unpopular opinions, and intellectual conflict are essential components of free societies—privacy helps to protect them**.

One important thing to take away from this discussion is that there is no neat split between information people think of as public versus information that is private. In part, this is because there is no easy definition of either. Consider medical information shared with your doctor—it will travel through various systems and hands before its journey is complete. Nurses, pharmacists, insurance companies, labs, and administrative staff will all see information that many citizens deem private and intimate. Here again we see the problem of construing privacy as secrecy. Information is shared among many people within a given *context*. One theory[22] within privacy scholarship says that when information crosses from one context into another—for example, medical information falling into nonmedical contexts, such as employment—people experience it as a privacy violation (see the section "Breakdown of Informational Contexts" on page 25 later in this report). Advances in technology further complicate notions of the public and the private, and cause us to

21 For example, recent research has documented how traffic to Wikipedia articles on privacy-sensitive subjects decreased in the wake of the Snowden NSA revelations: *http://bit.ly/2cwkivn*.

22 Nissenbaum, H. 2010. *Privacy in Context*. Stanford: Stanford University Press.

reflect more on where, when, and what is deserving of privacy protections.

It's worth noting that the public/private split in American privacy regimes is different than the European conception of data protection, which focuses on restricting the flow of *personal* data rather than private or confidential data. The recently enacted General Data Protection Regulation defines personal data as:

> any information relating to an identified or identifiable natural person...; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[23]

Much ink has been spilled in comparing the US and European approaches,[24] but suffice it to say that there are pros and cons to each. They yield different outcomes, and there is much to be gained from drawing upon the best elements of both.[25]

It's essential to remember that **privacy costs money**. That is, building information systems that incorporate strong security, user preferences, encryption, and privacy-preserving architectures requires investments of capital, time, and know-how—all things that organizations seek to maximize and conserve. It means that, when making devices and services, **the preservation of privacy can never be divorced from economic considerations**. Businesses must have a reason—an economic justification—for incorporating privacy into their designs: regulatory requirements, product/service differentiation, voluntary adherence to best practices, contractual obligation, and fear of brand damage among other reasons. There is also a view that managers, developers, engineers, and executives include privacy

23 General Data Protection Regulation, Article 4(1). Available at *http://bit.ly/2ddSjoD*.

24 See, e.g., Part 1 of Schwartz, P. 2008. Preemption and Privacy. *Yale Law Journal* 118(5): 902-947. Available at *http://bit.ly/2ddTYdY*; Reidenberg, J. (1999). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review* 52(5): 1315-71. Available at *http://bit.ly/2cPKL7W*; Sec. 4.6 of Waldo, J., Lin, H., and Millet, L. 2007. *Engaging Privacy and Information Technology in a Digital Age*. Washington, D.C.: The National Academies Press. Available at *http://www.nap.edu/catalog/11896.html*.

25 Rosner, G. 2015. There is room for global thinking in IoT data privacy matters. *O'Reilly Media*. Available at *http://oreil.ly/2ddSY9y*.

in their products because it is the right thing to do—that good stewardship of personal data is a social value worth embedding in technology. Recent research by Berkeley professors Kenneth Bamberger and Deirdre Mulligan, however, illustrates that the right thing might be driven by business perceptions of consumer expectations.[26] Often, there is no easy separation of the economic and social reasons privacy architectures are built into technology, but the point is, from an engineering or compliance perspective, someone must pay for privacy.

Privacy is not just the law nor just rules to protect data sharing and storage; it's a shifting conversation about values and norms regarding the flow of information. Laws and rules enact the values and norms we prize, but they are "carriers" of these ideas. This means, however, that **the current picture of privacy rules is not the only way to protect it**. The topic of the IoT affords an opportunity to reflect. *How things have been need not be how they will be going forward*. Research shows that people are feeling vulnerable and exposed from the introduction of new Internet technologies.[27] As a wave of new devices are entering our intimate spaces, now is an excellent time to review the institutional and technical ways privacy is protected, its underlying values, and what can be done differently.

26 Bamberger, K. and Mulligan, D. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. Cambridge: MIT Press.

27 E.g., see the Pew Research Center's "The state of privacy in post-Snowden America: What we learned," available at *http://pewrsr.ch/2daWMH7*, and findings from the EU-funded CONSENT project, "What consumers think," available at *http://bit.ly/2dl5Uf2*.

What's the Relationship Between Privacy and Security?

Sometimes, the domains of privacy and security can be conflated, but they are not the same thing. They overlap, and, technologically, privacy is reliant on security, but they are separate topics. Here's how one US federal law defines information security:[28]

- protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide
- (A) integrity—guarding against improper modification or destruction of data
- (B) confidentiality—ensuring only the correct authorized party gets access to systems
- (C) availability—making sure the system can be accessed when called for

Whereas one of these—confidentiality—has a direct relationship with privacy, security is concerned with making sure a system does what it's designed to do, and can be affected only by the appropriate, authorized people. Compare this to the preceding discussion about privacy; security covers a much narrower set of concerns. A good example is the news from 2015 that hackers were able to access the Bluetooth connection of a sound system in Jeep vehicles to remotely shut off the engine and trigger the brakes while it was driving.[29] This is a *security* concern. Wondering about who gets to see all the data that a Jeep's black box captures, where the car has been, and who was present in the vehicle are *privacy* concerns—they relate to information flows, exposure, and identifiability.

28 44 US Code § 3542.

29 Greenberg, A. 2015. Hackers Remotely Kill a Jeep on the Highway–With Me in It. *Wired*, 21 July. Available at *http://bit.ly/2d3uCyG*.

Privacy Risks of the IoT

Now that we've reviewed some definitions of the IoT and explored the concept of privacy, let's examine some specifics more closely. This section identifies six privacy risks suggested by the increasing number of networked, sensing devices in the human environment.

Enhanced Monitoring

The chief privacy risk implied by a world of sensing, connected devices is greater monitoring of human activity. Context awareness through enhanced audio, video, location data, and other forms of detection is touted as a central value of the IoT. No doubt, important and helpful new services will be enabled by such detection, but the privacy implication is clear: you will be under observation by your machines and devices you do not control. Certainly, this exists in the world today—public CCTV, private security cameras, MAC address detection, location data capture from phones, Bluetooth beacons, license plate readers... the list is quite long, and growing. The human world is highly monitored so the issue becomes one of *scale*. Perhaps such monitoring is a condition of modern life; that observation by both the state and the private sector are core features of the social landscape.[30] This, then, is a central reason why "the right to be let alone" is a prominent value within privacy discourse.

30 Rule, J. et al. 1983. Documentary Identification and Mass Surveillance in the United States. *Social Problems* 31(2):222-234. Available at *https://www.jstor.org/stable/800214*; Wood, D. and Ball, K. (eds.) 2006. *A Report on the Surveillance Society: Public Discussion Document*. Wilmslow: Office of the Information Commissioner. Available at *http://bit.ly/2dweqHd*.

When American lawyers Warren and Brandeis proposed this right in 1890, it was in response to the appearance of a new technology—photography (Figure 4-1). They saw the potential for photography to intrude upon private spaces and broadcast what was captured to ever-widening audiences through newspapers.[31]

Figure 4-1. The privacy scourge of the 19th century: an early Kodak camera

The discussion of privacy and the IoT is no different: it is not the *Internet* of Things that raises hackles—it is the *Intimacy* of Things. Warren and Brandeis worried about photographers snapping pictures through bedroom windows. A modern version of this is the bathroom scale and your Fitbit broadcasting your weight and (lack of) exercise discipline to an audience larger than you intended.

Another touted feature of the coming wave of devices is their invisibility or unobtrusiveness. Here again is tension between an attractive design characteristic and social norms of privacy. If monitoring devices fade out of view, you might not know when you're being watched.

31 See footnote 11.

A direct result of enhanced monitoring is greater ease in tracking people's movements. That is, more devices—and therefore more organizations and systems—will know where you are, where you've been, and, increasingly, where you're going next.[32] Location privacy has been eroding for many years now, but that fact alone should not inure us to the possible harms that implies. In a 2009 paper, the Electronic Frontier Foundation listed a series of answerable questions implied by devices and organizations knowing your whereabouts:

- Did you go to an antiwar rally on Tuesday?
- A small meeting to plan the rally the week before?
- At the house of one "Bob Jackson"?
- Did you walk into an abortion clinic?
- Did you see an AIDS counselor?
- Did you skip lunch to pitch a new invention to a VC? Which one?
- Were you the person who anonymously tipped off safety regulators about the rusty machines?
- Which church do you attend? Which mosque? Which gay bars?
- Who is my ex-partner going to dinner with?[33]

The loss of location privacy was tremendously enhanced by GPS-enabled mobile phones, but that doesn't mean more devices tracking your movements are a nonissue. Not only will more devices track you in your home and private spaces, but the preceding questions also imply much greater tracking *in public*. Even though public spaces have often been seen to carry no expectation of privacy, a

32 Johnstone, C. 2010. Cell phones show human movement predictable 93% of the time. *Arstechnica* 24 Feb. Available at *http://bit.ly/2cWVgIP*.

33 Adapted from Blumberg, A. and Eckersley, P. 2009. *On Locational Privacy and How to Avoid Losing it Forever*. Electronic Frontier Foundation. Available at *https://www.eff.org/wp/locational-privacy*.

closer examination of that idea shows that it's not so clear cut.[34] Consider a conversation between two people at a restaurant held at a low volume, or a phone call about a sick family member while someone is on a train, or someone visiting adult bookstores. Should your wearable device manufacturer know if and when you go to church, to an STD clinic, or to hear a speech by an unpopular political candidate? Modern privacy thinking discards the easy public/private dichotomy in favor of a more contextual, fluid view.[35] Fairness, justice, and senses of vulnerability contribute to the norms of society. Though the law might allow the collection of a wide range of intimate information, that does not invalidate people's feelings of discomfort. To greater and lesser degrees, businesses listen to the feelings of customers, politicians listen to the perceived harms of their constituents, and judges absorb collective senses of right and wrong. **Discussion of the interplay of technology and intimacy are a vital component of how the two coevolve**. Most of the legal and policy frameworks that govern personal data and privacy were created in the 1970s, '80s and '90s. There is widespread agreement that these frameworks need updating, but the process is both slow and contentious. Laws like the European General Data Protection Regulation and legislative activity in the US Congress move things forward, but there will be starts and stops along the way as well as varied degrees of tolerance for enhanced monitoring in different countries.

Nonconsensual Capture

The introduction of more sensing devices into the human environment raises questions of consent, long considered a cornerstone of the fair treatment of people. Although individuals can consent to data collection by devices they purchase and install, what of the people who enter spaces and don't know the devices are there? Imagine a guest in your home; will she know that the TV is always listening? Or what of a health device in the bathroom? When you walk into a

34 For background on "privacy in public," see Nissenbaum, H. 1997. Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior* 7(3): 207-219. For the American legal perspective, see Reidenberg, J. 2014. Privacy in Public. Available at *http://bit.ly/2d3vVOI*. For a European perspective, see Edwards, L. and Urquhart, L. 2016. Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence? Available at *http://bit.ly/2dm5NQI*.

35 See footnote 22.

coffee shop and it scans your phone for any identification data it's broadcasting, is that acceptable? These questions may or may not directly implicate policy choices, but they do implicate design choices.

The IoT can be seen as a product development strategy—the introduction of enhanced monitoring, computation, and connectivity into existing product lines. Consider the car: new models are being released with integrated location tracking, cellular connectivity to the car's subsystems, and even the ability for drivers to tweet. As more vehicles incorporate IoT-like features, will drivers be able to turn them off? **When someone buys a new or used car and does not want to have her movements tracked when driving, is there a big switch to kill the data collection?** If the current take-it-or-leave-it attitude toward consent is imported into the IoT, car buyers might be told, "You can't prevent the car (and therefore the dealer, manufacturer, and others) from monitoring you. If you don't like it, don't buy the car." This is the world of No Opt-Out, and it diminishes the ability to withhold consent.

Regarding mobile devices, a European data protection watchdog group has said that users should have the ability to "continuously withdraw [their] consent without having to exit" a service (see the section "The view of the EU Article 29 Working Party" on page 40 later in this report). In the case of a car, whose obvious main purpose is driving, strong support of user choices could mean creating an ability to kill all non-essential data gathering. However, in the case of services that rely upon personal data to function, it's unclear how consent withdrawal can work without disabling core functionality. To support a principle of autonomy, consent must be kept meaningful. However, designing systems that can do so without a take-it-or-leave-it approach is not an easy task. Fortunately, the research domain known as *Usable Privacy* (see the section "Usable privacy and security" on page 43) attempts to address this issue head-on.

It's important to briefly mention the risk of intelligent, sensing toys and other devices collecting children's data. Children are a protected class in society, and both the US and Europe have special data protection provisions to reflect that. For example, the US Children's Online Privacy Protection Act (COPPA) requires a clear and comprehensive privacy policy describing how information is collected online from children, obtaining verifiable parental consent before

collecting, prohibiting disclosure of children's information to third parties, and providing parents access to their child's personal information for review or deletion.[36] Similarly, Europe's General Data Protection Regulation states:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles...[37]

As the IoT encroaches on more intimate spaces, the opportunity to intentionally or unintentionally collect children's data increases.

Collecting Medical Information

In the US, "traditional" medical information—lab results, doctors' notes, medical records, drug prescriptions, and so on—are held to strict standards of disclosure. The policy regime governing those disclosures is called the Health Insurance Portability and Accountability Act, or HIPAA,[38] and it specifies rules for who is allowed to see your medical information and the security of its transport. In Europe, medical data is deemed to be "sensitive personal data," and is subject to heightened regulatory requirements. Moreover, there are cultural prohibitions and sensitivities around medical information that people feel in varying degrees. Key reasons for such privileged treatment of medical information are:

- An awareness that people will not disclose critical information to doctors if they fear a lack of privacy, leading to untreated illnesses
- Stigmatization, loss of job, or other harms from revelation of a medical condition or disease
- Challenges to dignity: a belief that people have rights to control the flow of information about their physical and mental health

36 See COPPA FAQ, *http://bit.ly/2cwmxPc*.

37 Recital 38, General Data Protection Regulation. Available at *http://bit.ly/2cWWLXq*.

38 See *http://bit.ly/2cWWtQl*.

The IoT muddles the world of medical data. Health- and fitness-oriented consumer IoT devices introduce new technologies, new data gathering techniques, new information flows, and new stakeholders. At the same time, they break down the traditional categories of medical information regulation: healthcare provider, lab, patient, medical device, insurance company. When nonmedical fitness wearables gather heart rate, sleep pattern and times, blood pressure, oxygenation, and other biometric data, it becomes difficult to see how they differ from medical devices that trigger heightened quality, security, and privacy protections.[39] The difference is one of use—if a doctor is to rely upon the data, it necessitates a shift in product safety and reliability. If it's only you, device manufacturers don't have an incentive to pay for a higher regulatory burden; this, of course, also allows the device to remain at a consumer price rather than a far more expensive medical device price.

The privacy questions at issue are *who can see my health information*, *how is it protected*, and *what uses can it be put to?* Dr. Heather Patterson, an expert on privacy issues of mobile health devices, succinctly observed:

> The scale, scope, and nontraditional flows of health information, coupled with sophisticated data mining techniques that support reliable health inferences, put consumers at risk of embarrassment and reputational harm, employment and insurance discrimination, and unwanted behavioral marketing.[40]

HIPAA is quite narrow in whom it applies to: health plans, healthcare providers, clearinghouses, and their business associates. IoT devices used in the course of medical treatment will likely fall under HIPAA, but fitness wearables, quantified self devices, sleep detectors, and any other object that tracks biometrics, vital signs, or other health information used for personal interest likely will not. As such, this sensitive information is weakly governed in the US in terms of

39 However, there is at least one report of "consumer-grade" medical information being used in an emergency medical context. See Jardin, X. 2016. Emergency room doctors used a patient's Fitbit to determine how to save his life. *boingboing* 7 Apr 2016. Available at *http://bit.ly/2ddVQDs*.

40 Patterson, H. 2013. Contextual Expectations of Privacy in Self-Generated Health Information Flows (p. 2). *TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy*. Available at *http://ssrn.com/abstract=2242144*.

privacy and security.[41] For example, a 2013 study of 23 paid and 20 free mobile health and fitness apps found the following:

- 26% of the free and 40% of the paid apps had no privacy policy.
- 39% of the free and 30% of the paid apps sent data to someone not disclosed in the app or the privacy policy.
- Only 13% of the free and 10% of the paid apps encrypted all data transmissions between the app and the developer's website.[42]

One area of concern is insurance companies using self-tracked fitness and health information against their customers. In *A Litigator's Guide to the Internet of Things*, the author writes:

> ...there are downsides to a person's voluntary collection of sensitive health information using a wearable device. Insurers and employers seeking to deny injury and disability claims can just as easily use wearable devices to support their own litigation claims and positions...[43]

In 2014, a personal trainer in Canada brought a lawsuit claiming that she was still suffering injuries from a car accident four years prior. The plaintiff's lawyers used her Fitbit data analyzed by a third-party company to corroborate the claims.[44] Privacy law expert Kate Crawford observed:

> The current lawsuit is an example of Fitbit data being used to support a plaintiff in an injury case, but wearables data could just as easily be used by insurers to deny disability claims, or by prosecutors seeking a rich source of self-incriminating evidence.[45]

41 For an in-depth explanation of both the lack of HIPAA protections for wearables and weak governance generally, see footnote 40, pp. 16-20.

42 Ackerman, L. 2013. *Mobile Health and Fitness Applications and Information Privacy*. Available at *http://bit.ly/2dhGc89*.

43 Peyton, A. 2016. A Litigator's Guide to the Internet of Things. *Richmond Journal of Law & Technology* 22(3):9-28. Available at *http://bit.ly/2dtHe0f*.

44 Olson, P. 2014. Fitbit Data Now Being Used in the Courtroom. *Forbes*. Available at http://bit.ly/2dm7z4A.

45 Crawford, K. 2014. When Fitbit is the Expert Witness. *The Atlantic*. Available at *http://theatln.tc/2cwn43M*.

Breakdown of Informational Contexts

A theme that emerges from the aforementioned risks is the blending of data from different sources and facets of people's lives. From enhanced monitoring we get the concept of *sensor fusion*. Legal scholar Scott Peppet writes:

> Just as two eyes generate depth of field that neither eye alone can perceive, two Internet of Things sensors may reveal unexpected inferences... Sensor fusion means that on the Internet of Things, "every thing may reveal everything." By this I mean that each type of consumer sensor... 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.[46]

The implication of sensor fusion and the trend toward sharing data across multiple contexts—health, employment, education, financial, home life, and so on—is the further breaking down of *informational contexts*. Privacy scholar Helen Nissenbaum and her colleagues and students have spent more than a decade refining the theory of *contextual integrity*, which attempts to explain why people feel privacy violations.[47] The theory focuses on the informational norms of appropriateness and transmission: which information is appropriate to reveal in a given context, and the norms that govern the transfer of one party to another. It's appropriate for you to reveal medical information to your doctor but not your financial situation, and the reverse is true with your accountant. As to transmission, it's right for a doctor to send your medical information to labs and your insurance company, but not to the police. When these boundaries are inappropriately crossed, people experience it as a violation of their privacy.

Context sensitivity exists within a variety of laws and policies. In the US, the Fair Credit Report Act specifies that credit reports assembled by credit reference agencies, such as Experian and Equifax, can be used only when making decisions about offering someone credit, employment, underwriting insurance, and license eligibility. The original intent behind "whitelisting" these uses was to preserve the

46 Peppet, S. 2014. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review* 93(1):87-176. Available at *http://bit.ly/2d0mmC7*.

47 See footnote 22.

appropriate use of credit reports and support privacy.[48] Across the Atlantic in Germany, a constitutional court case determined that the state could not be considered as one giant data processor. That is, information collected for one context, such as taxes, cannot be commingled with data from another context, such as benefits, without legal justification.

Modern discussions of privacy recognize that *context matters*: where information is gathered, which information is gathered, and with whom it's shared. In the case of medical information or credit reports, norms of appropriateness and transmission have been at least minimally addressed within the law, but there is a huge amount of data collected about us that policy has yet to tackle. In 2012, the White House released a Consumer Privacy Bill of Rights, which states:

> Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data...[49]

This rationale underpins the proposed Consumer Privacy Bill of Rights Act of 2015,[50] introduced by the Obama Administration. The bill is a step in the right direction, incorporating some concerns about contextual treatment of personal data in the US.[51]

With regard to connected devices, here are some questions to consider:

48 Hoofnagle, C. 2013. How the Fair Credit Reporting Act Regulates Big Data. Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet. Available at *http://ssrn.com/abstract=2432955*.

49 White House. 2012. *Consumer Data Privacy in a Networked World*. Available at *http://bit.ly/2dl84vh*.

50 White House. 2015. Administration Discussion Draft: Consumer Privacy Bill of Rights Act. Available at *http://bit.ly/2dm7UUJ*.

51 See the Center for Democracy and Technology's "Analysis of the Consumer Privacy Bill of Rights Act," available at *http://bit.ly/2ddezv5*.

- How do I ensure that my employer does not see health information from my wearables if I don't want it to?
- Can my employer track me when I'm not at work?
- If I share a connected device with someone, how do I ensure that my use of it can be kept private?
- What rules are in place regarding data collected in my home and potential disclosure to insurance companies?
- What data from my car can my insurer obtain?
- Who can see when I'm home or what activities I'm engaging in?
- What rights do I have regarding the privacy of my whereabouts?

Diversification of Stakeholders

The IoT is being brought about by a wide spectrum of players, new and old. Of course, well-established manufacturers such as Siemens, Toyota, Bosch, GE, Intel, and Cisco are developing new connected devices each year. However, startups, hobbyists, and young companies are also hard at work bringing about the Thing future. The difference between these two groups is that one is accustomed to being enmeshed in a regulatory fabric—data protection rules, safety regulations, best practices, industrial standards, and security. Newer entrants are likely less familiar with both privacy and security practices and rules. As mentioned earlier, privacy costs money, and so does security. Ashkan Soltani, former chief technologist of the FTC, said in 2015:

> Growth and diversity in IoT hardware also means that many devices introduced in the IoT market will be manufactured by new entrants that have very little prior experience in software development and security.[52]

Startups and small companies are under pressure to make sure their products work, fulfill orders, and satisfy their funders. Spending time, capital, and mental energy on privacy might be a luxury. Alex Deschamp-Sonsino, founder of the London IoT Meetup and creator

52 Soltani, A. 2015. What's the security shelf-life of IoT? *Tech@FTC*. Available at http://bit.ly/2dtGOqI.

of the WiFi-enabled Good Night Lamp,[53] summarized this succinctly: "I got 99 problems and privacy ain't one."[54]

Augmenting these issues is a culture of *data hoarding*[55]—the drive to collect all data whether it will be used now or not—which goes against the grain of the privacy principle of minimizing data collection. The economic and cultural pressures affecting companies encourage them to collect and monetize as much as possible.

Think of the collection of personal data as a supply chain. On one end are resources—human beings and the data they shed—which are collected, transported, enriched, and used by first parties and then sold to third parties and sometimes returned to the human source. In that chain are intermediaries: component manufacturers, transport layers, networking and communications, storage, consultants, and external analysis. As the ecosystem for connected devices evolves, that supply chain becomes longer while at the same time the data sources become larger and richer. The question then becomes how to ensure that everyone is playing fairly. How do organizations ensure that user privacy preferences are respected? A dominant method has been contractual representation: companies promise one another that they will behave in certain ways. As these personal data supply chains lengthen and diversify, it's important to find additional ways to prevent leakage and inappropriate uses of sensitive information.

More Backdoor Government Surveillance

Since the 2013 revelations of NSA whistleblower Edward Snowden, the public has been made aware of an exceedingly broad and far-ranging surveillance agenda by governments around the world. One critical component of this has been the passage of personal data collected by private companies to the government through both direct legal requests and, according to investigative reporters, spying inside

53 *http://goodnightlamp.com/*.

54 Comment made during presentation at Internet of Things Forum 2015, Cambridge, UK.

55 See Matwyshyn, A. 2009. Introduction. In Matwyshyn, M. (ed.), *Harboring Data: Information Security, Law, and the Corporation* (pp. 3-18). Stanford: Stanford Law Books.

the companies.[56] The relevance to the IoT is that the coming wave of devices is anticipated to collect tremendous amounts of personal, intimate data. One possible conclusion is that some of this data will fall into the surveillance dragnet. In early 2016, James Clapper, the US director of national intelligence, testified to Congress:[57] "In the future, intelligence services might use the [Internet of Things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials." Debates about law enforcement and intelligence overreach commingle with concerns about the IoT's penetration into intimate spaces. This amplifies the need for discussion of governance and technical methods of privacy protection.

56 Greenwald, G. et al. 2013. Microsoft handed the NSA access to encrypted messages. *The Guardian*. 12 July. Available at *http://bit.ly/2cycTAq*; Greenwald, G. and MacAskill, E. 2013. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. 7 June. Available at *http://bit.ly/2dm8LVq*.

57 Ackerman, S. and Thielman, S. 2016. US intelligence chief: we might use the internet of things to spy on you. *The Guardian*. 9 Feb. Available at *http://bit.ly/2dm8Ngb*.

How Are the IoT and Big Data Related with Regard to Privacy?

Big Data—that is, statistical analysis of large datasets, often for the purposes of prediction—has been a hotly debated topic for several years now. Scholars danah boyd and Kate Crawford summed up its importance and reach in a seminal 2011 essay: "Data is increasingly digital air: the oxygen we breathe and the carbon dioxide that we exhale. It can be a source of both sustenance and pollution."[58]

The benefits of Big Data are profound indeed: better disease detection, more efficient travel ticketing, harmful drug interaction detection, pricing optimization, and improved traffic management to name but a few.[59] The power of predictive data analytics, however, can wreak harms and amplify social problems as much as it can improve markets, healthcare, and the human environment. Issues such as discrimination, unaccountable automated processing, data-use ethics, and privacy are at the forefront of academic and legal meditations on the challenges that Big Data poses.[60] The IoT is characterized by a proliferation of sensing and monitoring—ergo, **the IoT acts as an *input* to large-scale data analytics**. Location detection, movement patterns, vital signs, identification, device use patterns—all of these are the myriad bits of data that feed large datasets for analysis by public and private organizations.

58 boyd, d. and Crawford, K. 2011. Six Provocations for Big Data. Presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society," September 21, 2011. Available at *http://ssrn.com/abstract=1926431*.

59 See Mayer-Schönberger, V. and Cukier, K. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray Publishers; Tene, O. and Polenetsky, J. 2013. Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property* 11(5):239-273. Available at *http://ssrn.com/abstract=2149364*.

60 See Gangadharan, S., Eubanks, V. and Barocas, S. (eds.) 2014. *Data and Discrimination: Collected Essays*. Washington, DC: Open Technology Institute, New America Foundation. Available at *http://bit.ly/2dm956L*; Collected papers from Workshop on "Big Data and Privacy: Making Ends Meet" held by Future of Privacy Forum and Stanford Center for Internet and Society, 2013. Available at *http://bit.ly/2dmdEt3*.

How Is Privacy Protected?

Before reviewing different frameworks that we can bring to bear on the privacy challenges of the IoT, it's helpful to review the main methods of privacy preservation. Note that these categories often overlap and reinforce one another in a "regulatory mix."

Law and Policy

Likely the most familiar mechanism, this includes laws such as HIPAA for medical information, FERPA for student information, the EU Data Protection Directive, the UK Data Protection Act, the US Privacy Act of 1974, and other formal legal instruments. It includes torts, court decisions, administrative policy, government contracting rules, and rules laid down by regulatory agencies. Two elements to keep in mind are *voluntary compliance* and *enforcement*. That is, some policies encourage voluntary behavior in line with the policies' goals, whereas others require it and use coercive sanctions to achieve conformance. Voluntary compliance might be encouraged by *soft law* or *aspirational policy*—formal laws or policies that do not contain a sanction mechanism. One example is the aforementioned Consumer Privacy Bill of Rights. Released within a report called *Consumer Data Privacy in a Networked World*,[61] the Consumer Privacy Bill of Rights was policy in the sense that it expressed the wishes of the Obama Administration, but it was not a required practice within the commercial world. In 2015, however, the Administration attempted to turn this soft law into hard law by promoting a draft of the Consumer Privacy Bill of Rights Act, a pro-

61 See footnote 50.

posed law that turns the aspirational principles of the 2012 version into one that could be enforced by the FTC and State Attorneys General.

Contract

Privacy policies and terms and conditions are the most visible mechanisms of privacy management. They are agreements between an organization and a data source, that is to say, a human being. When a person presses an "I Agree" button before using a website or service, she is entering into a binding contract. Contracts are not protection methods, per se, in that they are not by nature designed to protect people's interests or rights—they are neutral "containers" for rules about how an organization will behave. They can be written with a bias toward the protective treatment of people, or so as to privilege an organization's wishes. Contracts are constrained by many factors, including laws, court decisions, and existing business arrangements. In the US, if a company publishes a privacy policy, the Federal Trade Commission views it as a promise to consumers. If the company breaks that promise and does things with data it did not say it would, the FTC can investigate. Contracts between companies sometimes include requirements for each party to behave in a constrained way, adhering to particular security practices, promising not to use data in a certain way, and so on. These are two ways in which contracts become protective instruments.

Market Controls

Privacy can be protected by the behavior of the market. That is, the market rewards and punishes based on the preferences of consumers and buyers. A business might do something completely legal and, to them, completely normal. However, if the buying public does not like it for some reason, it can punish the business by refusing to buy or worse. An example is Samsung's sale of a television in 2015 that could accept voice commands. Its privacy policy said that the TV could pick up bits of personal communication spoken near it. This caused a spate of "Big Brother" comparisons in the media, injuring Samsung's brand a little, which could potentially harm

sales.[62] Market punishment through violation of consumer expectations, norms, and wishes is a core mechanism for an economically driven vision of privacy preservation.

Self-Regulation

One of the more common methods of privacy protection, self-regulation, as the name implies, means that businesses govern their own behavior with regard to privacy. The vehicles for self-regulation are agreed-upon codes of conduct, best practices, industry-based licensure, certification marks (see the next section), and other forms of regulating behavior where sanctions come from industry or the market and not from government. US examples include the Network Advertising Initiative, the Digital Advertising Alliance's AdChoices, and the ICT Coalition for Children Online. When governments become involved with self-regulatory efforts by, for example, taking on some of the tasks of managing the regulation or its sanctioning power, it is called *co-regulation*.[63] Self-regulation is a core feature of the American and European privacy landscapes, though its efficacy is a matter of much debate.[64]

Certification and Seals

There is a wide variety of certification programs and privacy seals. Mandatory certification in the privacy realm is rare, so when businesses apply to become certified or to obtain the right to display a seal, it's a voluntary choice to signal to various audiences their adherence to a set of guidelines or principles. When doing so, the two key methods of attesting to adherence are self-certification, by which a business assesses itself for conformance, and third-party certification, by which someone from outside an organization assess it for conformance. Examples of privacy certifications and seals are

62 Wingfield, N. 2015. Samsung Tweaks Television Policy Over Privacy Concerns. *New York Times*, 10 Feb 2015. Available at *http://nyti.ms/2cXdw4I*.

63 Marsden, C. 2011. *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*. Cambridge: Cambridge University Press.

64 Gellman, B. and Dixon, P. 2016. Failures of Privacy Self-Regulation in the United States. In D. Wright and P. De Hert (eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (pp. 53-78). Dordrecht: Springer; Federal Trade Commission. 2009. Self-Regulatory Principles For Online Behavioral Advertising. Available at *http://bit.ly/2cwzOr0*.

those offered by TRUSTe, EuroPriSe, and a seal for compliance with French data governance procedures offered by CNIL, the French data protection authority.

Best Practices

Companies, trade associations, nonprofits, governments, and others publish sets of the "best" practices for data handling and privacy for various segments of the market. These are, of course, subjective, but they can be effective when created with the help of experts who balance practicality, realism, and feasibility with broad goals and ethics. When done poorly, best practices merely reinforce existing business practices or offer infeasible suggestions. Examples of best practices abound; organizations like the UK Information Commissioner's Office, the American Bar Association, TRUSTe, the FTC, the W3C and many other bodies publish data privacy practice guidelines.[65] Best practices are nearly always voluntary.

Norms

When behaviors become more or less generally agreed upon within a group, they are called norms. Some are widely accepted—murder is evil and forbidden, for example—others, less so, such as the acceptability of talking during a movie. Norms are one of the constitutive forces of society, given voice through a variety of mechanisms; they play a central role in privacy. Consider the prohibition of surveillance in bathrooms. Whether explicitly banned by laws or not, this privacy norm powerfully constrains behavior in America and Europe. But what about eavesdropping in public? Here we see another norm that is less widely accepted; it's fine for some and impermissible for others. Feelings such as vulnerability, exposure, or a lack of control over data about us are important components of norms. They contribute to the social dialogue that ultimately informs the regulatory methods described earlier.

65 Information Commissioner's Office. (n.d.). Improve Your Practices. Available at *http://bit.ly/2db9OnQ*; TRUSTe. (n.d.). Protecting Customer Information Online. Available at *https://www.truste.com/resources/privacy-best-practices/*; W3C. 2012. Web Application Privacy Best Practices. Available at *https://www.w3.org/TR/app-privacy-bp/*; Federal Trade Commission. 2015. *Internet of Things: Privacy & Security in a Connected World* (pp. 27-46). Available at *http://bit.ly/2dwxDIY*.

Connected devices appearing in public and burrowing into intimate personal spaces encourage us to reflect on our privacy norms. Is it acceptable for children's toys to listen to what they say and then transmit it to a company's servers?[66] Should employers be able to get access to your fitness tracker's data? How about your location history when you're off the clock? Should devices in your home be able to identify your guests and remember times they arrive and leave? People's answers to these and similar questions will almost certainly vary, and the answers form part of our expectations and senses of fairness as we become further intertwined with technology.

Technology

Privacy is often protected through technical means. Just as the locks on your doors and windows offer some protection from burglary, we use software and hardware to prevent theft or unauthorized access to private data. By now, most people have heard of encryption, which is the use of complex math to scramble data; only with the right key (a chunk of data) can we unscramble it. But even the use of passwords is an example of technical means of privacy protection. Designing, building, buying, learning to use, and implementing any technology costs money. Systems that are designed with strong mechanisms to protect the privacy of data will cost more than systems with weak ones. This is a key issue in the IoT, which, at the consumer level, will be built to be cost-conscious. Further, companies that are good at making Things, like cars and wearables and TVs, might not be good at security and privacy. Encryption and other complicated methods of protecting privacy require specialized know-how and investment. That said, using technology to preserve privacy—versus the social methods of laws, contracts, markets, best practices, and norms—is one of the most important methods available. Consider again the example of locks on doors; you can rely on people not to break in because of the threat of arrest and because such behavior is socially unacceptable, but a piece of metal that prevents your door from opening is still an excellent strategy.

66 Walker, L. 2016. Security Firm Finds New Hello Barbie Vulnerabilities. *Newsweek* 26 Jan. Available at *http://bit.ly/2cXdrhz*.

Frameworks to Address IoT Privacy Risks

Now that we've explored what the IoT is, examined some of the many views of privacy, and considered the privacy risks the IoT portends, we can turn to different frameworks and tools that can be brought to bear on those risks.

Historical Methods of Privacy Protection

In many ways, IoT privacy risks reflect general historical privacy risks: surveillance, unbridled collection, poor security practices, limited privacy management knowledge inside companies, weak consent models, and loss of user control. Similarly, there are established, general tactics that we can employ at various layers of IoT system design:

Data minimization

Emerging from the 1970s, one of the oldest strategies in privacy and data protection is to minimize collection and use. The idea is very simple: limit the amount and type of data collected, limit its use, and limit its storage. As the FTC neatly states: "Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place."[67] Further, limiting use helps to ensure that the data is used in the context in which it was collected, thereby avoiding function creep. In the IoT, minimization can occur at two levels:

67 Federal Trade Commission. 2015. *Internet of Things: Privacy & Security in a Connected World*. Available at *http://bit.ly/2dwxDIY*.

Design: Designers should include only the sensors, functions, and capabilities necessary for a device's core feature set versus including the ability to capture information for a future yet-undetermined use.

Storage: Devices and systems shouldn't retain data that's no longer in use or relevant, nor should they necessarily keep raw data.

Encryption

Scrambling messages which can then be unscrambled only by using a related key is known as encryption.[68] As mentioned earlier, in the modern sense, encryption relies on complex math executed by computers or dedicated hardware to make messages unreadable. For connected devices, the main use of encryption would be for data storage and transmission so that unauthorized parties cannot see the information that's been collected.

Transparency

Transparency refers to practices that ensure data subjects know what is being collected about them, when, how it is used, and with whom it is shared. This is a central principle underpinning the use of privacy policies. Given how IoT devices can fade into the background or otherwise invisibly collect personal data, transparency remains a critical strategy. However, because IoT devices might have reduced user interactions in comparison with traditional computing, the challenge of meaningfully informing users is magnified. Thankfully, this challenge is being answered by *usable privacy* researchers (see the section that follows).

Anonymization/pseudonymization/de-identification

These three terms all point to the same strategy: removing identifying information from data collected about a person (name, IP address, phone number, etc.). De-identification is a

68 Research shows that this method of protecting information originates around 1900 BC. See Waddell, K. 2016. The Long and Winding History of Encryption. *http://theatln.tc/2debU8g*.

cornerstone of medical research, where ethics and policy mandate its use. In most other areas, its use is encouraged rather than required. Law and policy often point to de-identification as a desirable strategy, but research and news reports have shown that it's neither easy nor a panacea.[69] Also, de-identification can conflict with business goals because identifiable data is far more valuable for marketing purposes. Further, de-identification is not binary—data is not simply identifiable or not. Recent work by the Future of Privacy Forum describes a spectrum of characteristics—direct versus indirect identifiers, potentially identifiable versus not readily identifiable, de-identified versus "protected" de-identified, and others.[70]

Emerging Frameworks for IoT Privacy Challenges

Even though IoT privacy risks reflect historical risks, there are also particular challenges related to technology, sector, scale, and mode of governance. The frameworks and best practices that follow represent some of the current thinking about how to address IoT-specific challenges.

The view of the US Federal Trade Commission

In late 2013, the FTC hosted a workshop called *The Internet of Things: Privacy and Security in a Connected World*. The workshop, which included leading technologists and academics, industry representatives, and consumer advocates, was a broad review of IoT concepts and potential privacy and security challenges. The resultant report collected the participants' and FTC staff's recommendations for best practices for companies in the IoT space:

- Conduct a privacy and/or security risk assessment.
- Test security measures before launching products.

69 See, e.g., Ohm, P. 2010. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 57(6):1701-1777. Available at *http://ssrn.com/abstract=1450006*.

70 Polonetsky, J., Tene, O and Finch, K. 2016. Shades of Gray: Seeing the Full Spectrum of Data De-identification. Available at *http://bit.ly/2deeT08*; Future of Privacy Forum. 2016. A Visual Guide to Practical Data De-identification. Available at *http://bit.ly/2d41FkL*.

- Incorporate the use of smart defaults, such as requiring consumers to change default passwords during the setup process.
- Implement reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or network.
- Inform consumers about the "shelf-life" of products—how long a company plans to support them and release software and security patches.
- Impose reasonable limits on the collection and retention of consumer data (in other words, data minimization).
- Companies should consider de-identifying stored consumer data, publicly commit not to re-identify the data, and have enforceable contracts in place with any third parties with whom they share the data, requiring them to commit to not re-identifying the data as well.
- Continue to implement *Notice and Choice*, that is, providing consumers data use or privacy policies and giving them the ability to agree to or decline data collection. The report states, "Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents."

The view of the EU Article 29 Working Party

When Europe enacted its Data Protection Directive in 1995, it also created a watchdog group called the Article 29 Working Party (Art29WP), made up of data protection regulators from each of the EU member states. This independent group keeps an eye on data protection and privacy issues across all of Europe, issuing advice and proposing guidelines as new technology develops. In its 2014 Opinion on the Internet of Things,[71] it proposed a wide variety of recommendations:

- Believing that organizations mainly need aggregate data, the Art29WP states that raw data should be deleted as soon as the necessary data has been extracted, and that developers who do

71 Article 29 Working Party. 2014. Opinion 8/2014 on Recent Developments on the Internet of Things. Available at *http://bit.ly/2cXhOZM*.

not need raw data should be prevented from ever seeing it. The transport of raw data from the device should be minimized as much as possible.

- If a user withdraws his consent, device manufacturers should be able to communicate that fact with all other concerned stakeholders.
- IoT devices should offer a "Do Not Collect" option to schedule or quickly disable sensors, similar to a "Do Not Disturb" feature on mobile phones, as well as the silencing of the chips, discussed in a moment.
- Devices should disable their own wireless interfaces when not in use or use random identifiers (such as randomized MAC addresses) to prevent location tracking via persistent IDs.
- Users should be given a friendly interface to be able to access the aggregate or raw data that a device or service stores.
- Devices should have settings to be able to distinguish between different people using it so that one user cannot learn about another's activities.
- Manufacturers and service providers should perform a Privacy Impact Assessment on all new devices and services before deploying them (see "Privacy Impact Assessments" on page 46).
- Applications and devices should periodically notify users when they are recording data.
- Information published by IoT devices on social media platforms should, by default, not be public nor indexed by search engines.

Silencing of the chips

In the mid 2000s, the European Commission funded a great deal of research into the IoT, though much of this work was focused on Radio Frequency ID (RFID) technologies. Out of this research came a belief that people have a right to disconnect from their networked environment, and therefore be able to deactivate the tracking functions of their RFID devices. French Internet expert Bernard Benhamou coined the term the "silence of the chips" to capture this belief:

> [Citizens] must be able to control the way in which their personal data are used, and even the way in which these [RFID] chips can be deactivated. So in the future, citizens will have to intervene in the architecture of these systems in order to enjoy a new kind of freedom: the "silence of the chips."[72]

The oft-cited example for the expression of this right was in the retail sector.[73] If a person bought goods with embedded RFID tags, the principle of the silence of the chips would ensure that consumers could kill the tags temporarily or permanently so that purchased goods could not be tracked outside the store. An updated version of this right could be formulated as a Do Not Collect feature added to devices, wherein users could simply "blind" all of the sensors on a device (see the section "The view of the EU Article 29 Working Party" on page 40).

Privacy engineering

As the earlier section Chapter 3 shows, privacy is complex, culturally infused, ambiguous, and conceptually dense. For lawyers, researchers, compliance officers, policy-makers, and others, this comes with the territory. However, for those tasked with embedding privacy directives into technical systems—engineers, programmers, system architects, and the like—this contested, indefinite character can be detrimental. Engineers and their kin work in a world of definitions, specifications, constrained vocabularies, repeatability, and structured change. To bridge the two worlds, the ambiguous and the specified, a new field has begun to emerge: privacy engineering.[74] Although a unified definition has yet to be established, key characteristics of privacy engineering are requirements gathering, diagramming and modeling, use cases, classification, business rules, auditing, and system lifecycles. As such, privacy engineering overlaps with and compliments risk management frameworks and compliance activities (see the section "Privacy Impact Assessments" on

72 Quoted in Santucci, G. 2013. Privacy in the Digital Economy: Requiem or Renaissance? Available at *http://bit.ly/2dlpFDq*.

73 Baldini, G. et al. 2012. *RFID Tags: Privacy Threats and Countermeasures*. European Commission: Joint Research Centre. Available at *http://bit.ly/2dlrKPo*.

74 Dennedy, M., Fox, J. and Finneran, T. 2014. The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value. New York: Apress. Available at *https://www.apress.com/9781430263555*; Bracy, J. 2014. Demystifying Privacy Engineering. IAPP. Available at *http://bit.ly/2dbbhdV*.

page 46). Even though this field is not particular to the IoT, it's an important advancement in the ways that companies can approach the challenge of building privacy-preserving, ethical, respectful technical systems.

Vehicle privacy protection principles

In November of 2014, two car-manufacturing trade bodies released a set of Privacy Principles for Vehicle Technologies and Services.[75] Modeled largely on the White House's Consumer Privacy Bill of Rights,[76] the automaker's privacy principles call for transparency, choice, respect for context, data minimization, and accountability. Twenty members[77] of the two organizations have adopted the voluntary principles, committing to obtaining affirmative consent to use or share geolocation, biometrics, or driver behavior information. Such consent is not required, though, for internal research or product development, nor is consent needed to collect the information in the first place. One could reasonably assert that biometrics and driver behavior are not necessary to the basic functioning of a car, so there should be an option to disable most or all of these monitoring functions if a driver wishes to. The automakers' principles do not include such a provision. Still, the auto industry is one of the few to be proactive regarding consumer privacy in the IoT space. The vehicle privacy principles provide a foundation for critical discussion of the impact of new technologies in cars and trucks.

Usable privacy and security

The field of usable privacy and security examines how people interact with systems, and the design and use challenges that arise from those systems' privacy and security characteristics. Jason Hong, Lorrie Cranor, and Norman Sadeh, three senior professors in the field, write:[78]

75 Alliance of Automobile Manufacturers and Association of Global Automakers. 2014. Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services. Available at *http://bit.ly/2ddCvhT*; see also FAQ at *http://bit.ly/2d445ji*.

76 See footnote 50.

77 See Participating Members at *http://bit.ly/2cQ4h4w*.

78 Hong, J., Cranor, L. and Sadeh, N. 2011. Improving the Human Element: Usable Privacy and Security. Available at *http://bit.ly/2cyrifS*.

> There is growing recognition that privacy and security failures are often the results of cognitive and behavioral biases and human errors. Many of these failures can be attributed to poorly designed user interfaces or secure systems that have not been built around the needs and skills of their human operators: in other words, systems which have not made privacy and security *usable*.

The field draws upon a wide variety of disciplines, including human–computer interaction, computer security, mobile computing, networking, machine learning, cognitive psychology, social psychology, decision sciences, learning sciences, and economics.[79] Pioneering work has been done at the CyLab Usable Privacy and Security Lab[80] at Carnegie Mellon University and similar labs, and at the annual Symposium on Usable Privacy and Security.[81] Researchers have addressed issues directly relating to the IoT, including the following:

Authentication

Passwords have been a necessary evil since the 1960s,[82] but there is widespread agreement that people have too many to contend with, resulting in poor choices and weakened system security. Usable privacy and security researchers measure the usability and efficacy of authentication interactions and offer new methods to improve the overall system. IoT devices might lack keyboards, screens, or biometric readers, further complicating authentication. Research in this area serves the twin goals of improving the user experience and helping to ensure devices retain strong authentication features.

Privacy notices

The use of privacy notices to inform people of what data is collected about them, how it's used, and with whom it's shared is a common practice in the US and Europe. However, it's also widely agreed that these notices are ineffective because they are

79 Ibid.

80 *https://cups.cs.cmu.edu/*.

81 *https://www.usenix.org/conference/soups2016*.

82 Yadron, D. 2014. Man Behind the First Computer Password: It's Become a Nightmare. Available at *http://on.wsj.com/2cQ4MLD*.

too long and people are exposed to too many of them.[83] Again, a lack of screens on IoT devices exacerbates the problem. Usable privacy researchers have addressed this issue head-on, proposing the following design practices:[84]

Create different notices for different audiences, such as primary, secondary and incidental users.

Provide relevant and actionable information, in particular, explaining when data is collected or shared in ways that a user could not be expecting.

Use layered and contextual notices. Researchers argue that "showing everything at once in a single notice is rarely effective. Instead, all but the most simple notices should consist of multiple layers."[85] Different times, methods, and granularity of information displayed help users to absorb what's being presented.

Involve users in the design of notices through user-centered[86] *or participatory design.*[87] Include user testing and usability evaluation as part of the overall system's quality assurance.

---

83 A 2014 report to President Obama observed: "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent." See http://bit.ly/2d44pP6; see also Madrigal, A. 2012. Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days. *The Atlantic* 1 Mar. Available at *http://theatln.tc/2ddD6QK*.

84 This section is drawn from Schaub, F., Balebako, R., Durity, A. and Cranor, L. 2015. A Design Space for Effective Privacy Notices. Available at *http://bit.ly/2dwBkhZ*.

85 See footnote 84.

86 Usability.gov defines user-centered design as a process that "outlines the phases throughout a design and development life-cycle all while focusing on gaining a deep understanding of who will be using the product." See *http://bit.ly/2cXjmTS*.

87 Computer Professionals for Social Responsibility defined participatory design as "an approach to the assessment, design, and development of technological and organizational systems that places a premium on the active involvement of workplace practitioners (usually potential or current users of the system) in design and decision-making processes." See *http://bit.ly/2cwDUiL*.

Because privacy notices are mandated by regulation and user testing involves cost, businesses have little incentive to be progressive or experimental. As such, university-based experimentation and research is vital to advance the state of the art in notifying users and in interface design. The field of Usable Privacy and Security is essential to address the particular interface challenges of the IoT.

Privacy Impact Assessments

A Privacy Impact Assessment (PIA) is a systematic process to evaluate the impact and risks of collecting, using, and disseminating personally identifiable information in a project, product, service, or system. The goal is to identify privacy risks; ensure compliance with national or local laws, contractual requirements, or company policy; and put risk mitigation strategies in place. Privacy scholar Gary T. Marx writes that a PIA "anticipates problems, seeking to prevent, rather than to put out fires."[88] As such, a PIA is an integral part of planning and development rather than an afterthought. PIAs have traditionally been used by government agencies, but they have clear and direct application in the commercial sphere. The recently passed EU General Data Protection Regulation requires PIAs when data processing is "likely to result in a high risk for the rights and freedoms of individuals."[89] Each EU country will determine exactly what those activities will be, but it's safe to assume that some IoT systems will trigger this requirement when the GDPR comes into effect in 2018.

According to expert Toby Stevens,[90] PIAs analyze risks from the perspective of the data subject and are complementary to security risk assessments, which are done from the perspective of the organization. A security risk assessment might conclude that the loss of 10,000 customer records is an acceptable risk for the organization, but the PIA will consider the impact on the affected individuals. PIAs are also directly beneficial to the organization by preventing costly redesigns or worse—helping to curtail regulator fines, irreparable brand damage, lawsuits, or loss of customers because of a

88 Marx, G. 2012. Privacy is Not Quite Like the Weather. In D. Wright and P. De Hert (eds.), *Privacy Impact Assessment* (pp. v-xiv). Dordrecht: Springer.

89 Maldoff, G. 2016. The Risk-Based Approach in the GDPR: Interpretation and Implications. Available at *http://bit.ly/2d44diR*.

90 *http://privacygroup.org/*.

significant privacy failure. They are, as the New Zealand PIA Handbook states, an "early warning system... enabling [organizations] to identify and deal with their own problems internally and proactively rather than awaiting customer complaints, external intervention or bad press."[91] PIAs allow business stakeholders to get their ethics down on paper and into a process that can be applied over and over as new products and services are developed; this in turn enables staff to understand executive risk appetite.

A PIA is a flexible instrument, and can be configured to meet a variety of needs, policies, and regulations. Here are some basic elements it can include:

- Data sources
- Data flows through the product/service lifecycle
- Data quality management plan
- Data use purpose
- Data access inventory—who inside and outside the organization can access the data
- Data storage locations
- Data retention length
- Applicable privacy laws, regulations, and principles
- Identification of privacy risks to users and the organizations and the severity level (e.g., High, Medium, Low)
- Privacy breach incident response strategy

In 2011, a group of industry players and academics authored an RFID PIA framework[92] that was endorsed by the European Commission. At the time, RFID technology was considered a cornerstone of the IoT ecosystem, and the framework focuses on it to the exclusion of other IoT-like technologies. Use of the framework is not required by law, but is instead "part of the context of other

91 Office of the Privacy Commissioner. 2007. *Privacy Impact Assessment Handbook*. Auckland: Office of the Privacy Commissioner. Available at *http://bit.ly/2d3Qev4*.

92 See *http://bit.ly/2dmorbf*; also, for much more context on the RFID PIA and its development, see Spiekermann, S. 2012. The RFID PIA—Developed by Industry, Endorsed by Regulators. In D. Wright and P. De Hert (eds.), *Privacy Impact Assessment*, (pp. 323–346). Dordrecht: Springer. Available at *http://bit.ly/2cXjbb0*.

information assurance, data management, and operational standards that provide good data governance tools for RFID and other Applications."[93]

Whether a PIA meets the letter of the law and no more, or if it goes far beyond it, incorporating broad ethical concerns and sensitivities for users, a PIA can help organizations get a better sense of the personal data it handles, the associated risks, and how to manage issues before a disaster strikes.

Identity management

The field of identity management (IDM) is concerned with authentication, attributes, and credentials—methods of identification and access. Not only is this domain important for engineering-level objectives about how users and devices identify and connect to one another, but it also provides a framework and language for privacy design considerations.

For many years, identity practices have been converging around what is called *federated identity*, where people use a single sign-on (SSO) to access multiple, disparate resources. Examples include Facebook logins to access news sites, university logins to access academic publishers, Gmail logins to access other Google functions, and national IDs to log in to government websites. Using SSO means there's always someone looking over your shoulder online—unless a system is designed specifically not to. This and other challenges inherent to IDM systems have yielded several strategies to strengthen privacy protection. Three in particular are valuable for the IoT:[94]

Unlinkability

> This is the intentional separation of data events and their sources, breaking the "links" between users and where they go online. In the IDM world, this means designing systems so that one website does not know you are using another website even though you are using the same login on both. In the IoT context, the analogy would be your bathroom scale does not need to know where you drive, or your fitness band does not need to

93 See first reference in footnote 92.

94 Rost, M. and Bock, K. 2011. Privacy by Design and the New Protection Goals. Available at *http://bit.ly/2cFN4gf*.

know which websites you visit. There are certainly advantages to commingling data from different contexts, and many people will feel comfortable with it happening automatically. The point is for there to be options for those who do not. Ergo, there is a design imperative for IoT devices to not share cross-contextual data without explicit user consent, and for defaults to be set to opt-in to sharing rather than to opt-out.

Unobservability
: Identity systems can be built to be blind to the activities that occur within them. People can use credentials and log in to various websites, and the "plumbing" of the system is unaware of what goes on. We can apply this same design principle to the various intermediaries, transport subsystems, and middle layers that make up the IoT ecosystem's connective tissue of communications.

Intervenability
: This is exactly what it sounds like—the ability for users to intervene with regard to the collection, storage, and use of their personal data. Intervenability is a broad design and customer relationship goal; it aims to give users more knowledge and control over data that's already been collected about them, what raw data is stored, and what inferences a company has made. The ability to delete and withdraw consent, to determine who gets to see personal data and how it's used, and to correct erroneous information all support transparency, user control and rights, and autonomy.

Standards

A standard is an agreed-upon method or process. Standards create uniformity—a common reference for engineers, programmers, and businesses to rely upon so that products made by different companies can interoperate with one another. Standards reduce costs and complexity because companies seeking to enter a new market don't need to invent everything from scratch. Standards abound in the technical world: DVD, USB, electrical outlets, the screw threads on a lightbulb, WiFi, TCP/IP, Ethernet, RFID, the C programming language, Bluetooth... **information age technologies are typified by standardization**. Standards can originate with noncommercial or public organizations, such as the Institute of Electrical and Electronic Engineers (IEEE), or with commercial organizations and

groups, such as the AllSeen Alliance, "a cross-industry consortium dedicated to enabling the interoperability of billions of devices, services, and apps that comprise the Internet of Things."[95]

Successful standards wield much influence because they can specify what devices can and cannot do. As such, they are a powerful intervention point for privacy in a technical sense. There is a clear need for more research into which and how IoT standards can affect the privacy landscape. Given the complexity of building respectful, secure, privacy-preserving systems, IoT-specific and more general standards play a critical role in the evolution of connected devices. See the Further Reading section for references to existing and emerging standards.

95 AllSeen Alliance. 2016. Home page. Available at *https://allseenalliance.org/*.

Conclusion

The Internet of Things is a messy idea that's captured the attention of the public, governments, academics, and industry. Whatever it is, however it is defined, the attention it generates is valuable because it encourages reflection on the past and future of privacy protection. For those who wish to see strong privacy values reflected in the technologies infusing the human environment, it's helpful to review what those values are and what methods are available to embed them in products.

Privacy is not merely something to be traded upon, as if the data about us were currency and nothing else. It's an emergent social property, relating to values, culture, power, social standing, dignity, and liberty. This report began from the perspective that people are more than the data they shed and volunteer. "We are citizens, not mere physical masses of data for harvesting," observes socio-legal researcher Julia Powles.[96] Privacy is far more than a consideration of individualistic, personal harms—it is an essential element of a healthy, democratic society. Safeguarding it as technology progresses is both a personal and social interest.

There is plenty of room for people to knowingly divulge personal information in exchange for a service, and for businesses to make compelling cases for a symbiotic relationship with customers. But, when data is gathered invisibly and with weak permissions, or stored without easy ways to delete it, or the uses are poorly explained, or the custodians of personal data are not required to

96 Powles, J. 2015. We are citizens, not mere physical masses of data for harvesting. *The Guardian*. 11 Mar. Available at *http://bit.ly/2cFLw5W*.

handle it in secure ways, **institutional and technical controls become vital to effect privacy protection**. Relying on market forces alone to embed strong privacy practices in the IoT is a flawed approach. The social goals of *fairness*, *transparency*, *protecting the vulnerable*, and *respect* are paramount for this next evolution in technology.

Privacy is not simply a domain governed by extant laws, frameworks, and technology. How we talk about it, feelings of vulnerability, what we think is right—all of these contribute to the conversation society has with itself about privacy values and how they should be preserved. Whatever the current world looks like with regard to privacy, it's not set in stone.

Special Thanks

I'm deeply grateful to my editors and colleagues who've helped me write and refine this report. I'd like to thank in particular Susan Conant, Jeff Bleiel, Lachlan Urquhart, Dr. Anna Lauren Hoffman, Jennifer King, Professor Ian Brown, Professor Martin Elton, Erin Kenneally, Jo Breeze, Elliotte Bowerman, and Alex Deschamp-Sonsino for their time and thoughtful comments.

Further Reading

General Privacy and Data Protection Topics

- Bennett, C. and Raab, C. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Burlington: Ashgate Publishing
- DLA Piper. 2016. Data Protection Laws of the World. Available at *http://bit.ly/2dwDwWx*.
- European Union Agency for Fundamental Rights. 2014. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union. Available at *http://bit.ly/2cQ7MYC*.
- Nissenbaum, H. 2010. *Privacy in Context*. Stanford: Stanford University Press.
- Solove, D. 2008. *Understanding Privacy*. Cambridge: Harvard University Press.
- Waldo, J., Lin H., and Millet, L. 2007. *Engaging Privacy and Information Technology in a Digital Age*. Washington, D.C.: The National Academies Press. Available at *http://www.nap.edu/catalog/11896.html*.
- White House. 2012. Consumer Data Privacy in a Networked World. Available at *http://bit.ly/2dl84vh*.

Internet of Things Privacy Topics

- Ackerman, L. 2013. *Mobile Health and Fitness Applications and Information Privacy*. Available at *http://bit.ly/2dhGc89*.
- Article 29 Working Party. 2014. Opinion 8/2014 on Recent Developments on the Internet of Things. Available at *http://bit.ly/2cXhOZM*.
- Canis, B. and Peterman, D. 2014. "Black Boxes" in Passenger Vehicles: Policy Issues. Congressional Research Service. Available at *https://www.fas.org/sgp/crs/misc/R43651.pdf*.
- De Mooy, M. and Yuen, S. 2016. *Toward Privacy Aware Research and Development in Wearable Health*. Center for Democracy & Technology and FitBit, Inc. Available at *http://bit.ly/2cwESff*.
- Edwards, L. 2016. Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. *European Data Protection Law Review*, 2(1):28-58. Available at *http://ssrn.com/abstract=2711290*.
- Electronic Privacy Information Center. (n.d.). Domestic Unmanned Aerial Vehicles (UAVs) and Drones. Available at *https://epic.org/privacy/drones/*.
- Federal Trade Commission. 2015. *Internet of Things: Privacy & Security in a Connected World*. Available at *http://bit.ly/2dwxDIY*.
- Peppet, S. 2014. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review* 93(1):87-176. Available at *http://bit.ly/2d0mmC7*.
- Pew Research Center. 2014. *The Internet of Things Will Thrive by 2025*. Available at *http://pewrsr.ch/2dlvf8H*.
- Postscapes. (n.d.). IoT Standards and Protocols. Available at *http://bit.ly/2du6wzp*.

About the Author

Dr. Gilad Rosner is a privacy and information policy researcher and the founder of the nonprofit Internet of Things Privacy Forum, a crossroads for industry, regulators, academics, government, and privacy advocates to discuss the privacy challenges of the IoT. The Forum's mission is to produce guidance, analysis, and best practices to enable industry and government to reduce privacy risk and innovate responsibly in the domain of connected devices.

Dr. Rosner's broader work focuses on the IoT, identity management, US & EU privacy and data protection regimes, and online trust. His research has been used by the UK House of Commons Science and Technology Committee report on the Responsible Use of Data and he is a featured expert at O'Reilly and the BBC. Dr. Rosner has a 20-year career in IT, having worked with identity management technology, digital media, automation, and telecommunications.

Dr. Rosner is a member of the UK Cabinet Office Privacy and Consumer Advisory Group, which provides independent analysis and guidance on Government digital initiatives, and also sits on the British Computer Society Identity Assurance Working Group, focused on internet identity governance. He is a Visiting Scholar at the Information School at UC Berkeley, a Visiting Researcher at the Horizon Digital Economy Research Institute, and has consulted on trust issues for the UK government's identity assurance program, Verify.gov. Dr. Rosner is a policy advisor to Wisconsin State Representative Melissa Sargent, and has contributed directly to legislation on law enforcement access to location data, access to digital assets upon death, and the collection of student biometrics.

Dr. Rosner can be contacted at:

- *gilad@iotprivacyforum.org*
- *www.iotprivacyforum.org*
- *@giladrosner*, *@iotprivacyforum*