Dead Reckoning: Where We Stand On Privacy and Security Controls for the Internet of Things

by

Brandon Allan Karpf

B.S., Weapons and Systems Engineering (Honors Program)
United States Naval Academy (2015)

Submitted to the Institute for Data, Systems, and Society
in partial fulfillment of the requirements for the degree of

Master of Science in Technology and Policy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2017

Author . . . .
Institute for Data, Systems, and Society
May 12, 2017

Certified by . . . .
David D. Clark
Senior Research Scientist, CSAIL
Thesis Supervisor

Accepted by . . . .
W.A. Coolidge Professor Munther Dahleh
Director, Institute for Data, Systems, and Society

Dead Reckoning: Where We Stand On Privacy and Security Controls for the Internet of Things

by

Brandon Allan Karpf

Submitted to the Institute for Data, Systems, and Society
on May 12, 2017, in partial fulfillment of the
requirements for the degree of
Master of Science in Technology and Policy

Abstract

This thesis provides an analysis of privacy and security controls for internet-connected data-driven systems, known as the Internet of Things (IoT). The grounding theory is that numerous pre-existing privacy and security control methods – not necessarily crafted for IoT – will bear on the future of IoT privacy and security. This thesis covers fifteen case studies across six different control categories: Individual Choice, Command and Control Regulations, Operational Standards, Technical Standards, Compliance Frameworks, and Federal Authorities.

These case studies reveal major deficiencies in current IoT privacy and security controls. IoT privacy and security controls lack a domain or contextual-use focus. Further, most current controls also fail to specify the risks or harms they intend to resolve. Therefore, the current IoT privacy and security controls induce a significant privacy and security market failure. This market failure is evident in recent IoT privacy and security events such as the Federal Trade Commission's cases against the IoT system developers TRENDnet and D-Link.

I define three necessary paradigm shifts needed to improve IoT privacy and security controls. I also recommend a specific research endeavor to develop domain-, risk-, and harms-centric privacy and security standards. The realization of these paradigm shifts, and the products from this research endeavor, will navigate the IoT ecosystem towards more effective privacy and security control.

Thesis Supervisor: David D. Clark
Title: Senior Research Scientist, CSAIL

Acknowledgments[1]

David D. Clark thank you for giving me this extraordinary experience. Your mentorship and flexibility made this opportunity one of immense growth. Thank you for allowing me to discover the balance that works best. Your support and feedback was invaluable – I could not have survived without it. I've never know a man to be busier than you, and yet you still made the time to read through the entire density of this work again and again. May your blueberries be forever fresh.

Daniel J. Weitzner thank you for giving me this fantastic opportunity and accepting me during "year zero" of the Internet Policy Research Initiative. Your feedback on my thesis pushed my work to the next level. Thank you for sharing your experiences, wisdom, and knowledge. I follow the road ahead prepared to think strategically thanks to your guidance.

Steve Bauer, **Shirley Hung**, and **Susan Perez** thank you for your continued help navigating this graduate school experience. Sweets flowed like ale, technical knowledge extended as deep as the sea, and life advice proved as reliable as the trade winds.

Bill Lehr, **Karen Sollins**, and **Arthur Berger** thank you for your support, wisdom, and friendship these past two years.

Nathaniel Fruchter and **Ilaria Liccardi** thank you for your hard work on our IoT device/consumer sentiment study that I have included in full as Appendix A.

Office 32-G806: Zane Markel, Cecilia Testart Pacheco, Samuel DeLaughter, Nathaniel Fruchter, Georgios Smaragdakis, and yes, even James Loving, thanks for the laughs, the good company, and the challenging discussions.

Frank Field thank you for your friendship and pilotage through this crazy world that is technology *and* policy. Everyone else knows how much I want to be you (even down to the bracelets). I hope you know it as well.

Barbara DeLaBarre and **Ed Ballo** thank you both for being the most incredible, lively, and consistently happy people I know. You are the soul of TPP and none of us would even come close to succeeding without you. TPPers should express this more often: we are forever indebted to you.

TPP and all of my fascinating classmates who do some of the most varied and interesting work at MIT. Thank you for teaching me so much.

[1] My work was supported by the William and Flora Hewlett Foundation grant.

Disclaimer: Brandon Karpf is an active duty Officer in the U.S. Navy. Any views, opinions, assumptions, or conclusions expressed in this work are those of the author and do not reflect the official policy or position of any agency of the U.S. government.

My surrogate family, who gave me a home whenever I felt a bit too normal: Luke, Alex, and Marilyn Koblan, and Bart Johnston and Annaliesa Routh, thank you for always being there when I needed you the most.

Most importantly, **my actual family**: Drs. Gary and Robin Karpf, and Sarah and Evan Kasowitz who put up with my ever-distracted mind. You, who encourage me to "keep your head when all about you are losing theirs and blaming it on you" and to "fill the unforgiving minute with sixty seconds' worth of distance run"; who taught me that "the credit belongs to the man who is actually in the arena, whose face is marred by dust and sweat and blood; who strives valiantly; who errs, who comes short again and again"; You are my rock. Everything I do, I do to make you proud. Your support and pride means more to me than I can express. Thank you, and I love you all.

Fair winds and following seas.

The Road goes ever on and on
Down from the door where it began.
Now far ahead the Road has gone,
And I must follow, if I can,
Pursuing it with eager feet,
Until it joins some larger way
Where many paths and errands meet.
And whither then? I cannot say.

⚓

The Road goes ever on and on
Out from the door where it began.
Now far ahead the Road has gone,
Let others follow it who can!
Let them a journey new begin,
But I at last with weary feet
Will turn towards the lighted inn,
My evening-rest and sleep to meet.

– J.R.R. Tolkien

Contents

List of Figures

Nothing to see here. Move along.

List of Tables

Nothing to see here. Move along.

Chapter 1

Introduction

1.1 Thesis Overview

This thesis provides an analysis of current privacy and security controls for the Internet of Things (IoT). The primary goal of this analysis is to evaluate where current controls fail and to draw a course correction to improve the privacy and security of IoT systems and services. First, I present an analysis framework for privacy and security controls based on three factors: contextual use domains, stakeholders, and key privacy and security challenges. I then conduct fifteen case studies that describe the current IoT privacy and security controls. These case studies reveal control faults that lead to a market failure in IoT privacy and security. Finally, I present key findings in respect to the current state of IoT privacy and security controls, and outline a navigable approach to establish more effective future control.

The method of control (MoC) analysis framework covers contextual use domains, IoT stakeholders, and the key IoT privacy and security challenges that MoCs must address. This framework provides a nuanced perspective on MoC applicability and effectiveness. While most analyses of the IoT ecosystem define only two domains – consumer IoT and industrial IoT – privacy and security risks and harms are specific to contextual technology use. The framework defines fifteen contextual IoT use domains to provide a more nuanced perspective. Further, IoT privacy and security MoCs are only effective insofar as they impact specific stakeholders. The description and application of IoT privacy and security risks, harms, and controls must be salient to those specific stakeholders. The framework outlines the IoT stakeholder categories and provide examples for each. Finally, the IoT ecosystem has a number of specific privacy and security challenges that define the major risks and harms that must be controlled. The framework describes the sixteen most significant challenges.

The MoC case studies involve fifteen different MoCs across six distinct MoC categories. While these case studies are not exhaustive, they are extensive and describe the current approach to IoT privacy and security control. They reveal that the most tangible current control derives from the Federal Trade Commission's regulatory authority, as well as the application of the Notice and Choice framework. Both lack significant effectiveness. Further, the case studies allow conclusions to be drawn about the current state of IoT privacy and security controls, and where academic researchers and policymakers can focus their efforts to improve such controls.

This thesis draws a number of conclusions regarding the most significant MoC faults. The faults can be distilled into two common veins related to specificity. First, current IoT privacy and security controls lack domain focus. Domain focus is the narrow scope in which a MoC applies. It relates to the IoT system *context.* Second, current IoT privacy and security controls lack a risk and harms focus. Risk and harms focus is the specific IoT privacy and security implication that a MoC targets. It relates to the *use* of IoT systems. These faults demonstrate the current crisis of control that plagues the IoT ecosystem. This crisis of control, framed in this thesis as a market failure, must be addressed if IoT stakeholders wish to internalize effective privacy and security as driving tenets.[1]

I recommend three major paradigm shifts to address this market failure. First, the Federal Trade Commission must acknowledge that its current adjudicative approach that controls *business practices* without addressing more fundamental *business models* has failed and will continue to fail to improve IoT privacy and security. Second, the

[1] The scope of this thesis does not include a discussion of the primary factors present in a "crisis of control." Instead, this thesis frames the "crisis of control" theory in the tangible concept of a market failure. For more on the theory of control crises, I recommend James Beniger's seminal work "The Control Revolution: Technological and Economic Origins of the Information Society" as required reading for any person interested in the effective control of socio-technical systems.

Notice and Choice framework must undergo a thorough redesign or be discarded as the primary IoT privacy and security MoC. The structure of the current Notice and Choice framework is at odds with the realities of the IoT ecosystem. This conclusion is derived from a detailed analysis in Chapter 3 as well as the results of an IoT consumer study included in Appendix A. This study, in which we evaluated consumer discourse regarding IoT devices, shows that IoT device privacy and security is rarely a primary discussion topic even when those devices have significant publicized privacy or security risks. Therefore, personal choice control mechanisms like Notice and Choice should not be relied upon to improve IoT privacy and security. Third, new IoT privacy and security standards must be developed that embody the tenets of specificity and provide baseline privacy and security controls. The MoC case studies demonstrate that the extensive market for IoT operational and technical standards fails to control the fundamental IoT privacy and security challenges due to lack of specificity. The realization of these paradigm shifts will navigate the IoT ecosystem towards more effective privacy and security control.

1.1.1 Intent and Contributions

The intent of this thesis is to better understand specific MoCs available for improving IoT privacy and security. The foundational theory is that there are numerous pre-existing privacy and security control methods – not necessarily crafted for IoT – that will bear on IoT. The MoCs discussed in this work are broadly diverse in an attempt to analyze different strategies that impact IoT privacy and security. The MoC categories analyzed in this thesis are:

MoC 1 – Individual Choice (Chapter 3)

MoC 2 – Command and Control Regulations (Chapter 4)

MoC 3 – Operational Standards (Chapter 5)

MoC 4 – Technical Standards (Chapter 6)

MoC 5 – Compliance Frameworks (Chapter 7)

MoC 6 – Federal Authorities (Chapter 8)

Each MoC case study includes background information, an analysis of its effectiveness, as well as a discussion of which IoT domains the MoC addresses, to which IoT stakeholders the MoC grants power, and which fundamental IoT privacy and security challenges the MoC improves or exacerbates. In this context, MoC effectiveness is determined by considering its success and usefulness in relation to the domains it addresses, the stakeholders it provides with power, and the privacy and security challenges it affects.

This thesis provides the following contributions:

1. A MoC analysis framework. The same framework can also be used to categorize and analyze IoT systems. The framework involves three sections:

   Chapter 2.1 – An IoT domain framework for use in discussing IoT systems, services, risks, and harms across various use-contexts.

   Chapter 2.2 – An IoT privacy and security stakeholder system.

   Chapter 2.3 – A list of the most influential and fundamental challenges that MoCs must address in order to improve IoT privacy and security.

2. A case study into each MoC category's effectiveness in addressing IoT privacy and security: (Chapters 3–8)

   1. The Notice and Choice Framework (Chapter 3)
   2. The Health Insurance Portability and Accountability Act (Chapter 4)
   3. ISO/IEC 27k Series Standards (Chapter 5.2)
   4. ITU-T Global Standards Initiative (Chapter 5.3)
   5. The 3rd Generation Partnership Project (Chapter 6.2)
   6. oneM2M (Chapter 6.3)
   7. Information Technology Infrastructure Library (Chapter 7.2)
   8. Control Objectives for Information and Related Technologies (Chapter 7.3)
   9. Capability Maturity Model Integration (Chapter 7.4)
   10. The Open Group Architecture Framework (Chapter 7.5)
   11. The Federal Trade Commission (Chapter 8.2)
   12. The Federal Communications Commission (Chapter 8.3)
   13. The U.S. Legislative Branch (Chapter 8.4)
   14. The U.S. Executive Branch (Chapter 8.5)
   15. The Department of Homeland Security (Chapter 8.6)

3. A tangible example of where current IoT privacy and security MoCs have failed, a discussion of the paradigm shifts required to improve IoT privacy and security, as well as immediate steps academic researchers can take to best improve IoT privacy and security controls. (Chapter 9)

1.1.2 How To Approach This Work

It is my hope that this thesis evaluates the current MoCs that affect IoT privacy and security, how they affect IoT privacy and security, and what immediate actions can be taken to improve them. This work applies to the following audiences:

- Academic Researchers
- Privacy and Security Advocates
- Standards Developing Organizations
- Federal Policymakers

The thesis is split into three parts. Part I (Chapter 2) covers the MoC effectiveness framework and is split into three sections: IoT operational domains, IoT stakeholders, and key IoT privacy and security challenges. All audiences should read Part I in its entirety. It provides details on the current IoT ecosystem that are paramount to the situational awareness of interested audiences. Further, it explains the framework for evaluating MoCs in the context of IoT privacy and security.

Part II (Chapters 3–8) covers the fifteen MoC case studies addressed by this thesis and outlined in Subsection 1.1.1. All audience members should read Chapter 3, *Individual Choice*. This chapter represents the current de facto standard for IoT privacy and security control. Further, it reveals the significant deficiencies in how the IoT ecosystem controls privacy and security. Individual audience members should also read the chapters in Part II that relate closest to their domain. For example, Standards Developing Organizations should read Chapters 5 and 6, whereas academic researchers can gain the most from reading the introduction and conclusion of each chapter in Part II.

Part III (Chapter 9) covers the conclusions of this thesis as well as a discussion and recommendation for immediate next steps for improving IoT privacy and security. It includes two tangible examples that demonstrate that the current MoCs have led, and will continue to lead, to lax privacy and security controls in the actual IoT ecosystem. Further, it explains three paradigm shifts required to develop more effective IoT privacy and security controls. All audiences should read Part III.

1.2 Background and Motivation

Three additional topics require elaboration as they are relevant and fundamental to the discussions throughout this work. In the following section, I present IoT definitions, discuss the more technical concept of an IoT reference architecture, and examine the meaning of IoT privacy and security. The purpose of this section is to provide the necessary background and motivation needed to better understand the scope of my research within the IoT ecosystem.

1.2.1 IoT Definition

A brief search for "IoT definition" reveals that no universal definition exists. Put simply, this is because IoT is a paradigm and not a tangible thing. Intangible concepts rarely have single definitions. Further, IoT is a concept that is adaptable in operations and technology to the domain in which it is applied.[2]

IoT definitions reveal the definer's inherent bias. For example, the NIST definition refers to IoT as a cyber physical system (CPS)[3], revealing NIST's institutional focus on industrial systems.[156] The FTC's definition refers to IoT as devices "sold to or used by consumers," revealing the FTC's bias towards their consumer protection responsibilities.[75] The definition offered by the International Telecommunications Union, an operational and technical standards developing organization, is "a global infrastructure for the information society" – as overbroad and interpretive as the organization's mandate.[120] The Department of Homeland Security's definition reveals their concern with critical infrastructure by referring to IoT as a "connection of

[2] The domain-specific nature of IoT is discussed in more detail in Chapter 2.1.

[3] CPS is a term most often used in the industrial systems context. For example, see the National Science Foundation's program solicitation 17-529.[68]

systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks."[49]

The most illustrative of IoT definitions is offered by a Greek research scientist as "a world where computers would relieve humans of the Sisyphean burden of data entry by automatically recording, storing and processing in a proper manner all the relevant information about the things involved in human activities."[80]

What these definitions have in common is that IoT refers to the system of interactions between computers, sensors, actuators, objects, and society. IoT is a system in which the control signal is raw data and the result is any function imaginable. Sensors collect data from objects and people. Computers process that data to add purpose and meaning, which derives information. Actuators act on information to provide a function. People use functions, often in a network of other functions, to provide a service. Therefore, IoT is a societal system. The Internet Society's definition is most relevant and comprehensive: "the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers."[62] This definition leaves little to interpretation. IoT is the convergence of the physical and virtual realms. Further, it defines the boundaries of the IoT system in a way that approaches the definition of a biological ecosystem.[4,5] For the rest of this work, I refer to this as the *IoT ecosystem*.

In recognition of my own bias, I acknowledge that I believe the IoT ecosystem to be a widely pervasive phenomenon that is not limited by domain, function, capability, or pre-existing technologies. It has evolved almost as a natural derivative of the digital

[4] *"When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do his will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."* – Nikola Tesla (Interview by John B. Kennedy, 1926)[125]

[5] *"In the next century, planet earth will don an electronic skin. It will use the Internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies — even our dreams."* – Neil Gross (In *Business Week*, 1999)[84]

economy. I am perhaps a bit radical in comparing it to a biological ecosystem. I define an IoT system as any system that 1) uses data as a control signal, 2) processes that data to create information, 3) uses that information to provide a function, and 4) networks with other systems to develop a service. Good examples of widely used IoT systems are automatic teller machines, electronic toll collection systems, closed-circuit television video surveillance, any new motor vehicle, and the Nest home thermostat. Under this definition and for the remainder of this work IoT, Machine-to-Machine (M2M), and CPS are considered synonymous systems.

> **IoT Definition**: Any system that uses data as a control signal, processes that data to create information, uses that information to provide a function, and networks with other systems to offer a service.

This definition allows one to identify the types of technologies, use-contexts, stakeholders, and privacy and security challenges relevant to the IoT ecosystem.

1.2.2 IoT Reference Architecture

Now that we have an established definition for the IoT ecosystem, it is important to describe the structure of an IoT system. Such a high-level representation of a technical system is called a reference architecture.

Reference architectures are important because they translate a general definition into an operational definition. All MoCs rely to some degree on an IoT reference architecture. A reference architecture allows a MoC to identify the particular part or stage of an IoT system it intends to control. Further, effective MoCs use reference architectures to identify the parts of an IoT system that must *implement* controls. The idea of an IoT reference architecture, and whether or not a MoC uses one to describe its impact on an IoT system, is a signal for a MoC's effectiveness.

That being said, there is no universal standard IoT reference architecture. Many organizations, international SDOs and developers and manufacturers in particular, have released a version of their own IoT reference architecture. For example, Symantec – an international cybersecurity firm – designed and published an IoT reference architecture for security in 2015.[207] ISO/IEC – an international technology SDO – designed and published an IoT reference architecture for future technology requirements based on a host of pre-existing reference architectures.[113] Stakeholders design and publish reference architectures that meet their specific needs.

There is one IoT reference architecture that stands above the rest. The International Telecommunications Union (ITU) released their IoT reference architecture in 2012 as part of an IoT standards series. The ITU reference architecture is unique in the fact that it explains the physical *and* virtual nodes of the IoT ecosystem, and the connections between them. It represents the IoT ecosystem as dependent on the interactions between physical things (the subjects that emit data), networked devices (the systems that capture data), and application platforms (the functions that create value from data). Further, it is simple enough to offer a generic model that fits IoT systems across domains and use-contexts.[6]

ITU's reference architecture operationalizes the IoT definition derived in Subsection 1.2.1. It takes a layered-communications approach that reveals *why* and *how* data is used in an IoT system from both a technical and a policy perspective. This thesis considers the business policy and technical requirements of privacy and security MoCs for IoT systems. As such, this operational reference architecture serves as an important foundation to understand the functional IoT ecosystem.

Though I will not describe the ITU reference architecture in extenso, I will outline the four fundamental layers of the IoT ecosystem as defined by ITU. The layer definitions are important because it is these layers that MoCs must control in order to develop IoT privacy and security. The layers are **Application**, **Service**, **Network**, and **Device**. Figure 1-1 represents this ITU layer model as an IoT system hierarchy.

The Application Layer is the applications that interact with IoT devices and provide interaction methods between users and IoT systems. It is the most observable layer of the IoT ecosystem because IoT users interact directly with this layer when using an IoT system.[7]

[6] For a more detailed explanation of the ITU reference architecture, please see [201]. For the ITU recommendation that defines the reference architecture, please see [119].

[7] It is a misconception that the **device layer** is the most observable layer in the IoT ecosystem.

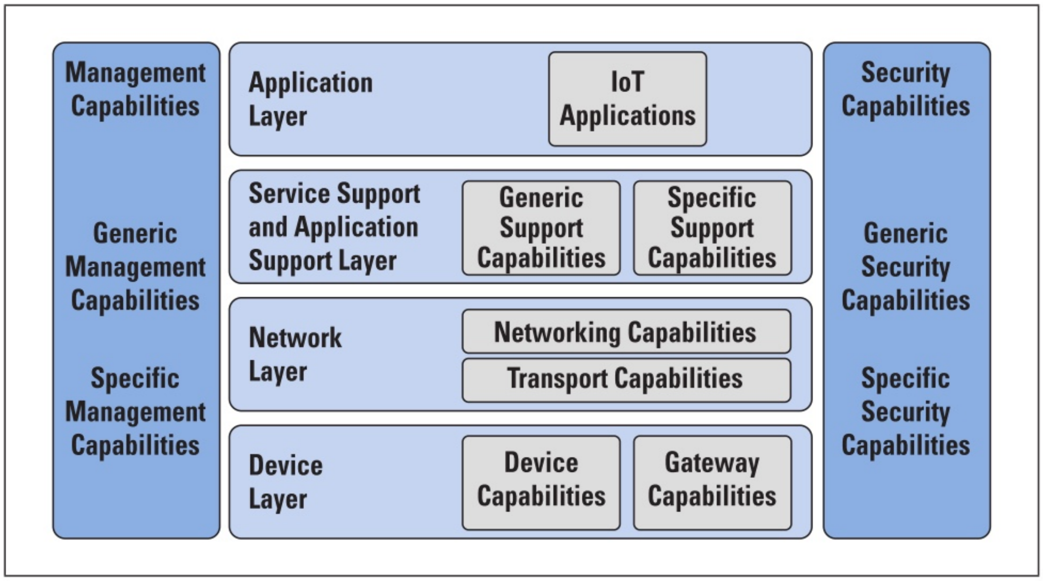

Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application Layer
IoT Applications
Service Support and Application Support Layer
Generic Support Capabilities
Specific Support Capabilities
Network Layer
Networking Capabilities
Transport Capabilities
Device Layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Security Capabilities
Specific Security Capabilities

Figure 1-1: The ITU reference architecture for IoT systems.[8]

The Service Layer provides capabilities used by IoT applications and devices in such a way as to derive value. Examples include data processing, data storage, and information security management systems.

The Network Layer performs two functions: networking capabilities and transport capabilities. Networking capabilities create connections between IoT systems and devices. This function is useful in the context of sensor nets in domains such as transportation, manufacturing, and infrastructure. Transport capabilities create the communication networks for data from IoT applications, services, and devices, as well as for IoT-related control and management information.

The Device Layer is the physical devices that constitute an IoT system or service.

1.2.3 IoT Privacy and Security

Finally, it is important to discuss the scope of IoT privacy and security in this thesis. In the following section, I discuss the meaning of privacy and security and how these concepts relate to the IoT ecosystem. The purpose of this section is to provide an

While device ubiquity is projected to be massive, devices for many IoT applications are typically *not* observable. For example, consider a smart parking meter use case. In this scenario, the user interacts with the parking application, not the smart meter device.

[8] Found in [201].

understanding of what IoT privacy and security actually means, as well as provide the motivation for why IoT privacy and security is a field of study that matters.

There is no universal definition of IoT privacy or security. In general terms the concept of *achieving* some degree of IoT privacy and security is the act of minimizing risk and maximizing value.[9]

Privacy Definition

There are two popular archetypal definitions of privacy.[10] The first comes from the article "The Right to Privacy" by Samuel Warren and Louis Brandeis published in 1890. In it, the authors define the extent to which an individual has a right to privacy, and what that right actually means. Most clearly, they define privacy as the extent to which a person's "thoughts, sentiments, and emotions shall be communicated to others."[213] In a similar vein, the second popular definition comes from Alan Westin's 1967 book, "Privacy and Freedom." Westin expands Warren and Brandeis' privacy definition beyond the right of individuals as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[219] Both of these definitions have a common theme from which we can derive a general working definition of privacy: the extent to which information is collected, shared, and used.

Clear from both definitions is the implication that privacy is not absolute – it is a spectrum. It is also clear that privacy requires a choice, or threshold, in regards to the extent and type of information shared or communicated. These two facts lead to a third implication, that acceptable privacy is a *relative* construct. In other words, one person or group's definition of acceptable privacy is different than another person or group's definition.

[9] By this definition, achievable privacy and security controls require a definition of risk and value for the specific "thing." Further, risk and value definitions require granularity in terms of contextual- and use-specific considerations. This process forms the logic for the framework described in Chapter 2 as well as the key conclusions drawn from this thesis and described in Chapter 9.

[10] For a lengthy discussion on privacy definitions in the age of digital technology, please see [155]. For a comprehensive discussion into the legal and policy history of privacy in the U.S., please see the second appendix in [157].

In regards to the IoT ecosystem, this implication must be expanded to consider contextual issues. No only are individual, group, or institutional definitions of privacy different, but those definitions also change with shifting domains and use-contexts.

> **IoT Privacy** is the extent to which information is collected, shared, or used in a specific context.

Security Definition

The definition of IoT security is a bit more concrete than that of privacy. For the purposes of this thesis, I derive the IoT security definition from a 2016 article by Vinton Cerf, et al. titled, "IoT Safety and Security as Shared Responsibility." In this article, the authors define both digital safety and online security.

> "**Digital Safety** is the protection of the user in his or her environment, with technical mechanisms and policies that protect the users from being harmed by improper operation of the device.
> **Online Security** is the protection of the physical network, operating systems and content from exposure, modification or functional damage, utilizing a combination of software and hardware mechanisms."[34]

I modify these definitions for my own definition of IoT security. First, I combine both **digital safety** and **online security** as the same concept. IoT security is about the protection of the user, network, systems, *and* content. Second, I remove the *improper operation* qualifier. Improper operation alludes to some degree of nefarious intent. IoT security harms can derive from proper use of poorly designed systems. Third, I modify the **online security** subjects in order to align the definition with the IoT reference architecture layers described in Subsection 1.2.2.

> **IoT Security** is the protection of the user, devices, network, services, applications, and content from context-specific risk and harms through the use of technical mechanisms and policies.

Part I

MoC Analysis Methodology

Nothing to see here. Move along.

Chapter 2

MoC Analysis Framework

The MoC analysis framework outlined in this chapter is a waterfall-style guide to IoT systems, technologies, and services. It is to be used in sequence starting with a contextual domain analysis. Once the domain analysis is complete, the user should proceed to a stakeholder analysis, and then to the IoT privacy and security challenges analysis. Therefore, the specific domain or domains in question influence the stakeholder analysis, and the domains and stakeholder analysis influence the impact on privacy and security challenges. For example, stakeholders such as service providers and users in the IoT government domain are different than the service providers and users in the IoT finance and IoT domestic domains. Further, because the stakeholders and domain considerations are different across domains, the impact and implications of key IoT privacy and security challenges are also different. The intent of this framework is to provide a more granular analysis of the IoT ecosystem than what is currently available, hence why I use the framework as a common analysis structure for IoT privacy and security MoCs.[1]

[1] It is also important to note that this framework is as applicable to "things" as it is to privacy and security MoCs. Though not demonstrated in this thesis, it can be used to analyze an IoT technology or service in order to label, categorize, or further understand the specific privacy and security considerations necessary for the specific technology or service.

2.1 IoT Contextual Domains

The current analysis approach for the IoT ecosystem is to split the ecosystem into two domains: consumer IoT and industrial IoT.[17] This approach is evident in publications such as a 2015 report by DHL and Cisco titled "Internet of Things in Logistics" that combines the commerce, manufacturing, retail, transportation, healthcare, and infrastructure domains all under the concept *industrial IoT*.[141] This trend is also evident through technical standardization groups such as oneM2M (Chapter 6.3) that split standardization activities between consumer IoT technologies and industrial IoT technologies.[169] While recent work acknowledges the importance of such a split – that technology uses, privacy and security implications, resources to address challenges, and incentive structures are different between consumer and industrial applications[134] – the bilateral domain distinction does not provide enough granularity. For example, the data privacy considerations within the IoT finance domain are far more sensitive than the data privacy considerations within the IoT manufacturing domain. Similarly, the system security implications within the IoT infrastructure domain are far more serious than the system security implications within the IoT retail domain. With the current approach, all four of these domains fall within the industrial IoT sector.[2]

Instead of the standard approach, I present a more granular domain perspective based on the contextual uses of IoT technologies. While the same technology might fall under multiple domains, the *use* of that technology is a significant factor in determining its privacy and security risks and harms.[56] This method was motivated by the *contextual integrity* framework to information privacy designed by Helen Nissenbaum in her seminal work, "Privacy in Context: Technology, Policy, and the Integrity of Social Life."[155]

Below, I have defined the fifteen IoT operational domains with use cases for each. I derived these fifteen domains from an extensive IoT literature review during which I tracked the various case studies present in IoT literature and categorized them into

[2] Another similar approach is to split the IoT ecosystem into IoT private sector domains and IoT public sector domains. This approach faces similar granularity faults.

contextual IoT domains. For similar works on IoT contextual domains that validate my results, please see [201] and [116].

Healthcare

IoT systems that rely on personal healthcare data, provide services for care or research, or constitute the infrastructure of a healthcare provider. Examples include automated diagnoses, prescription tracking and management, automated medical records systems, medical implants, drug discovery and diagnostics, surgical equipment, and automated hospitals or treatment facilities.

Telecommunications[3]

IoT systems that incorporate or provide network management, communication, or cloud infrastructure services. Examples include information technology and data centers, mobile carrier systems, servers, routers, switches, private networks, network device tracking, and network predictive analytics.

Manufacturing/Trade

IoT systems that provide industrial manufacturing or commerce services (to include mining systems), or are used in the manufacturing and trade context. These systems might rely on enterprise or proprietary information. Examples include inventory management, equipment monitoring and tracking, equipment maintenance, process and efficiency analysis, transaction tracking, and order fulfillment.

Finance

IoT systems that rely on financial data (personal or otherwise) or provide services for financial infrastructure. Examples include point-of-sale terminals, automatic teller

[3] In the current ecosystem, telecommunication technologies *facilitate* or *augment* IoT technologies, and are not considered IoT technologies themselves. However, it is conceivable that future IoT use-contexts will include devices and services that create local mesh networks or other traditional telecommunications services.

machines, desktop/home banking, automatic investment allocation and tracking, loan fulfillment and financial health analysis.

Insurance[4]

IoT systems that rely on data for the purpose of insurance policies or claims, or provide services for the insurance industry infrastructure. Examples include individually tailored insurance plans based on IoT data analysis, casualty tracking, and subject monitoring (objects, persons, actions) to determine insurance coverage.

Agriculture

IoT systems that rely on agricultural data or provide a service for agricultural use. Examples include produce quality management, livestock quality management, environmental monitoring and engineering, equipment monitoring and repair, automated harvesting, automatic ordering, automatic fulfillment, and automatic billing.

Transportation

IoT systems incorporated into the transportation infrastructure or that provide services for the transportation infrastructure. Examples include smart transportation systems and autonomous vehicles, adaptable traffic infrastructure and routing, infrastructure quality monitoring and automated repairs, roadside safety operations, automated toll systems, automated ticketing systems, and smart parking services.

Domestic

IoT systems that rely on data from within a private residence or that provide a service within a private residence. Examples include home automation and efficiency,

[4] Current IoT insurance use-contexts rely on IoT technologies from domains such as transportation and healthcare. However, IoT insurance is still a separate category because those technologies and the resulting data from those IoT services are *used* for insurance purposes. This domain framework is one that highlights a technology's contextual use as the key factor in determining privacy and security risks and harms.

smart thermostats, home security, home routers, object tracking and monitoring, and personal assistant technologies.

Workplace

IoT systems that rely on data from within a workplace or that provide a service within a workplace. Examples include object tracking, person and activity tracking, quality of life and environmental monitoring, workplace automation and efficiency, smart thermostats, workplace routers and network infrastructure, and security systems.

Education

IoT systems that rely on data from within an education center or that provide a service within an education center. Examples include security and identity systems, student data tracking and real-time activity analysis, enhanced learning, education center automation and efficiency, and education center routers and network infrastructure.

Infrastructure

IoT systems that rely on data from public utilities and infrastructure or that provide a service to public utilities and infrastructure. Examples include water quality and service monitoring, leak detection and repair, electricity metering, coordination between redundant/ adaptable energy systems, electrical load balancing, smart-grid technologies, pipeline management, resource security, and infrastructure repair.

Entertainment

IoT systems that rely on data from entertainment services or that provide an entertainment or leisure service. Examples include enhanced reality for gaming and sports, enhanced reality tourism, language systems, targeted advertising, ticketing systems, and resource management.

Public Safety/ Defense

IoT systems that rely on data from the defense industry, that are integrated into public safety infrastructure, or provide a service for public safety or defense applications. Examples include border defense and monitoring, smart surveillance systems with object and action detection and tracking, drone control, and disaster relief systems.

Retail/ Hospitality

IoT systems that rely on retail or hospitality data or that provide a service for retail or hospitality infrastructure. Examples include inventory management and tracking, facility management, accessibility and language systems, advertising systems, automatic ordering, automatic fulfillment, automatic billing, and resource management.

Government

IoT systems that rely on government data, that are integrated into government infrastructure, or that provide a service for public sector government uses. Examples include compliance monitoring and auditing systems, environmental monitoring and analysis, data distribution and communication systems, routers and network infrastructure, security systems, and facility management.

2.2 IoT Stakeholders

There are nine IoT stakeholder categories. It is important to acknowledge that the stakeholders within these categories change depending on the IoT domain. For example, the service providers and consumers in the IoT domestic domain are different than the service providers and consumers in the IoT defense domain. The fifteen IoT domains have fifteen different stakeholder systems. Further, individual IoT systems within a single domain might have different stakeholder systems. Therefore, I only provide the nine stakeholder categories with limited generalized examples.[5]

[5] For detailed explanations and examples on how to conduct a formal stakeholder analysis, please see [211] and [212].

Network or Service Providers

Examples: Amazon Web Services; AT&T

Developers or Manufacturers

Examples: Samsung; Qualcomm; Foscam; Amazon; Google

Data Brokers

Examples: Acxiom; Experian

Privacy or Security Advocates

Examples: The Center for Democracy & Technology; Internet Society

Regulatory Authorities

Examples: Federal Trade Commission; Department of Transportation

Standards Developing Organizations

Examples: International Organization for Standardization; oneM2M

Academia or Research Labs

Examples: Internet Policy Research Initiative; UNH InterOperability Laboratory

Testing or Certification Vendors

Examples: Cyber Independent Testing Lab; FIT/ IoT-Lab

Consumers

Examples: You; City of Chicago [24]; NPower [53]

2.3 IoT Privacy and Security Challenges

Through my research and literature review, I have identified sixteen key challenges that impact IoT privacy and security.[6] While not exhaustive, this list does represent the most significant challenges that degrade IoT privacy and security today. Therefore, effective MoCs must address these challenges in order to provide salient controls to IoT privacy and security.

Information Asymmetry

Current IoT systems are not conducive to clear communication between stakeholders, and users often have incomplete information about data collection and use. For example, many IoT devices lack an interface through which to communicate data use or security policies. Further, even when communicated, those data policies tend to be unclear and incomplete.

Solution Costs

The resource costs to implement privacy and security solutions can be prohibitive depending on the context. These costs include time, money, as well as functionality and usability tradeoffs.

Standards Saturation

A massive supply market for operational and technical standards leads to complexity, uncertainty, and inefficiency, as well as the adoption of suboptimal standards that are not specific for an IoT domain or use-context. For example, there exists more than 400 operational and technical standards that apply to IoT technologies. Few of these standards have been evaluated for completeness or effectiveness. Instead, the standards market relies on network effects where the biggest names with the most

[6] There are five primary sources that conduct analyses of the IoT ecosystem in order to identify major privacy and security challenges.[21][74][120][200][171] I derived many of these sixteen key challenges from those sources. Other relevant sources for the key IoT privacy and security challenges include [10], [44], [134], [150], [196], [217], and [218].

followers continue to propagate.

Regulation Uncertainty

Without IoT-specific regulations or legal rulings, it is unclear how current existing regulations impact IoT technologies.

Data Aggregation

Aggregating data from IoT technologies and services can lead to harmful inferences. Further, perfect anonymization is improbable due to the insights and collisions that result from aggregated datasets.

Business Models

Current IoT business models rely on broad permissions to use and retain data to support innovation and success, often going beyond the scope and context of the original service or technology.

Economic Incentives

The economic incentive for increased data privacy and system security are often limited to service providers, manufacturers, and developers, and not to the users or other stakeholders. Service providers, manufacturers, and developers often have competing incentives that do not necessarily support increased privacy and security. This fact leads to misaligned incentives within the IoT privacy and security sphere.

Information Scope

The information needed for various stakeholders to make a privacy or security enhancing choice can be extensive and prohibitive, especially in use-contexts that require rapid choices or provide fleeting momentary services.

Psychological Biases

Users often desire functionality, usability, and convenience over increased privacy or security, even when functionality and convenience come at a direct cost to privacy or security. This challenge compounds the issue of economic incentives.

Accountability

With minimal legal precedent, regulatory rules, or insurance standards, many domains have unclear accountability procedures for data. Further, the popular business model that relies on third party service and data sharing compounds this challenge.

Device Ubiquity

IoT market forecasts suggest massive device ubiquity and connectivity across domains. The separation between online and offline information decreases as ubiquity and connectivity increases. This IoT market ubiquity can lead to conflicts with societal norms for online and offline information.

User Knowledge

IoT users have varying technical expertise and perceptions of data risks and harms, therefore limiting the effectiveness of user control methods for privacy and security.

Slow Legislation

Technology changes faster than regulations. Regulations designed without reflexivity or adaptability can stifle innovation or limit growth.

Dynamic Context

IoT technologies can present different privacy or security risks and harms depending on domain and use-context. Further, single IoT services or technologies have the potential to cross domains and use-contexts, presenting a dynamic scenario with constantly shifting privacy or security risks, harms, expectations, and norms.

Device Capabilities

IoT devices for many domains, uses, and services are limited in capability and technologies. Privacy and security solutions must meet the technological constraints of low-power, low-cost, and low-capability systems.

Negative Externalities

In many IoT domains and use-contexts, privacy and security decisions by various stakeholders do not only affect the decision maker. This effect includes the choices made by technology consumers. Due to the nature of IoT systems and data sensors, a user can make a decision that impacts the privacy and security of an unknowing party. Therefore, some IoT domains and contextual uses lead to negative externalities where user decisions can have a larger impact on individuals or stakeholders other than the decision maker.

Part II

MoC Case Studies

Chapter 3

Individual Choice

3.1 Introduction

In the context of IoT privacy and security, the most fascinating and complex MoC is that which relies on individual choice mechanisms. This method relies on personal idiomatic values in the sense that a consumer or group of consumers makes a value-based judgment to use or not use a device or service. It also relies on the convergence of those values with practical and behavioral economics. Therefore, one requires working knowledge of individual and group psychology, market economics, and U.S. culture in order to comprehend the entirety of such a MoC.

These topics are far beyond the scope of this thesis. Instead, I will summarize those topics by stating that this MoC influences, and attempts to improve, the privacy and security challenges *Accountability*, *Economic Incentives*, *Information Asymmetry*, and *Slow Legislation*. It relies on theories of laissez faire market systems in which the market expects consumer choice to influence what technologies and services are available for use and purchase. The common guiding colloquialism is that people "vote with their feet."

In this chapter, I conduct a case study on the most entrenched of such control methods, the notice and choice (NaC) framework. In fact, other individual choice control frameworks within the IoT ecosystem do not exist. Any other individual choice mechanisms is an NaC derivative. For example, other NaC implementations include AdChoices, nutrition labels for privacy, and the Privacy Preferences Project (P3P). Therefore, unlike the other MoCs that may include hundreds, thousands, and even tens-of-thousands of separate methods, NaC represents the entire effective body of individual choice mechanisms.

NaC describes a set of requirements for service providers. These requirements affect business policies and values by allowing consumers to make informed market decisions related to the use of their data. These informed market decisions are supposed to ultimately influence market demand and supply. However, this chapter reveals a number of problems with the NaC framework, as well as problems at the intersection of NaC and IoT. NaC is related to IoT because it is the current market standard and de facto best practice for providing a consumer MoC over data collection and use. Most of these online services and technologies, such as the Nest Thermostat and Fitbit, rely on devices that fit within the IoT ecosystem. This chapter shows that the reliance on NaC leads to a significant privacy and security market failure. Further, I conducted an IoT study with two fellow researchers that yielded results that suggest NaC will continue to fail in the domestic domain due to how consumers interact with IoT devices in the modern marketplace.[1]

3.2 The History of Notice and Choice

The NaC framework involves the creation and publication of, and the adherence to, privacy and data policies by companies that collect and use consumer data. These policies must also include consent mechanisms that allow consumers to make their own choices regarding data use and collection. The origin of the NaC framework comes from what is known as the Fair Information Practices (FIPs). Since the late 1970s, this list has served as “internationally recognized practices for addressing the privacy of information about individuals.”[2][81]

[1] For the entire text of this study, please see Appendix A.

[2] The origin of FIPs traces back to a 1973 report from the Department of Health, Education, and Welfare.[18] For a complete transcript and summaries of the meetings that led to the creation of FIPs, please see [94] and [95]. Other origins include a 1972 report from Great Britain’s home office [160], the Privacy Protection Study Commission’s 1977 report [40], and an OECD report from

The actual list of FIPs is different depending on the source. For example, the FTC and DHS have different lists even though they are both federal agencies with some enforcement capabilities in the IoT privacy and security space.[3] The version of FIPs that matters in the context of the NaC framework is the list released by the FTC in 1998, and updated in 2000 and 2010.[69][70][71] In the 1998 report, the FTC provided the ICT industry with a simplified FIPs.[45] The FTC list includes the following four principles:[4][71]

1. **Notice** - Websites must provide consumers "clear and conspicuous notice" of data practices, including what is collected, how it is collected, how it is used, how they provide Choice, Access, and Security, whether they disclose collected data to third parties, and whether third parties collect data through the site.
2. **Choice** - Websites must offer consumers choices regarding how personal identifying data is used beyond the use for which the information was provided.
3. **Access** - Websites must provide consumers access to collected personal data, including the ability to review and correct inaccuracies

1980 [158] (updated in 2013). These parallel endeavors demonstrate an international convergence on data privacy and security ideals.[23] This realization, first demonstrated and analyzed by the book "Regulating Privacy: Data Protection and Public Policy in Europe and the United States," is a profound conclusion.[23] Though it is beyond the scope of this thesis, it would be worth investigating how the European and U.S. practical approaches to data privacy and security ultimately diverged after this initial convergence and should be considered in the context of the work "Privacy on the Books and on the Ground."[22] An interesting aspect of these supporting endeavors is not only their similarity to each other, but also the similarity between the state of information privacy and technology in the 1970s to the state of information privacy and technology today.[81] In short, not much has changed in 40 years, and that which has changed, such as the scale of data usage and harms, has worsened.

[3] For a complete review of the many different interpretations of FIPs, FIPs lists, and FIPs history, please see [81].

[4] It is important to note that the 1998 and 2000 versions of this list also included **Enforcement** as a fifth principle.[69][70] The most recent 2010 version refers to **Enforcement** as a fifth principle but does not include it in the explicit FIP list.[71] It is also important to note that this 2010 version of FIPs is considered outdated since the White House released the "Consumer Privacy Bill of Rights" in 2012. However, the FTC is yet to explicitly publish an updated list of FIPs, and since the FTC is the organization that enforces and champions NaC, these four FIPs must be highlighted. For the sake of completeness, the "Consumer Privacy Bill of Rights" describes a more comprehensive list of principles: **Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability**.[98]

or delete information.

4. **Security** - Websites must take reasonable steps to protect the security of the consumer data they collect.

One can see the genesis of the NaC framework as the application of these FTC FIP principles.[5] Publishing a data policy and allowing users the opportunity to consent to data use and collection complies with the FIPs. Between the initial publication of the FTC's FIP in 1996 and the most recent version in 2010, the FTC has encouraged a market-based approach to data privacy through individual choice control.

3.3 The Problems with Notice and Choice

The NaC framework is a pragmatic and market-based approach to information privacy and security. It recognizes that companies are reluctant to stop collecting or using consumer data, while also acknowledging that users expect to retain a degree of control. However, there are a number of issues with this framework along philosophical, implementation, and use grounds.[6] Further, as demonstrated by an IoT consumer study I conducted with two fellow researchers (See Appendix A), the degree to which consumers concern themselves with privacy and security issues suggests the NaC framework will *not* be an effective MoC for improving IoT privacy and security.

3.3.1 Philosophical Problems

The NaC framework provides meager privacy and security values. There is a wide consensus among privacy advocates, academic researchers, and policymakers that privacy policies and the NaC framework are poor mechanisms for communicating to users the privacy and security harms related to the collection and use of personal

[5] One can also see a major issue with NaC as applied to IoT - the fact that NaC was designed specifically for websites and not devices. This fact is discussed in Subsection 3.3.2

[6] For a comprehensive review of NaC problems, a design space for creating usable and effective privacy notices, and three case studies that include website and social media services, smartphone apps, and photo/video lifelogging, please see also [189]. Further, for a focused case study on IoT healthcare privacy, security, and consumer protection mechanisms (including NaC), please see [150].

data.[32] A casebook titled *Privacy Law and Society* characterizes the NaC framework not as a MoC that ensures an organization's obligations towards information privacy and security, but rather as a waiver system that allows companies to use private data as they desire.[186] The implications of such a system are clear. The intent is not to protect users' privacy and security. The intent is to monetize and utilize user data in a legally defensible manner. This intent is not the same as the values inherent in FIPs, which are to protect consumers from data-related harms. Therefore, this structure actually exacerbates the IoT privacy and security challenges *Business Models* and *Economic Incentives*. Further, it also exacerbates the challenge *Psychological Bias* because it often forces the consumers to choose between an unobservable harm and a tangible, present benefit.

3.3.2 Implementation Problems

There are three major implementation problems with the NaC framework in relation to IoT: user interfaces, language clarity, and consent scope. First, it is often challenging to find IoT device data policies or for IoT services to ask for user consent. Many devices do not have usable interfaces through which to transmit privacy and data policies. The standard NaC implementation often creates too great a burden for an IoT company to provide user consent mechanisms, as demonstrated by the stakeholder comments on page 20 of the 2015 FTC report, *IoT Privacy & Security in a Connected World*.[75] For example, an automobile telemetry-based IoT system like the *Automatic Connected Car* has no user interface on the device. Even more challenging, consider IoT services in the domains retail, transportation, and healthcare that capture a person's data in fleeting moments. A good example of such a system is a traffic management scheme that uses RFID tags or license plate readers to track individual vehicle movement. With these systems, it would be inconvenient and burdensome to stop a subject and ask for consent. Solutions for this problem do exist, such as offering data-related policies when a consumer purchases a device, or through a computer or common interface such as a smartphone data policy application. However, one study of 20 available IoT devices discovered that none included any privacy- or data-related information at the time of purchasing, including on the device's box.[171] Additionally, the IoT consumer study I conducted with two fellow researchers (Appendix A) suggests that consumers typically do not look for or consider data privacy and security information when they purchase an IoT device. Further, the former study also determined that most of the online data policies related to the 20 devices were unclear and unspecific regarding data practices.[171]

This fact leads to the second major NaC implementation issue: language clarity. It is non-obvious in many data policies what constitutes personal information, and sensor data is rarely included. Unclear language in privacy policies has plagued efforts such as P3P,[130][135] crowd-sourcing annotations for privacy policies,[220] and standardized privacy notices in the nutritional label approach.[124] Overall, privacy and data policies are confusing regardless of length or format, and this lack of clarity leads to consistent comprehension and effectiveness failures – a result demonstrated in a 2009 study that compared 749 internet users' comprehension of six companies' data policies.[144]

The third implementation problem is due to data collection ubiquity and scope in IoT systems. The fact that NaC relies on an individuals' consent has troubling IoT implications. Many IoT systems have the potential to collect information far beyond the purview of a single user – consider IoT services such as security systems, object tracking, and activity analysis. Therefore, NaC also compounds the IoT privacy and security challenge *Negative Externalities* since one user's consent might reveal information about a different user, especially in the context of an IoT system. For example, it is unclear whether or not every member of a home or workplace will have an opportunity to opt-in to services provided by IoT technologies such as the Amazon Echo. Current NaC rules to not address problems such as ubiquitous devices and continuous collection. Therefore, NaC fails to consider the social impact of privacy and security decisions.[182]

3.3.3 Use Problems

A study completed by a group at Carnegie Mellon University demonstrated that NaC, when used by consumers, is not an effective way to help users control which data gets shared, when, and with whom.[45] These results are due to both functional and psychological use problems.

Functional Use Problems

Most online services, including IoT services, use third parties to collect, track, and analyze data.[7] A service's data policies can provide some clues as to how it uses third parties, but it does not govern the third parties. Nor do most privacy policies provide much information on third parties. A 2015 study on the Network Advertising Initiative (NAI)[8] member companies' data policies found that while 78% mention data-sharing relationships with third parties, none indicate that those sources provide any data protections or NaC. 22% of member companies' policies did not even mention third party relationships.[46] Therefore, it is challenging for users, through a consent framework based on service data policies, to control what happens to their data.[9] This fact is especially true when the structure and content of those policies is not standardized. After a small number of abstractions – third parties sharing with third parties – it becomes impossible to know the full scope of data tracking, analysis, current and future data uses, and potential harms.[182] This problem compounds the IoT privacy and security challenges *Economic Incentives*, *Information Scope*, *Accountability*, and *Data Aggregation*.

[7] For a good review on the problems that third party services bring to privacy and security, please see [191].

[8] The NAI is a non-profit SDO comprised of digital advertising companies with the intent of self-regulating data collection and use for advertising online and in mobile ecosystems.

[9] Since NAI is a group of digital advertisers, not IoT service providers, this study might seem out of scope. However, the exact same NaC framework applies to both realms. Further, the study results revealed a fundamental flaw with data policies as a controlling factor through the NaC framework. There is no evidence that suggests data policies will somehow work for the IoT ecosystem when they have failed in others.

Psychological Use Problems

Psychologically, the NaC framework is also ineffective because humans suffer from specific cognitive biases. This fact is best demonstrated in a study in which participants believe that the *existence* of a privacy/data policy means that the service is committed to *protecting* personal information.[162] This effect is a *non sequitur* fallacy since a company could write a privacy policy that legally removes many privacy protections and asks for consent to do so. This problem compounds the IoT privacy and security challenges *Psychological Biases* and *Information Scope*.[10]

Other NaC Use Problems

Another practical NaC use issue is the untenable costs to the users. A study completed in 2008 found that it would take the average internet user about 244 hours per year to read every privacy policy relevant to their online lives.[143] This problem compounds the IoT privacy and security challenges *Solution Costs* and *Information Scope*, and is itself further compounded by the challenge *Device Ubiquity.* With the predicted growth of the IoT ecosystem in every domain, there is little doubt that this barrier to enacting meaningful user control mechanisms through the traditional NaC framework will continue to grow. Further, this barrier to providing meaningful consent exists even when the actual content of the policies is considered complete, robust, and transparent. The issue was best characterized by Daniel Solove in his 2013 work on the consent dilemma when he wrote,

> ”The problem is reminiscent of the beleaguered student whose professors collectively assign too much reading each night. From the perspective of each professor, the reading is a reasonable amount for an evening. But when five or six simultaneously assign a night’s worth of reading, the amount collectively becomes too much. Thus, even if all companies provided notice and adequate choices, this data management problem would persist; the average person just

[10] For another fascinating study on user’s psychological biases, see [131]. In this study, the researchers reveal how privacy practices affected users’ attitudes toward data sharing, and ultimately find that more restrictive data-retention and use policies increase a user’s willingness to allow more sensitive data collection.

> does not have enough time or resources to manage all the entities that hold her data."[198]

Even more generally, the NaC framework is not a broadly applicable privacy and security control mechanism, even though it is used as such. The FTC's limited FIPs (**Notice, Choice, Access, and Security**) are only considered in relation to a user's *private information*. *Private information* has a strict definition that rarely includes sensor data. In the IoT ecosystem, it is conceivable that the most risky and harmful data is the sensor data that might reveal desires, values, and actions. When one considers the various domains and use-contexts for IoT technology, the NaC framework is not applicable as a privacy and security control mechanism.

Finally, the information offered by NaC policies can be interpreted differently depending on the user's backgrounds. One study demonstrates that privacy policies lead to mismatched understandings between users with different levels of technical knowledge, thus propagating the privacy and security challenge *User Knowledge.*[181] These mismatched understandings exist not just *between* different groups, but also *within* the same group. Even those users with a high level of technical expertise and knowledge could not come to a consensus regarding the practical meaning of privacy policies. This study concluded that, "If websites are not effectively conveying privacy policies to consumers in a way that a "reasonable person" could understand, NaC fails as a framework. If consumers cannot successfully decode privacy policies, the underpinnings of the U.S. approach to privacy are unsustainable, and regulation may be necessary."[181] As has been discussed, it is clear that the NaC framework, as currently applied, fails to allow consumers to decode data policies.

3.4 Proposed Improvements

The fundamental challenge with NaC as applied to the IoT ecosystem, highlighted by every problem above, is that it was conceived as a website-based system where every user has a common interface and most users act in ways that only affect their own data, not the data of others. IoT systems and services have fundamental differences.

Not only do many IoT systems not have user interfaces and tend to collect data on numerous subjects, but they also collect new types of data using sensors that NaC was not designed to address. Private information in the IoT ecosystem is fundamentally different, and the traditional concept of private information must broaden to include new types of sensor data and, most importantly, uses of that data. Data harms in the IoT ecosystem come from the use of sensor data in ways that draw actionable inferences, whether accurate or not. For example, IoT data "creates the possibility of new forms of racial, gender, or other discrimination [. . .] data can be used as hidden proxies for such characteristics. In addition, such data may lead to new forms of economic discrimination as lenders, employers, insurers, and other economic actors use Internet of Things data to sort and treat differently unwary consumers."[171]

For NaC to provide effective controls for IoT privacy and security, new interfaces must be developed. Some researchers have proposed a control device, such as a smartphone, with a management portal to configure privacy settings per device, machine readable forms or icons, or even learning algorithms that make choices for the consumer based on prior behavior.[44][75] However, a well-known researcher in this space, Lorrie Cranor, highlights that these recent discussions mirror a national discussion in the mid-1990s that led to a 1997 Department of Commerce report, "Privacy and Self-Regulation in the Information Age." She characterizes this twenty-year-old discussion on data privacy and security self-regulation and consumer choice as a market failure when she states that the NaC mechanisms "have failed users and they will continue to fail users unless they are accompanied by usable mechanisms for exercising meaningful choice and appropriate means of enforcement."[45] Therefore, the traditional concepts of improving individual choice mechanisms have failed in the IoT ecosystem.

3.5 Individual Choice Conclusion

The individual choice mechanism for controlling IoT privacy and security has a laundry list of challenges working against it, including *Economic Incentives*, *Information Scope*, *Psychological Biases*, *Business Models*, *Solution Costs*, *Accountability*, *Device*

Ubiquity, *Data Aggregation*, and *Negative Externalities*. The NaC framework does not solve any of these problems, although it was designed as an attempt to solve *Information Asymmetry* and *Accountability*. In practice, it provides some degree of improvement for both those challenges, though these improvements are marginal compared to the challenges that it exacerbates. As one legal research scientist concluded, "NaC is an ill-fitting solution to these problems, both because Internet of Things devices may not provide consumers with inherent notice that data rights are implicated in their use and because sensor-device firms seem stuck in a notice paradigm designed for websites."[171] In its current state, NaC, the de facto industry standard individual choice MoC, is ineffective at improving IoT privacy and security. In fact, NaC often works *against* improving IoT privacy and security by supporting and propagating key challenges and business practices that degrade IoT privacy and security. Table 3.1 demonstrates these deficiencies.

That being said, consumer choice mechanisms as applied to IoT privacy and security is an important research endeavor. Users of these systems, across various domains, still deserve the right to evaluate the data policies and implications of the IoT services they use. If anything, this fact supports the idea that the NaC framework must be improved since it is a means of controlling the data use-contexts, actions, and values of an IoT service provider, device manufacturer, or data broker.

More importantly, as will be discussed in Chapter 8, data policies and adherence to the FTC's FIPs are one of the few regulatory controls available to address data privacy and security. Therefore, in order to improve the current framework, IoT individual choice mechanisms must take into account a few fundamental aspects of IoT domains. First, the use-contexts, implications, and harms are different for each domain and therefore the application of a individual choice mechanism such as NaC must be different for each domain. Second, the data policies that form the "notice" arm of NaC must *represent* the use-contexts, implications, and harms for each domain. Third, regulation and authorities must be developed to apply and control the use-contexts, implications, and harms for each individual domain. These requirements and areas for work are discussed in more detail in Chapter 9.

Table 3.1: Domains covered, stakeholder power, and challenges impacted by the NaC framework.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Developers/Manufacturers (+++)	Accountability (+/–)
Domestic	Consumers (+)	Info Asymmetry (+/–)
Education	Government Agencies (++)	Business Models (–)
Entertainment	Service Providers (+++)	Data Aggregation (–)
Finance	Data Brokers (+++)	Economic Incentives (+/–)
Government		Information Scope (–)
Healthcare		Negative Externalities (–)
Infrastructure		Psychological Biases (–)
Insurance		Slow Legislation (+)
Manufacturing/Trade		Solution Costs (–)
Retail/Hospitality		User Knowledge (–)
Telecommunications		
Transportation		
Workplace		

Chapter 4

Command and Control Regulation

4.1 Introduction

There exists no command and control regulation in the U.S. written to control IoT data privacy and security. The U.S. approach to such regulation is one characterized by the influence of market control and de facto controls through the FTC's common law authority.[1][22] In practice, data privacy and security in the U.S. often relies on context-specific rules administered by domain-specific authorities such as the Federal Trade Commission or the Food and Drug Administration.

That being said, a few "on the books" U.S. regulations have the *potential* to impact IoT privacy and security as the ecosystem develops. Therefore, it is crucial to consider the current command and control regulation MoC.[2] This chapter considers one such regulation: the Health Insurance Portability and Accountability Act (HIPAA).[3]

[1] This style of privacy and security control is called "on the ground" regulation, as opposed to the EU's "on the books" style of formal written privacy and security regulations.[22]

[2] I draw a distinction between command and control regulations, which declare direct and specific goals and procedures for improving privacy and security, and more indirect forms of regulation, such as those that grant authority to an agency such as the FTC to write rules and adjudicate issues related to privacy and security. This section only deals with command and control regulations.

[3] Other command and control regulations that impact IoT privacy and security exist, though they are not discussed in this thesis. These include the Child Online Privacy Protection Act (COPPA) and the Privacy Act of 1974, neither of which are discussed in this section because the MoC they support, Individual Choice, is discussed in Chapter 3. Other regulations with the potential to impact IoT privacy and security include the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), and the Dodd–Frank Wall Street Reform and Consumer Protection Act. For a full discussion of these regulations and their impact on IoT privacy and security, see [163].

HIPAA enacts privacy and security controls within the healthcare domain. This chapter contributes an explanation of how this MoC impacts IoT privacy and security. Ultimately, this chapter demonstrates that the command and control regulation MoC for improving IoT privacy and security is currently sparse and confusing, but has potential to be an effective IoT privacy and security control. However, that potential is limited by tremendous resistance from IoT stakeholders such as developers, service providers, and data brokers.

4.2 Resistance to Command and Control Regulation

Vinton Cerf, chief architect of the TCP/IP protocol and co-founder of *Internet Society*, wrote that IoT privacy regulation "is tricky [. . .] we're going to have to experience the problems before we understand the nature of the problems."[51] Cerf has also been a champion of the self-regulatory framework. He, along with other principle directors at Alphabet Inc., has advocated for a system of shared responsibility where all stakeholders retain some locus of privacy and security control while developers and service providers retain broad power to design and implement their own solutions.[34] Most interestingly, this framework proposed in the 2016 work "IoT Safety and Security as Shared Responsibility" limits government's responsibilities to 1) enforce consumer protection and health & safety (such as the FTC's authority discussed in Chapter 8), and 2) educate consumers on topics like identifying common attacks and harms.[34] This popular framework does not acknowledge command and control regulation as an approach to enhancing IoT privacy and security. In fact, most renowned technologists who represent stakeholders such as developers, service providers, and data brokers, have advocated for self-regulation in the space of IoT data privacy and security.[139]

This advocacy is logical since it seeks to retain their onus of control. The sole expressed argument against command and control regulations is the hypothetical yet detrimental effects on economic growth and innovation (the challenges *Slow Legislation* and *Regulation Uncertainty*).[4][146] However, regardless of the economic and

[4] Calling this the "sole" argument against command and control regulations might seem

innovation concerns expressed by companies such as AT&T [17][145] and the Consumer Technology Association [106], a lack of command and control regulation has been shown to lead to consumer harms like economic and racial discrimination in the healthcare and insurance domains.[74][150][171] In 2013, The Privacy Rights Clearinghouse, a privacy and security advocate, released a study on 43 health and fitness systems that showed none encrypted locally stored data and only 15% encrypted transmitted data.[97] Further, the key privacy and security challenges *Economic Incentives*, *Information Asymmetry*, *Business Models*, *Solution Costs*, and *Accountability* encourage the self-regulatory model to develop lax privacy and security controls.

The issue of the command and control regulation MoC is one that seems to balance the values of economic growth and innovation against the values of consumer protection and safety. There is industry consensus that the intent of any IoT privacy and security regulation would be to protect consumer safety by restricting the acceptable activities of stakeholders such as developers, service providers, and data brokers.[146] However, it is unclear whether the effectiveness of such regulations would outweigh any detrimental impacts. It is also unclear if those detrimental impacts will actually occur. Since no IoT-specific command and control regulations exist, I present a case study on HIPAA as a proxy. HIPAA is a reasonable case study because it creates privacy and security controls for data handling within the healthcare domain. Further, it has already impacted the adoption of IoT healthcare technologies.

grandiose. However, it is an intentional and factual claim. Industry stakeholders such as service providers, manufacturers and developers, data brokers, and even federal authorities have all *verbally* expressed this singular concern regarding command and control regulation in the IoT ecosystem (see Chapter 8.4). These same stakeholders, as well as SDOs and privacy and security advocates, have also expressed this singular concern in writing.[6][10][16][21][27][34][44][62][72][75][49][106][139][146][150][182][198][218] It is likely that each stakeholder has their own motivation for making such an argument. For example, the current industry approach to privacy and security control is one of self-regulation. Therefore, service providers, manufacturers and developers, and data brokers have immense power and every incentive to argue against relinquishing it. Regardless of the merits or intention of this argument, its singular nature suggests that if someone were to show that command and control regulation could enhance innovation and economic potential, or build a coalition of these same stakeholders, one could rapidly increase the effectiveness of IoT privacy and security controls.

4.3 The Health Insurance Portability and Accountability Act (HIPAA)

4.3.1 Background

HIPAA is a sector-specific regulation originally passed in 1996 that concerns the healthcare industry.[65] Though this law was not designed to influence the IoT, IoT devices and services are expected to influence health insurance, healthcare diagnoses, treatment efficiency, healthcare data analysis, and more.[150] Therefore, HIPAA will also influence the IoT healthcare domain. Further, two HIPAA provisions will impact IoT privacy and security, the Privacy Rule and the Security Rule. The Privacy Rule dictates a set of roles, responsibilities, and rules to "protect individual's medical records and other personal health information" regardles of medium, digital or physical.[88] The Security Rule dictates a standard designed "to protect individual's electronic personal health information that is created, received, used, or maintained by a covered entity."[88] Both rules govern the collection and use of personal health information (PHI). PHI is a broad category that includes personally identifiable information related to health and wellness, and transactional information such as payment history.[5]

The organizations required to adhere to HIPAA include healthcare providers (doctors, nurses, dentists, etc.), medical establishments (hospitals, clinics, pharmacies, etc.), health plan providers (health insurance companies, Medicare, Medicaid), and healthcare clearinghouses (organizations that provide services related to healthcare data).[87] It is entirely conceivable that a number of IoT manufacturers, data brokers, and service providers who provide IoT healthcare devices and services will fall under these covered entities. Therefore, HIPAA has the potential to directly influence IoT privacy and security.

[5] For the complete definition of PHI, please see Appendix B.

4.3.2 The Privacy Rule

The intent of the Privacy Rule is to limit the use and disclosure of PHI without patient consent to the minimum degree necessary to provide the service. It includes an explicit set of acceptable PHI uses. This fact is important because it shows that HIPAA is concerned with the harms created by data use, and not just by the existence of the data. Further, it also grants patients rights over their own data, including rights to examine and obtain a copy of their data, and to correct errors.[6] Finally, the Privacy Rules also includes a set of normative compliance actions for covered entities. These actions include designing a restricted access and use plan for PHI, providing a notice of privacy practices, providing users a means to review and obtain their data, providing users a means to correct inaccuracies in their data, providing users a report on what of their PHI has been disclosed and to whom, and allow users to restrict the use and disclosure of their PHI. Due to the explicit nature of the acceptable data uses, the Privacy Rule is effective at improving the challenges *Business Models*, *Data Aggregation*, and *Dynamic Contexts*. Due to the clear required compliance actions, the Privacy Rule is effective at improving the challenges *Accountability* and *Information Asymmetry*.

4.3.3 The Security Rule

The intent of the Security Rule is to specifically protect both the privacy and security of electronic PHI (e-PHI). It requires administrative, physical and technical safeguards. By dealing with all levels of an organization's data handling system, it endeavors to improve the challenge *Business Models*. It also builds an inherently adaptable data protection system by allowing covered entities to determine their own degree of risk and solutions. It uses terms such as "reasonably anticipated threats" and "reasonably anticipate, impermissible uses or disclosures" to allow organizations to develop their own prescriptive standards.[88] The rule goes so far as to explain the types of factors a covered entity should consider while developing solutions, such as its

[6] These rights are akin to the Fair Information Practices discussed in Chapter 3.

size, complexity, and capabilities; its technical, hardware, and software infrastructure; the costs of security measures; and the likelihood and impact of e-PHI risks to the user. By doing so, the Security Rule creates a compliance structure that allows organizations to adapt to their own needs within desired privacy and security constraints [31], thus improving the challenge *Dynamic Contexts*, *Regulation Uncertainty*, and *Business Models*.

4.3.4 HIPAA and IoT

There is little doubt that IoT will permeate the healthcare domain. A few use cases include connected hospitals [129], healthcare wearable technologies [206], new medical sensors implemented in systems such as a stool-analyzing toilet [28][180], and an in-home connected personal healthcare laboratory testing and diagnosis kit [138]. However, a literature review at the junction of HIPAA and IoT reveals three major concerns with the impact the regulation will have on IoT: the complexity of the HIPAA privacy and security rules as related to software development, the narrow definition of PHI, and uncertainty regarding if HIPAA rules control IoT technologies and services.

HIPAA's Complexity

An impressive recent study extracted, analyzed, and modeled the HIPAA privacy and security requirements and their impacts on software developers.[8] This work concludes that the complexity inherent in total HIPAA compliance are too great for software developers to extract meaningful requirements for their work. In a separate study, the same group extracted HIPAA data privacy and security rules and applied them to various e-health services.[9] They attempted to create a mechanism for developers and service providers to wade through HIPAA's complex rules. While their proof of concept worked, it also demonstrated that HIPAA's overall compliance complexity negatively impacts the efficiency with which developers, manufacturers, and service providers can bring their products to market and force those stakeholders to incur higher time and monetary costs. Therefore, HIPAA negatively impacts the IoT privacy and security challenges *Solution Costs* and *Regulation Uncertainty.*

HIPAA's Narrow PHI Definition

Another concern is the fact that it is unclear whether or not information collected by IoT sensors can be considered PHI. Both the Privacy Rule and the Security Rule apply narrowly to PHI. If IoT sensor data is not PHI, then HIPAA will have no impact on IoT privacy and security. According to HIPAA, PHI is "any information, including genetic information, [. . .] that (1) [i]s created or received by a healthcare provider, health plan, [. . .] and [. . .] (2) [r]elates to the [. . .] physical or mental health or condition of an individual."[126] There is little doubt that in some clear cases, such as cardiovascular data from a connected pacemaker, that this data is related to the physical health of an individual. However, issues arise on the margins. For example, it is unclear if data such as sleep trends and caloric intake from fitness devices is considered PHI. According to one legal scholar, Scott Peppet, "HIPAA's definition would most likely *not* encompass fitness- or health-related - let alone other - potentially sensitive sensor data."[171] Other stakeholders in the IoT healthcare industry are currently unsure.[150] This information can be used to extrapolate a person's health, but it is not clear whether the raw data itself is considered PHI. Combined with the costs associated with HIPAA compliance, technologies and services on the margins have every incentive to distance themselves from being considered responsible to HIPAA rules. This fact has the potential to negatively impact the IoT privacy and security challenge *Business Models* by encouraging companies to find loopholes in the PHI definitions and operate on those margins.

HIPAA's Uncertain Applicability to IoT

Similar to the issue comparing PHI with IoT sensor data, it is similarly unclear whether IoT developers, IoT service providers, and IoT data brokers fall under the category of covered entities. A good example is Fitbit, a company that serves as an IoT healthcare developer and service provider. HIPAA does not currently apply to Fitbit by the letter of the law.[171] Further, the only way that such technology companies would be covered by the regulation in its current form is if they partner with a covered entity, such as a hospital. That being said, companies like Fitbit and Medtronic, a producer of connected pacemakers, have achieved HIPAA compliance standards for specific services due to the business opportunities inherent in partnering with covered entities.[67][147] These actions suggest that IoT healthcare developers and service providers will implement HIPAA standards on their own accord. Further, there is no evidence that either Medtronic or Fitbit had to sacrifice innovative capability or economic growth in order to comply with HIPAA rules. Therefore, HIPAA improves the challenge *Business Models* while avoiding the challenge *Slow Legislation*.

While it is promising that Medtronic and Fitbit voluntarily chose to align with HIPAA controls, these stakeholders are not required to comply with HIPAA. The lack of such a requirement creates a potential avenue for privacy and security failure in the IoT healthcare domain. In a 2015 report, the FTC called for more IoT-specific guidelines under HIPAA.[75] None have been proposed. This lack of clear regulatory guidance leads to self-regulation and potential non-compliance with unclear legal and ethical ramifications.[6][217]

4.4 Command and Control Regulation Conclusion

HIPAA, the healthcare-specific regulation, provides privacy and security rules related to individual healthcare data. These rules are comprehensive across all aspects of a healthcare organization's data and business operations. Further, they cover a wide set of entities that handle PHI data, including technology developers, service providers, and data brokers. Most importantly, the rules are written in such a way as to allow individual organizations to determine the best way to achieve compliance based on their own contextual concerns.

A few concerns do exist at the intersection of IoT and HIPAA. First, some aspects of the rules provide unclear or overly complex requirements for software developers. This fact increases *Solution Costs* and has the potential to deepen the issue of *Reg-*

ulation Uncertainty. Further, the extent to which the definition of PHI covers IoT sensor data is unclear. This fact has the potential to deepen the challenge *Business Models* by encouraging IoT service providers to circumvent the unclear definitions by operating on the margins. Finally, the extent to which HIPAA privacy and security rules actually apply to IoT developers and service providers is also unclear and has led to uncertainty within the IoT healthcare domain. In practice, a few IoT healthcare developers and service providers, like Medtronic and Fitbit, have achieved HIPAA compliance on their own accord. This fact suggests that the HIPAA regulation has had a positive impact on IoT privacy and security on the ground, and will continue to do so as the IoT healthcare domain expands.

However, HIPAA is not an IoT healthcare privacy and security panacea. In a recent disturbing case, an internet connected pacemaker distributed by healthcare technology provider St. Jude Medical was shown to be vulnerable to malicious attack.[136] Further, this same report demonstrated a significant and persistent laxity in data privacy and security standards implemented by St. Jude Medical in their healthcare technology products. In testing, sensitive health data was manipulated, leaked, and stolen from the device. Even more disturbing, the device functions were altered in a way that could deliberately kill a user. While St. Jude Medical is responsible to the HIPAA privacy and security rules, this recent case questions whether those protections are effective and powerful enough on the ground to protect consumers from harm. Further, there is also some evidence that suggests St. Jude Medical knew about these vulnerabilities and only chose to address them after they were made public by a third party.[122] Therefore, it seems that the HIPAA controls do not improve *Business Models* to a significant degree.

Table 4.1 shows HIPAA's effect on the IoT ecosystem based on the MoC evaluation factors outlined in Part I. The results of this analysis suggest that domain-specific regulations that establish data use standards based on contextual concerns provide an effective MoC for IoT privacy and security. However, analysis of that effectiveness suggests there are areas where HIPAA privacy and security controls could be improved such as *Regulation Uncertainty*, *Solution Costs*, and *Business Models*.

Table 4.1: Domains covered, stakeholder power, and challenges impacted by the HIPAA data privacy and security rules.

Domains	Stakeholder Power	Impact on Challenges
Healthcare	Data Brokers (+)	Accountability (+)
	Developers/ Manufacturers (+)	Business Models (+/–)
	Regulatory Authorities (++)	Data Aggregation (+)
	Service Providers (+)	Dynamic Contexts (+)
		Info Asymmetry (+)
		Regulation Uncertainty (+/–)
		Solution Costs (–)

Chapter 5

Operational Standards

5.1 Introduction

Operational standards are a well-developed realm of IoT privacy and security MoCs. In fact, standards developing organizations (SDOs) have already created IoT-specific privacy and security standards. Due to this maturity, there are a wealth of IoT privacy and security standards – more than 400 by the count of one recent research endeavor.[1][114][115] No authority or industry partnership in the U.S. has agreed upon a single operational standard for IoT privacy and security. These facts lead to the first major deficiency in the IoT standards MoC, the challenge *Standards Saturation*. With hundreds of operational standards and a lack of standardization between them, the current market appears to be structurally ineffective. However, de facto norms and industry leaders do exist, and it is important to address them.

Operational standards are primarily geared towards enterprise and private organizations. They provide strategic, structural, and organizational best practices. The industry leaders in this space are the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU). This chapter provides a MoC case study for two

[1] The full catalog of IoT relevant standards cited in this report can be downloaded from [114]. While extensive, this catalog is *not* comprehensive and many more than the 418 IoT relevant standards cited in this document do exist. For example, the list does not include any IETF standards. A beneficial research project would be to expand this catalog to make it comprehensive.

sets of relevant data privacy and security standards, the ISO/IEC 27k series and the ITU Y.20xx series, and reveals how those standards impact IoT privacy and security.

5.2 ISO/IEC 27k Series Standards

5.2.1 Introduction

The 27k series is the main ISO/IEC standard that relates to IoT privacy and security, and is considered the "common language of organizations around the world" for information privacy and security.[52] The 27k series is concerned with information security management systems (ISMS). An ISMS involves all physical and operational requirements to ensure proper information privacy and security, including the data handling policies in an organization's business model.[195]

The 27k series includes dozens of individual standards, though those specifically related to IoT can be found in Appendix C. These standards cover every topic from governance instructions, risk management, measurement, auditing procedures, a more domain-specific standards for the finance, cloud services, public infrastructure, and healthcare sectors.[61] This fact reveals the type of domains and stakeholders targeted by this standard.

It is important to note that the 27k series' overall approach is risk management independent of specific technologies. It provides broad, high-level requirements in order to encourage companies to internalize privacy and security goals based on the risks of their specific information systems.[61] In that sense, it is effective at improving the challenges *Economic Incentives* and *Accountability*.

The standard is currently used in 132 countries.[112][205] As of 2015, there were 27,536 ISO/IEC 27001 certificates granted worldwide, a 20% increase since 2014 and a 76% increase since 2010.[52][111] Therefore, it is clear that not only is the 27k series popular, it is also growing in popularity. In 2015, 38% of the 27,536 certifications were for European companies, 44% were for companies in the East Asia/Pacific region, 9.3% were for companies in Central/South Asia, and only 5.2% were for companies in North America.[112] The other 3.5% were for companies in Africa, Central/South America, and the Middle East.

It is interesting that so few certificates are issued in North America. Some researchers believe this is due to the fact that North American and European companies outsource their information management services to companies in Asia.[52] This conclusion makes sense due to the fact that there are no federal rules in the U.S. against exporting personal data internationally, and few state regulations.[121] However, this explanation is only partial. EU certification numbers are large because the EU pressures companies to institute prescriptive information privacy and security controls. For example, the UK national standard BS7799 served as the framework for the ISO/IEC 27k series discussed in this section.[14][195] In that context, few North American companies implement ISO/IEC 27k certifications partly because they outsource information management, and partly because the U.S. has a history of self-regulation in the ICT realm.[22] The ISO/IEC 27001 certificate is not as significant a signal in the U.S. as it is in other parts of the world. This fact limits ISO/IEC 27k series effectiveness in addressing IoT privacy and security challenges.

5.2.2 ISO/IEC 27k Compliance

The costs associated with 27k series compliance can be prohibitive for some IoT companies, especially in the domestic domain. To achieve compliance, the organization has to implement an appropriate ISMS under the guidelines of ISO/IEC 27001, pass a preliminary examination by a Registered Certification Body (RCB), pass a final examination by the RCB, pass annual audits by the RCB, and re-certify once every three years. Depending on the current implementation of a company's ISMS, this process will cost IoT companies upwards of $60,000.[2][1][42]

As one consultant group who helps companies achieve ISO/IEC 27001 compliance explains, "ISO 27001 is not a one-time exam, it is more like a religion. It is a commitment to do things the right way every day, and to submit to regular audits to confirm you are observing the religions[sic] practices every day, not just when

[2] For a complete cost breakdown, please see [1] and [42].

the vicar comes to tea."[1] This quote describes the ISO/IEC 27k series as a standard that intends to develop proper organizational values in the form of information privacy and security. Therefore, the standard does improve the challenges *Business Models* and *Accountability*. However, while this implementation style suggests that full compliance leads to effective privacy and security practices, it also suggests that full compliance involves massive *Solution Costs*.

While a "religious" burden might work for large developers or service providers in the finance, commerce, and transportation domains, many domestic services and technologies today are provided by small companies.[107] Large organization that offer IoT solutions for domains with significant economic power such as healthcare, manufacturing, finance, and agriculture can incur such large costs. However, IoT domains like domestic and retail contain small businesses that might find those costs prohibitive. Therefore, we can conclude that a burdensome operational standards like the one provided by ISO/IEC is inappropriate for many IoT applications because they fail to capture key domains with a high potential for consumer harm. The effectiveness of this standard in those domains is limited.

Further, a study published in 2016 by three researchers discovered no significant correlation between achieving ISO/IEC 27001 certification and a higher return-on-assets or increased stock market performance.[99] This result suggests that if a firm were to simply conduct a cost-benefit or return-on-investment analysis on implementing the ISO/IEC 27k series controls, they would choose not to adopt that standard. Therefore, it somewhat exacerbates the challenge *Economic Incentives*. While the ideals represented by such endeavors are admirable, they are far from practical. Still, the ISO/IEC 27k series does offer companies in IoT domains with large market power and the ability to incur large capital expenditures an excellent framework for developing secure and private informational systems.

5.2.3 Conclusion

While the ISO/IEC 27k series standards for information security management systems has seen widespread adoption, its application to IoT domains is limited to capital intensive domains and stakeholders with market power. Further, the ISO/IEC's own IoT working group concluded that the current number and massive scope of such standards creates too much uncertainty to improve the privacy and security of the IoT ecosystem.[115] Finally, the costs associated with such broad standards can be too great for effective implementation in a number of IoT domains. Therefore, future work on IoT operational standards for information security and privacy must take a closer look at domain-specific challenges. These additional requirements subsequently demand more work in defining and organizing the various IoT applications and technologies into specific use-contexts and domains. IoT is no longer a single entity, but an entire ubiquitous force of society.

Table 5.1 maps the ISO/IEC 27k series case study to the MoC analysis framework. As one can see, the domain applicability is broad due to the lack of a clear domain focus. Further, the stakeholders with power are similarly broad with most power centralized around the actual standard developer. Overall, while it is clear that such an operational standard can be effective at addressing some IoT privacy and security issues, it is also clear that such a standard requires a narrowed scope.

Table 5.1: Domains covered, stakeholder power, and challenges impacted by the ISO/IEC 27k series standards.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Data Brokers (+)	Accountability (+)
Entertainment	Developers/ Manufacturers (+)	Business Models (+)
Finance	SDOs (+++)	Economic Incentives (+/–)
Healthcare	Service Providers (+)	Regulation Uncertainty (+)
Infrastructure	Testing/Cert. Vendors (++)	Slow Legislation (+)
Insurance		Solution Costs (–)
Manufacturing/Trade		Standards Saturation (–)
Telecommunications		
Transportation		

5.3 ITU-T Global Standards Initiative

The International Telecommunication Union (ITU) is a UN agency dedicated to developing technical standards for information communication technologies (ICTs). It is a unique UN agency in the sense that it collaborates with both public- and private-sector stakeholders. Its membership includes 193 nations and 700 technology companies, academic institutions, and SDOs.[118] ITU is also a unique SDO in the sense that the information technology standardization arm of ITU, ITU-T, has conducted research and standardization processes for the IoT ecosystem since the mid-2000s. Most notably, the 2005 ITU-T report titled "The Internet of Things," defined the new IoT technologies, enterprise opportunities, policy challenges (including privacy and security), and the global implications of such a technology, while also considering and defining many of the numerous IoT domains and stakeholders.[117]

ITU-T operates through study groups (SGs), each with an individual focus. There are currently 11 SGs for the 2017-2020 work period, and one is specifically related to IoT: *SG20 - IoT, Smart Cities, & Communities.* This SG's standardization efforts focus on the infrastructure and transportation domains.

To date, ITU-T has released overarching IoT-centric standards in their Y.206x series. This review will specifically discuss standard *Y.2060 Overview of the Internet of Things* (2012) and *Y.2066 Common Requirements of the Internet of Things* (2014) as the primary IoT operational standards released by ITU-T. These are by no means the only ITU-T IoT standards. To date, they have released at least 61 different IoT-related standards that cover everything from highly specific and technical standards (such as security requirements for wireless sensor network routing), to more general standards (such as a framework for the web of things).[3] This broad list lacks a cohesive guide for an IoT stakeholder to choose the appropriate standard for their purposes and domain-specific concerns. Therefore, ITU's standards exacerbate the challenge *Standards Saturation.*

[3] For a full list of all IoT-related ITU recommendations, please see the annexes of [115] available at `https://www.iso.org/isoiec-jtc-1.html`.

5.3.1 Y.2060

Y.2060 defines IoT on both physical and virtual grounds. It accomplishes this definition through a three-dimensional structure with the following axes: Any Time Connection (day/night), Any Thing Connection (computer-computer, human-human, human-computer, thing-thing, human-thing, etc.), and Any Place Connection (in the home, on the move, outside, inside etc).[201] Therefore, this structure improves the challenge *Dynamic Contexts* by standardizing an IoT reference architecture that evaluates IoT devices and services through the idea of contextual risks. For example, the reference architecture includes operational considerations for topics such as system interconnections, integrations, management, and service applications.[201][119] Thus, this standard also attempts to alleviate the challenge *Device Capability* by addressing device limitations and risks in relation to the dynamic contexts.

Y.2060 was one of the first standards to define the IoT ecosystem across four distinct operational layers: **Application, Service, Network, and Device.**[4] By doing so, it demonstrates that all privacy and security risks and harms have different definitions, considerations, and potential resolutions at each layer and each contextual use. Once again, this approach alleviates the challenge *Dynamic Contexts.* Further, the emphasis on service and application level privacy and security improves the challenges *Business Models* and *Data Aggregation* as those challenges relate specifically to service and application level privacy and security risks. The *Business Models* challenge is also alleviated by the five specific business models developed by the Y.2060 standard.

The other major contribution of Y.2060 is a series of functional definitions for key IoT ecosystem terms such as *Communication Network, Thing, Device, Data-carrying Device, Data-capturing Device, Data Carrier, Sensing Device, Actuating Device, General Device, and Gateway.*[119] These definitions are important for operational standards because they provide a common lexicon for all IoT stakeholders. Therefore, when applied, the standard can also alleviate some of the issues associated with the

[4] These layers and their meaning for the IoT ecosystem are discussed in more detail in Chapter 1.2.2, and discussed in the context of technical standards in Chapter 6.

challenge *User Knowledge.* The framework also dictates responsibilities to each of these IoT functions and parts. For example, the definition of IoT *Gateway* not only includes relevant technologies (Zigbee, Bluetooth, Wi-Fi, LAN and W-LAN, etc.), it also describes the responsibility a *Gateway* has to provide and support interactions between applications, network management, device management, and security functions.[119] Once again, this focus alleviates issues arising from the challenge *Device Capability* while also addressing the challenge *Accountability.*

Overall, Y.2060 is a general operational standard. It provides an important first-look at IoT ecosystem considerations for organizations that intend to adopt an IoT service model. It offers a clear and common lexicon, high-level requirements, per-layer responsibilities, and even five individual business models for an IoT enterprise service.[119] However, Y.2060 is only a foundational standard. It offers background information and guidance for starting an IoT company and service. In terms of IoT privacy and security, it does suggest privacy and security are foundational components to every IoT process when it states, "Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled."[119] While a promising suggestion, it does not actually provide any functional standards or recommendations to improve information privacy or security. Y.2060 is more a framework for operational ideals than operational functions.

5.3.2 Y.2066

Y.2066 provides a more complex description of IoT operations, functions, and considerations than Y.2060. Further, it specifically includes IoT privacy and security as a fundamental requirement of all IoT systems. Y.2066 organizes all requirements under two headings, *functional* and *non-functional.* Functional requirements are those pertinent to device management, data management, security, communications, and services.[123] Non-functional requirements are those pertinent to the implementation, operations, and governance of an IoT system.

Y.2066 also defines and explains the four general use cases for IoT technology. The intent of these use cases is to explain every IoT system through a set of first principles that apply to all IoT domains. The general use cases are:[120]

1. Sensing or Actuating - involves the activities of connecting with physical things, sensing the states of physical things or actuating the physical things.
2. Data Management - involves the activities of capturing, transferring, storing and processing the data of physical things.
3. Service Provision - involves the activities of providing services by the service provider and using services by the IoT user.
4. Privacy Protection - involves the activities of securing and hiding the private information of the physical things.

One would be hard-pressed to find an IoT operation in any IoT domain that does not apply to one of these general use cases. Most importantly, Y.2066 defines IoT privacy and security as a fundamental first principle in each use case, therefore improving the challenge *Business Models.* The fact that ITU-T includes a set of first principles that can apply to every IoT domain, and ensures that privacy and security are part of those first principles, encourages stakeholders to not only include privacy and security as a building block of their IoT systems, but also do it in a way that works for their own unique domain risks.

Not only are these values evident in the ITU-T's IoT first principles structure, but also in Y.2066 section 7, "Important Areas for Consideration from a Requirement Perspective."[120] Three of the seven issues in this section mention privacy: *end-to-end intelligence, human body connectivity,* and *privacy protection related with things.* The first discusses technical and service-oriented considerations for privacy, and improves the challenge *Data Aggregation.* The second discusses user-centric considerations for privacy. The third discusses the organizational values, ethical, and strategic considerations for privacy, and improves the challenge *Device Ubiquity.*

Y.2066 also discusses security considerations for IoT systems. It identifies six requirements. They are 1) communication security, 2) data management security, 3) service provision security, 4) integration of security policies and techniques, 5) mutual authentication and authorization, and 6) security audit.[120] These requirements capture most aspects of the IoT security picture and improve the challenges *Business Models*, *Data Aggregation*, *Device Ubiquity.* However, these requirements also use a prescriptive approach that does not differentiate between use-contexts or domains, therefore harming the challenges *Dynamic Contexts*, *Standards Saturation*, and *Accountability.*

While Y.2066 creates an effective general operational framework for IoT services that includes privacy and security tenets, it is by no means perfect. A recent review of ITU-T's IoT standardization activities revealed seven requirements for an IoT system where Y.2066 currently falls short.[123] Of those seven, four relate specifically to IoT privacy and security considerations. They are 1) A trustable and reliable infrastructure; 2) Service-aware, data-aware, and user-centric networking; 3) Auto-configurable and remotely controllable devices and services; and 4) Open application programming interfaces. This list demonstrates that the Y.2066 standard does not focus on user-centric risks or harms. Therefore, this standard does not do anything to address user-centric challenges such as *Information Asymmetry*, *Information Scope*, *Psychological Biases*, *Economic Incentives*, or *User Knowledge.* Y.2066 is an operational standard that applies across IoT domains. However, it is still general and only provides basic privacy and security considerations.

5.3.3 Conclusion

ITU-T's IoT recommendations are, for the most part, broad and oriented towards unspecified operational values. This standardization style is not necessarily negative. It allows stakeholders who adopt this standard to adjust to their own domain's needs and requirements. Further, it helps standardize operational and organization choices across domains, which can help reveal areas for collaboration and applicable best practices and policies. However, in order for such a standardization style to be functional, it requires additional standards that are focused, technical, and geared towards applicable best practices and policies by domain and use-context. Therefore, ITU-T's standards cannot stand by themselves and require other standards to provide more domain- and stakeholder-specific recommendations. Table 5.2 maps the ITU-T IoT standards case study to the MoC analysis framework. As one can see, the domain applicability is broad due to the lack of a clear domain focus. Further, the stakeholders with power are also broad with most power centralized around the actual standard developer. Overall, while it is clear that such operational standards can be effective at addressing some IoT privacy and security issues, it is also clear that such a standardization style requires a more narrow scope with specific best practices.

Table 5.2: Domains covered, stakeholder power, and challenges impacted by the ITU's Y.2060 and Y.2066 standards.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Data Brokers (+)	Accountability (+/–)
Domestic	Developers/Manufacturers (+)	Business Models (+)
Education	SDOs (+++)	Data Aggregation (+)
Entertainment	Service Providers (+)	Device Capability (+/–)
Finance	Testing/Cert. Vendors (++)	Device Ubiquity (+)
Government		Dynamic Contexts (+/–)
Healthcare		Slow Legislation (+)
Infrastructure		Solution Costs (–)
Insurance		Standards Saturation (–)
Manufacturing/Trade		User Knowledge (+)
Public Safety/Defense		
Retail/Hospitality		
Telecommunications		
Transportation		
Workplace		

5.4 Operational Standards Conclusion

The IoT operational standards, characterized best by the work from ISO/IEC and ITU, offer solutions to a number of the key IoT challenges, apply to several IoT stakeholders, and have the *ability* to operate in numerous IoT domains. However, the most important conclusion to draw from the IoT operational standards case studies is the market saturation and the over-broad nature of the most well-known standards. This fact results in a market of hundreds of competing standards that apply in broad and general ways to address privacy and security challenges.

In a sense, the operational standards available in the IoT realm are sufficient in covering large-scale operational considerations such as how to build an IoT system and the general privacy and security considerations necessary for the first steps of such a system. The major challenge still faced by these standards is the realization that IoT is more complex than a single domain. Each individual operational domain has special considerations. For example, the ISO/IEC 27k series is less effective for many domestic services since many of those companies are too small to incur the certification costs.

ITU's set of IoT recommendations provides widely applicable privacy and security solutions. However, that generality is also its undoing. ITU's recommendations are not domain-specific. In order to provide effective privacy and security controls, domain- and use- specific recommendations must be provided on top of the ITU standards. The challenge with large-scale operational standards is that if they fail to consider the differences between IoT domains and use cases, they can potentially introduce more harms to privacy and security by failing to address all privacy and security harms and risks related to specific domains and uses. Both of the case studies in this chapter led to the same final conclusion: the operational standards MoC is currently characterized by systems that lack narrow scope and domain- and use-specific best practices, yet still provide a beneficial first pass at addressing IoT privacy and security challenges.

Chapter 6

Technical Standards

6.1 Introduction

This section reviews two of the largest and most popular IoT technical standards projects currently in the market: The 3rd Generation Partnership Project (3GPP) and oneM2M.[1]

Technical standards of all sorts rely on a *reference architecture* for the technology they specify. There is no such widely accepted architecture for IoT. As discussed in Chapter 1.2.2, a number of IoT stakeholders have proposed IoT reference architectures, though none has been universally accepted.[2] However, the proposed IoT

[1] I selected these two IoT technical standards projects due their prevalence in IoT and M2M literature, as well as their perceived completeness, popularity, and success in the marketplace. The most important reasons I chose 3GPP and oneM2M is the fact that they are both collaborative technical standards processes.[168][169] In other words, they represent a combination of multiple narrow technical standards and relate to large swaths of IoT technology development and use cases. Under the constraints of a reasonable thesis, it would be inappropriate to review all the narrow and technology-specific technical standards related to IoT privacy and security. There are thousands of such standards and the scope is too broad. Therefore, I acknowledge that 3GPP and oneM2M are by no means the only technical standards available. However, they do represent the best that the market currently has to offer. Therefore, they are ideal subjects for a case study on current technical standards related to the IoT ecosystem. For complete surveys on narrow technology-specific IoT standards, though not specifically in the context of privacy and security, please see [43], [80], [153], and [168].

[2] A full discussion of IoT reference architectures is beyond the scope of this thesis. For more information on IoT reference architectures, please see [2], [55], [120], [137], [153], [196], and [222]. Each of these works proposes an IoT reference architecture or uses a pre-existing IoT reference architecture to demonstrate IoT uses, benefits, or risks. Further, for a complete market review of all available IoT reference architectures, please see [201] and [113]. An IoT reference architecture is a research focus worth further investigation and standardization.

architectures share common core characteristics that can be distilled into four layers – **application**, **service**, **networking**, and **device**.[3][101][120][222]

All IoT systems operate on these four layers, and therefore technical standards must address all four in order to be operational and effective MoCs.[4] No single technical standard addresses all four layers. However, 3GPP operates on the networking and device layers, and oneM2M operates on the application, service, and device layers. Therefore, all four layers are covered by these two case studies.

6.2 3GPP

6.2.1 Mission and Structure

3GPP started as a strategic business collaboration between AT&T Wireless and Nortel Networks in 1998. It has since morphed into an industry leading SDO and governance collaboration for developing the future wireless communications and internet network. It applies to large-scale IoT communication and networking technologies since it seeks to support IoT technologies and service on top of broadband mobile networks.[168] It is interesting to note 3GPP's desire to standardize IoT technical specifications on top of its mobile network technologies. While some IoT applications certainly apply to a mobile cellular network, to include monthly subscription and connection fees, it is unlikely that all IoT technologies will rely on such a system. Therefore, there is a question regarding the scope of the 3GPP standards and if they will only impact a small subset of the IoT ecosystem. However, that does not deter 3GPP from *attempting* to expand their power within the IoT ecosystem. 3GPP's incentives towards consolidating power under the mobile cellular model has the potential to damage *Solution Costs* and *Dynamic Contexts* by forcing IoT systems into a privacy and security architecture not designed for their specific use.

3GPP specifications cover the entirety of cellular telecommunications technologies, including radio access, the core transport network, service capabilities, codecs,

[3] See Chapter 1.2.2.

[4] For a complete case study regarding how these layers interact in an IoT system, see [102].

security, and quality of service.[176] The actual standardization activities are split between three Technical Specification Groups (TSGs)–**Radio Access Networks (RAN), Services & Systems Aspects (SA), and Core Network & Terminals (CT)**. While each TSG has their hands on an aspect of the IoT that impacts privacy and security, only SA has the defined responsibility of providing privacy and security controls.[5]

6.2.2 Privacy and Security Controls

According to their website, SA

> "has the overall responsibility for security and privacy in 3GPP systems [. . .] will perform analysis of potential threats to these systems. Based on the threat analysis [. . .] will determine the security and privacy requirements for 3GPP systems, and specify the security architectures and protocols [. . .] will ensure the availability of any cryptographic algorithms which need to be part of the specifications [. . .] will accommodate, as far as is practicable, any regional regulatory variations in security objectives and priorities for 3GPP partners [. . .] will further accommodate, as far as is practicable, regional regulatory requirements that are related to the processing of personal data and privacy."[177]

This description is rather promising. It signals that the 3GPP considers privacy and security as a crucial part of the implementation and design process for new technologies. This process is called *privacy and security by design.* Further, the actual process they use, as described by this mission statement, is also encouraging. They start by characterizing the threat and risk to individual systems. They do not just create a blanket policy that covers all systems. Instead, they strive to tailor privacy and security controls to a system's needs, improving the challenges *Dynamic Contexts* and *Device Capability.* Further, they also provide solutions for regulatory and legal

[5] SA coordinates across the three TSGs in order to define the architecture and service capabilities of 3GPP-based systems and specifications. It also is specifically responsible for network management and the creation of security frameworks and security reviews for the entire 3GPP system.[178] This group is essentially the systems engineering task force for 3GPP, and therefore the logical authority on integrating privacy and security measures in the 3GPP IoT architecture.

requirements. This provision suggests that 3GPP will maintain its effectiveness in a more prescriptive regulatory environment than what currently exists, improving the challenge *Regulation Uncertainty.*

In terms of 3GPP's technical endeavors that relate to IoT privacy and security, 3GPP has also conducted work on proximity based services (ProSe) and single sign-on (SSO) frameworks. ProSes are case studies on context-specific service considerations. Context-specific privacy and security requirements are a fundamental requirement for the future of IoT privacy and security and are the first pillar of my recommendations in Chapter 9.[43] SSOs involve identity management and authentication, access control frameworks (such as third party services and access to data) and authorization, and user preference management (such as when and what types of information can be collected). In terms of IoT privacy, such frameworks are fundamental to a privacy-enhancing system because they take a risk-based perspective on correcting for privacy harms, the second pillar of my recommendations in Chapter 9.

6.2.3 What 3GPP Offers and What It Needs

A recent 3GPP review determined that the 3GPP standards do not currently provide effective controls in the areas of reduced device complexity, improved battery life and longevity, coverage improvement, user ID and control, service exposure and service support.[168] These areas for future 3GPP development map directly to the IoT privacy and security challenges *Device Capability*, *Device Ubiquity*, *Accountability*, *User Knowledge*, and *Business Models.* The same study mentions privacy in regards to ensuring services do not link "exposed network information" with "private user/subscriber information," and issue related to the challenge *Dynamic Contexts.*[168] Further, the study notes that private information such as location and identity data does not currently have reasonable safeguards under current 3GPP implementations. These results were validated by a second study that identified support for low-cost and low-complexity devices, enhancing device and network coverage, improving device power consumption, and enhancing the system architectures to better support services as areas for future 3GPP improvement.[102]

The most privacy and security supporting function of 3GPP is their focus on making all 3GPP releases, specifications, standards, and systems fully backwards and forwards compatible. This function is a key tenet of improving the challenges *Business Models*, *Accountability*, and *Device Capability*. For example, their work on LTE and LTE-Advanced has prioritized the ability for an LTE-A terminal to work on an LTE cell and an LTE terminal to work on an LTE-A cell.[176] This value is crucially important for IoT operations in domains such as transportation, manufacturing, and government where infrastructure is expected to last decades. It suggests that 3GPP accepts accountability for the continued life-span support for technologies, organizes their business model around the idea that systems should maintain availability–to include privacy and security–in reasonable perpetuity, and that current device capabilities should not restrict the future development and improvement of the entire system network and architecture.

6.2.4 Conclusion

Table 6.1 maps the 3GPP IoT technical standardization endeavors to the MoC effectiveness framework. 3GPP does not yet offer domain-specific IoT standards or frameworks. However, they are structured as an organization to do so. Further, the 3GPP-SA guiding vision suggests that their values and philosophy as an SDO are aligned with the belief that *different* IoT domains may require *different* standards and considerations that incorporate privacy and security controls. At the same time, 3GPP's incentives as the mobile cellular standardization body might cause their IoT standards to be less effective in domains that do not require the cellular architectures. Further, as a widespread and well-established SDO, 3GPP has the power and the potential to significantly impact IoT technical standards.

In terms of 3GPP's impact on IoT privacy and security challenges, it is clear that 3GPP provides a framework and an organizational structure that embraces organizational policies that improve privacy and security (*Accountability*, *Regulation Uncertainty*, *Standards Saturation*, and *Business Models*), as well as technical considerations that improve privacy and security (*Device Capability* and *Dynamic Contexts*).

However, uncertainty does exist regarding 3GPP's effectiveness and scope across all IoT domains that potentially damages *Dynamic Contexts* and *Solution Costs*.

Table 6.1: Domains covered, stakeholder power, and challenges impacted by the 3GPP technical standardization initiatives.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Developers/ Manufacturers (+)	Accountability (+)
Domestic	SDOs (++)	Business Models (+)
Education	Service Providers (+)	Device Capability (+)
Entertainment	Testing/Cert. Vendors (++)	Dynamic Contexts (+/–)
Finance		Regulation Uncertainty (+)
Government		Solution Costs (–)
Healthcare		Standards Saturation (+)
Infrastructure		
Insurance		
Manufacturing/Commerce		
Public Safety/Defense		
Retail/Hospitality		
Telecommunications		
Transportation		
Workplace		

6.3 oneM2M

6.3.1 Mission and Structure

Founded in 2012 by seven SDOs to ensure global alignment of M2M standards, oneM2M intends to standardize a common service layer platform for M2M. The organization has a close working relationship with technical and operational SDOs like ITU, industry alliances like OMA and BBF, and internet standardization bodies like the IETF.[80] Since its inception, it has released two sets of comprehensive IoT and M2M service and architectural standards (Release 1 was distributed in 2015 and Release 2 was distributed in 2016). Their operations and efforts to develop IoT standards are ongoing and continual. So far, the standard has been succesfully implemented in **Application**, **Service**, and **Network** layer technologies.[165]

The most recent release included 27 individual specifications. Of those 27, the eight related to IoT privacy and security are:[6]

1. TS0001 Functional Architecture - *Sections:* Security Concepts, Security Procedures, Trust Enabling Architecture, M2M Communication Models, Device Management
2. TS0002 Requirements - *Section:* Security Requirements
3. TS0003 Security Solutions - *Sections:* All
4. TR0001 Use Cases - *Sections:* Personal Data Management Mechanism Based on User's Privacy Preferences, Terms and Conditions Markup Language for Privacy Policy Manager, All case studies include security
5. TR0008 Security - *Sections:* All
6. TR0012 oneM2M End-to-End Security and Group Authentication - *Sections:* All
7. TR0016 Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies - *Sections:* All
8. TR0018 Industrial Domain Enablement - *Section:* Security Analysis

Therefore, it is clear that oneM2M's technical standards have a significant impact on IoT privacy and security. From these specifications, it is clear that oneM2M has a positive impact on *Accountability*, *Business Models*, *Data Aggregation*, *Device Capability*, *Device Ubiquity*, and *Dynamic Contexts.*

oneM2M has three high-level goals: 1) To clarify the uncertainty in IoT standards by decreasing the market fragmentation regarding service layer standards, 2) To develop and manage a common service layer architecture that supports network-agnostic services and functions that use the full store of pre-existing M2M systems and technologies, and 3) To define and design common IoT interfaces and APIs for devices, gateways and infrastructure nodes. Goal 1 seeks to resolve the IoT privacy and security challenge *Standards Saturation.* Goals (2) and (3) relate specifically to finding the similarities between IoT domains in the interface, service, and device technical layers, and implementing the best privacy and security practices and solutions

[6] A complete list of these specifications can be found in Appendix D and the documents themselves can be found at [166]

for each layer, improving *Dynamic Contexts* and *Device Ubiquity*.

6.3.2 Architecture

The practical effect of oneM2M, evident in the standards and goals proposed by the initiative, is the creation of a single IoT service platform that is applicable and implementable across IoT domains. It accomplishes this effect through system and layer abstractions, much like what SDNs do for data center architectures. The oneM2M framework is organized into 3 layers:[80]

1. The Application Layer (AL) that includes all M2M Application Entities (AE),
2. The Common Services Layer (CSL) that includes functions of the oneM2M architecture and services, AKA Common Service Functions (CSFs). Related CSFs are divided into Common Service Elements (CSEs).
3. The Network Services Layer (NSL) that includes an abstraction of the network infrastructure and describes network capabilities through Network Services Entities (NSEs).

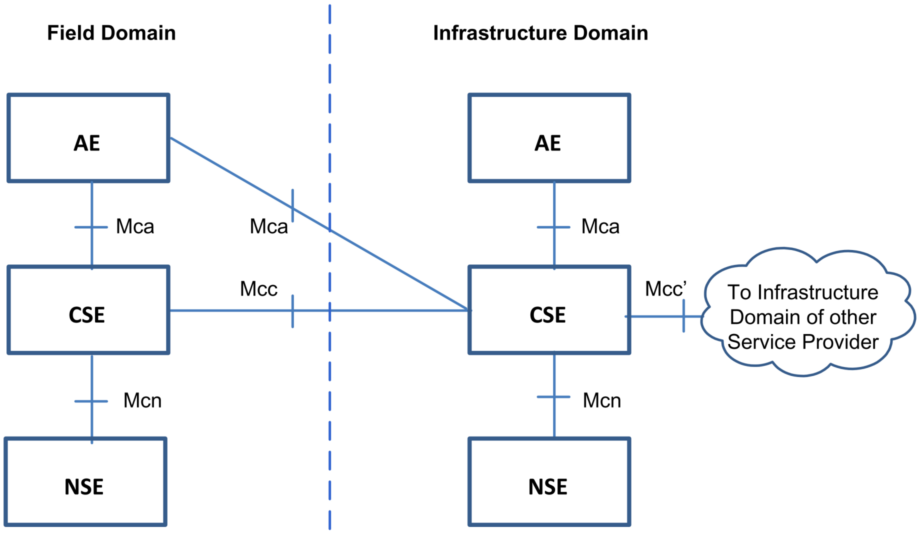


Figure 6-1: oneM2M functional architecture for IoT systems.[7]

As one can see in Figure 6-1, this technical architecture does not prescribe specific

[7] Found in [164].

technologies for IoT and M2M applications and services.[8] Instead, it provides an abstracted structure for devices, services, interfaces, and their interactions. It does not prescribe privacy and security solutions that are supposed to fit every IoT domain. Instead, it specifies all interactions taking place over the oneM2M reference points on the basis of a request-response pattern with standard privacy and security goals.[166]

6.3.3 Privacy and Security Controls

A comprehensive review of each part of the oneM2M architecture is beyond the scope of this thesis.[9] However, there are individual parts of oneM2M within the scope of this case study that support the ideals of IoT privacy and security. The best layer to consider IoT privacy and security controls is the Common Services Layer (CSL) due to the defined and operationalized Common Service Functions (CSFs). Many of these CSFs relate to IoT privacy and security. Below is a list of key CSFs and how they each relate to privacy and security and which challenges they improve.[164]

1. **Application and Service Layer Management:** Configuring, troubleshooting, and upgrading functions and applications relevant to the service - necessary in order to include and develop new security features as well as implementing policies in the architecture. *Business Models*, *Device Capability*, *Device Ubiquity*.
2. **Registration:** A form of entity identification and role management, allows for processing a registration request from an AE or another CSE to allow the registered entities to use the services offered by the Registrar CSE. Implementing security procedures here would impact who can use data-driven service and in what ways. *Business Models*, *Accountability*, *Economic Incentives*.
3. **Communication Management/ Delivery Handling:** Decides when to use which communication connection to deliver information - conducted based on predetermined policies and delivery handling parameters that can be specific to each request for communication, which should include privacy preferences and security procedures. *Business Models*, *Device Capability*, *Dynamic Contexts*.

[8] For the purposes of this review, the communications modes Mca, Mcc, and Mcn are irrelevant. Please see [164] for a more detailed discussion of this architecture.

[9] For more comprehensive reviews of the oneM2M architecture and process, please see [57], [80], [102], [113], and [169].

4. **Group Management:** Responsible for managing group membership and bulk operations supported by the group. In this context, a group is a set of interconnected systems or devices. When adding or removing members to/from a group, validates whether the member complies with the policies of the group. Bulk operations include read, write, subscribe, notify, device management, etc. Relevant to the creation of trusted networks of devices and services based on security and role policies. *Accountability*, *Device Capability*, *Data Aggregation*, *Dynamic Contexts*.
5. **Security:** Has five sub-functions–Sensitive data handling; Security administration; Security association establishment; Access control including identification, authentication and authorization; Identity management - and is specifically tailored to implement and support all predetermined privacy and security policies within a system. *Accountability*, *Business Models*, *Data Aggregation*, *Device Capability*, *Dynamic Contexts*.
6. **Data Management & Repository:** Provides data storage functions including the aggregation of large amounts of data, converting this data into a specified format, storing it for processing and analysis, and providing controls for data accessibility. These functions, and their implementation, are entirely dependent on privacy and security choices. *Accountability*, *Business Models (+/–)*, *Data Aggregation (+/–)*.

6.3.4 What oneM2M Offers and What It Needs

A recent and comprehensive review of oneM2M discusses how the standardization group not only creates their own standards for IoT services, but also works in collaboration with other SDOs and IoT standardization groups in order to create a comprehensive IoT standard applicable across IoT domains.[169] For example, oneM2M has collaborated with SDOs such as ITU-T, Open Mobile Alliance (OMA), and Broadband Forum (BBF) by including the oneM2M architecture into other groups' frameworks (ITU-T SG20 and IEEE P2413) or by including existing standards and architectures into the oneM2M service layer architecture (OMA Device Management protocol and BBF TR-069).

Further, oneM2M also recognizes the importance of developing standards within different IoT domains and has worked specifically with the Home Gateway Initiative (HGI), an SDO for IoT domestic systems, and IEEE P2413, an IoT standard architecture for the healthcare, transportation, and manufacturing domains. While these two initiatives only target two of the many IoT domains, oneM2M's work demonstrates the popular perspective that IoT architectures and use cases are fundamentally split between IoT domestic and IoT industry.[10] While this thesis argues that such a general split is incomplete, it represents the right mindset. It suggests that oneM2M is looking towards implementing standards that are more focused to individual IoT domains. Finally, oneM2M also works to coordinate between multiple IoT connectivity standards to develop cross-device, cross-technology, and cross-network compatibility with groups like the Open Connectivity Foundation (OCF) and 3GPP.

While each of these activities do not specifically target IoT privacy and security improvement, they do have inherent implications in the development of IoT privacy and security functions. First, oneM2M is committed to the idea of an adaptable and malleable framework that can be morphed, adjusted, and implemented as needed across the various IoT domains. A recent study demonstrates that adaptability by outlining two case studies, one in the infrastructure domain and another in transportation domain, that both use the oneM2M service architecture.[102] There is enough leniency and flexibility in oneM2M's system that each separate IoT domain can determine the best implementation for their domain-specific services.

Second, oneM2M is also dedicated to collecting and coordinating with other projects that have determined best practices, best policies, and best architectures for IoT technologies and services. They do not purport to re-invent the wheel, and they rely heavily on pre-existing successes and collaborations. This fact allows oneM2M to absorb work completed by others, such as more domain-specific controls and architectures for protecting data privacy and information security. For example, if an academic research group were to develop a clear set of best practices, privacy policies, security features, and a complete privacy and security architecture for IoT transportation, oneM2M adapt its published standards to include such work. Therefore, not only is the functional oneM2M architecture driven towards improving IoT privacy and security, but so is oneM2M's operational structure. This adaptable structure

[10] This concept was discussed in more detail in Chapter 2.1.

helps improve the challenge *Slow Legislation*.

6.3.5 Conclusion

Table 6.2 maps oneM2M to the MoC analysis framework. From this case study, we can conclude that oneM2M is an adaptable technical standards process with immense potential to improve IoT privacy and security on the application, service, and device layers. The oneM2M process also suggests its openness to incorporating more domain-specific standards under a common framework and reference architecture. While oneM2M is still a budding SDO, its approach to designing and implementing technical standards makes it an effective MoC for future IoT privacy and security controls.

Table 6.2: Domains covered, stakeholder power, and challenges impacted by the oneM2M technical standardization initiatives.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Developers/ Manufacturers (+)	Accountability (+)
Domestic	SDOs (++)	Business Models (+/–)
Education	Service Providers (+)	Data Aggregation (+/–)
Entertainment	Testing/Cert. Vendors (++)	Device Capability (+)
Finance		Device Ubiquity (+)
Government		Dynamic Contexts (+)
Healthcare		Economic Incentives (+)
Infrastructure		Slow Legislation (+)
Insurance		Standards Saturation (+)
Manufacturing/Commerce		
Public Safety/Defense		
Retail/Hospitality		
Telecommunications		
Transportation		
Workplace		

6.4 Technical Standards Conclusion

The entire IoT technical standards ecosystem, represented by the two IoT technical standardization collaborations 3GPP and oneM2M, are both promising frameworks in terms of improving IoT privacy and security. Between them, they target all four layers of the IoT technical architecture. Further, they both incorporate privacy and security tenets and values as a fundamental aspect of system design. Finally, they also both support the idea of IoT domains and the need to provide separate privacy and security solutions for each domain. While neither offer specific privacy and security solutions and best practices for individual IoT domains–a significant fault in the IoT privacy and security MoC ecosystem–they are both structured in such a way that encourages the inclusion of such standards as they are made available. For example, oneM2M has already coordinates with HGI, an SDO for IoT domestic systems, and IEEE P2413, an IoT standard architecture for the healthcare, transportation, and manufacturing domains. Therefore, once more research has been conducted that demonstrates domain-specific considerations, oneM2M and 3GPP can incorporate those requirements within their frameworks and standards, thus improving overall IoT privacy and security.

Nothing to see here. Move along.

Chapter 7

Compliance Frameworks

7.1 Introduction

A number of compliance frameworks exist that apply to IoT privacy and security. Compliance frameworks often bridge operational and technical standards and provide a framework that companies can use to achieve standards compliance based on accepted industry best practices. Overall, they serve as de facto norms and best practices within an operational domain. In this chapter, I analyze four different compliance frameworks.

The first two frameworks, the Information Technology Infrastructure Library (ITIL) and the Control Objectives for Information and Related Technologies (COBIT), cover the topic IT management similar to the ISO/IEC 27k Series. ITIL covers IT service development and management. COBIT covers IT governance and responsibilities from a business perspective. The other frameworks, Capability Maturity Model Integration (CMMI) and The Open Group Architecture Framework (TOGAF), are focused on software and enterprise architectures. CMMI covers a company's services and capabilities. TOGAF covers the development of enterprise IT architectures for the purpose of designing services. Each of these compliance frameworks apply to the creation of IoT data services, and are currently used by some IoT developers, manufacturers, and service providers.

These are by no means the only compliance frameworks related to IoT privacy and security. Other major frameworks include the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the Business Information Services Library (BiSL), and the Project Management Body of Knowledge (PMBOK). In fact, there are more than one hundred such frameworks, though many are too broad and insufficiently documented to be considered effective.[172] The four frameworks I selected provide a representative sample of the types of goals, processes, controls, styles, and compliance scopes found in the most successful compliance frameworks that relate to information privacy and security within the IoT domains.[1]

7.2 The Information Technology Infrastructure Library (ITIL)

ITIL is a best practices framework for IT Service Management (ITSM) systems. ITSMs include a company's information technology policies and procedures, as well as the designing, delivering, and operating of IT services offered to customers. Therefore, ITIL applies to the application and service layers of the IoT ecosystem.

ITIL captures the "life-cycle perspectives on service strategy, design, transition, operation, and continuous improvement."[221] It is the most widely accepted and used of such ITSM frameworks.[19][103][173] It applies to both private sector and public sector entities. For example, it has been used by organizations such as Shell, Hewlett Packard, IBM, NASA, Microsoft, and Disney.[175] ITIL also covers the entire set of operational IoT domains. The similarity between ITIL compliant organizations is their market power and scope of operations, not operational domains or use-contexts.

[1] Compliance frameworks are marketplace signals. The certification under a compliance framework serves as a badge to other organizations, users, and stakeholders that the certified organization has achieved a sufficient level of standardization or de facto best practices and norms. The theory of network effects means that the most popular compliance frameworks serve as the strongest signals. As such, I have chosen four of the most popular compliance frameworks in the realm of IoT data services. Therefore, the case studies in this chapter represent a reasonable overview of the available compliance framework MoCs.

7.2.1 Effectiveness

The intent of ITIL is split into the following twelve goals:[175]

1. Manage business risk for your services.
2. Minimize service disruption.
3. Quantify and clearly demonstrate the true value of the services you provide.
4. Benchmark services and maximize return on investment.
5. Obtain value for money from your service providers.
6. Support the marketing and consumption of your services.
7. Ensure the quality of services matches customer needs and expectations.
8. Ensure your customers can use the services when and where needed.
9. Ensure the business and your customers are not affected by unexpected service failures.
10. Forecast, respond to and influence the demand for your services in a cost effective way.
11. Support business change at the speed your customer needs while ensuring stable and low-risk environment.
12. Build and maintain positive business relationships with customers and improve customer satisfaction.

These goals cover three topics: service operations (**goals 1, 2, 6, 7, 8, 9, and 10**), business concerns (**goals 1, 3, 4, 5, 6, 9, 10, and 11**), and user concerns (**goals 3, 7, 8, 9, 10, 11, and 12**). This structure suggests that ITIL is a service-oriented framework that takes a business operations and user-oriented approach to create usable, effective, and secure IT systems. Therefore, ITIL does address the challenges *Business Models* and *Accountability*. **Goals 1, 2, 7, 8, 9, and 11** all influence the challenge *Economic Incentives* by attempting to align the business' incentives with those of their customer.

Some researchers in the ITSM realm have lauded ITIL's structure and applicability across domains. Specifically, two separate groups have used the ITIL framework to develop comprehensive compliance structures based on ITIL controls. In one, researchers developed a framework that uses ITIL to define organizational strategies for companies that rely on data services similar to those offered by IoT technologies – demonstrating ITIL's ability to address the challenge *Business Models.*[187] Another group utilized ITIL to implement IT security controls that achieve compliance under large federal regulations such as Sarbanes-Oxley – demonstrating ITIL's ability to somewhat resolve the challenge *Regulation Uncertainty.*[100]

While all of these cases support the idea that ITIL can apply across IoT domains, there are confounding factors yet to be addressed that limit its effectiveness for IoT privacy and security. First, ITIL does not address the engineering and design of systems. If the architecture and software are designed with poor privacy and security principles, ITIL can only do little to improve those systems. Therefore, ITIL compliance might actually exacerbate the challenges *Business Models* and *Device Capability* if applied to poorly designed systems.

Second, the ITIL certification process is costly and time-consuming. This fact exacerbates the IoT privacy and security challenge *Solution Costs.* Many organizations that start the process fail to achieve compliance.[142] Just like ISO/IEC 27001 certification, the cost of ITIL certification is prohibitive. In order to achieve the **Expert** certification level, it requires between 200-350 hours of commitment and costs \$35-40k online and \$55-60k in the classroom.[2][197]

ITIL adoption statistics reveal similar trends. A number of studies exist that reveal ITIL adoption rates by various stakeholders within key domains and use-contexts. One study in the EU showed an adoption difference between developed economies (e.g. Germany) and transitioning economies (e.g. Poland), with higher instances of successful adoption in developed economies.[224] While this might bode well for IoT companies located within the U.S., a number of small IoT developers, producers, and

[2] The **Expert** certification is the 4th of 5 certification levels, and necessary for the certified organization to be considered knowledgeable and compliant in the entirety of ITIL.

vendors in domains such as domestic are based in transitioning economies.[107]

Another study conducted in Brazil revealed that organizations that adopt ITIL tend to also adopt COBIT, a result that corroborated three previous studies on the same subject.[3][60] This result suggests that companies who wish to achieve market competitiveness and state-of-the-art status for their IT systems must receive certification under both frameworks, further inflating *Solution Costs*.

Finally, two studies reveal that ITIL is actually limited in its adoption across domains. One study demonstrates high levels of adoption in finance, management, and telecommunications domains, with much lower adoption in the public sector and education.[142] The same study further concluded that ITIL compliance tends to apply well in large, customer-oriented, profit-centric organizations. Another study also revealed low adoption rates in healthcare.[93] Therefore, we can conclude that ITIL for IoT might apply well in the same domains with already large adoption rates such as finance and telecommunications.

ITIL, while a proven and effective information systems development framework, is still missing a few key characteristics. Table 7.1 maps ITIL to the MoC analysis framework. This case study has shown that ITIL relies on pre-existing systems and therefore does not encourage privacy and security by design. Further, ITIL effectiveness is not independent of business size, location, or domain. It is costly to implement and not applicable for small organizations or those in transitioning economies. In practice, ITIL adoption is limited to large, customer-oriented and profit-centric organizations. Therefore, it does not apply to domains such as government. ITIL does provide some privacy and security controls for IoT domains such as finance, entertainment, and hospitality; however, it also has the potential to exacerbate a number of key challenges such as *Business Models*, *Device Capability*, and *Solution Costs*.

[3] One was published by Gartner Inc. in 2002 [149], one was published by the Hewlett-Packard Company in 2004 [188], and the final was published in Europe in 2006 [33].

Table 7.1: Domains covered, stakeholder power, and challenges impacted by ITIL.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Data Brokers (+)	Accountability (+)
Domestic	Developers/ Manufacturers (+)	Business Models (+/–)
Entertainment	SDOs (++)	Device Capability (–)
Finance	Service Providers (+)	Economic Incentives (+)
Infrastructure	Testing/Cert. Vendors (+++)	Regulation Uncertainty (+)
Insurance		Solution Costs (–)
Manufacturing/Trade		
Public Safety/Defense		
Retail/Hospitality		
Telecommunications		
Workplace		

7.3 Control Objectives for Information and Related Technologies (COBIT)

COBIT is an IT governance, management, and responsibilities framework designed to address ITSM systems on the business side of operations.[128] Therefore, it addresses the IoT privacy and security challenges *Business Models* and *Accountability*. IT governance, the driving tenet of COBIT, "ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives."[128] Therefore, it also attempts to improve the challenge *Economic Incentives* by aligning the incentives, goals, and needs of system stakeholders.

7.3.1 Effectiveness

The most recent version has five primary operational goals. As one can see, these goals are framed around business values such as profit, cost reduction, and risk:

1. Audit and assurance: Manage vulnerabilities and ensure compliance.
2. Risk management: Evaluate and optimize enterprise risk.

3. Information security: Oversee and manage information security.
4. Regulatory & compliance: Keep ahead of rapidly changing regulations.
5. Governance of enterprise IT: Align IT goals and strategic business objectives.

Goal 1 addresses the potential vulnerabilities (cyber, liability, etc.) that IoT technologies add to a company's infrastructure. One program under this goal is actually based on NIST's Cybersecurity Framework.[4][110] As such, it targets the challenges *Business Models*, *Dynamic Contexts*, and *Accountability.*

Goal 2 addresses the risks associated with IoT technologies by providing mechanisms to identify, quantify, and managing those risks as they affect a specific business' operations.[109] As such, it targets the challenges *Economic Incentives* and *Slow Legislation.*

Goal 3 addresses the security of IoT data and information, and provides controls to limit security incidents while maintaining cost-effectiveness.[108] As such, it targets the challenges *Data Aggregation*, *Device Capability*, and *Accountability.*

Goal 4 addresses uncertainty in future regulations for IoT privacy and security, as well as the concerns that IoT regulations will limit innovation and decrease profitability. It includes specific controls regarding data retention and disposal.[140] As such, it targets the challenges *Regulation Uncertainty*, *Slow Legislation*, and *Standards Saturation.*

Goal 5 addresses the primary benefit that IoT promises to serve: increased efficiency and operational success as related to specific companies' needs and strategic goals. Therefore, it is clear that COBIT can apply to IoT domains that involve private enterprise, as it takes a functional and cost-oriented approach to managing IT infrastructure. As such, it targets the challenges *Accountability* and *Economic Incentives.*

COBIT 5 has been operationalized as an information security mechanism for or-

[4] I do not specifically discuss the NIST Cybersecurity Framework in this thesis because it has been analyzed in extenso. However, it is important to acknowledge the NIST Cybersecurity Framework as a first-of-its-kind policy framework that created a common taxonomy for cybersecurity and identified a significant set of highly-generalized best practices. Further, it has been the target of numerous legitimate critiques, chief of which is the fact that it somehow manages to be both too complicated for high-level implementation and too broad for effective operational guidance.[15]

ganizations that rely on information resources and data-rich technologies like IoT. In a complete case study published in 2015, it was determined that COBIT 5 provides information security guidance that is “complete, consistent and easily navigable,” uses a control mechanism that “promotes access to information, functionality and user satisfaction” and contributes to a final result that “provides users with the foundational tools to protect information.”[128]

However, COBIT 5 is incomplete and misses some key aspects of IoT privacy and security. First, it is important to declare what COBIT 5 actually accomplishes. COBIT 5 ensures compliance with regulations, management of business risks, and compliance with internal enterprise policies. Further, it accomplishes information security controls through reactive indicators. For example, it would consider the number of security incidents that have caused financial loss or public embarrassment in the past, and attempt to correct for the same specific service risks in the future. The problem with this approach is that it assumes that data is specific to a single service or function. Therefore, it only applies privacy and security considerations to specific applications and processes instead of applying privacy and security considerations to data use, contexts, and communications. Therefore, COBIT exacerbates the challenges *Device Ubiquity* and *Dynamic Contexts*.

IoT technology promises to move data, and the borders of security, far beyond the internal applications and processes of a company. Privacy and security controls must be developed to target not only systems, but also the harms that those systems create. For example, the data itself is not the only factor that creates risk and harms. The use and movement of that data can create risk and harms. Therefore, the primary issue with COBIT 5 is its reactivity and narrow systems focus.[204] The IoT ecosystem requires proactive privacy and security by design that considers use-contexts. This practice requires well-considered and specific harms analysis for various IoT domains and operational use cases that COBIT does not provide.

COBIT is a fascinating and useful framework because, unlike most other compliance frameworks, it addresses the primary concerns of private enterprise in the context of information security: profit, cost reduction, and risk. Table 7.2 maps COBIT to the MoC analysis framework. COBIT is an umbrella-like framework that combines operational best practices with governance and business requirements without domain specificity. While it does apply to many operational privacy and security challenges across domains, it is a reactive framework. The biggest limitation of COBIT 5 is that it does not take a holistic view of data privacy and security. It provides controls and mechanisms to review potential risky endeavors and systems within an organization, but it fails to consider the actual data use as a potential for risk.

Table 7.2: Domains covered, stakeholder power, and challenges impacted by COBIT.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Data Brokers (+)	Accountability (+)
Domestic	Developers/ Manufacturers (+)	Business Models (+)
Education	SDOs (++)	Data Aggregation (+)
Entertainment	Service Providers (+)	Device Capability (+)
Finance	Testing/Cert. Vendors (+++)	Device Ubiquity (–)
Government		Dynamic Contexts (+/–)
Healthcare		Economic Incentives (+)
Infrastructure		Regulation Uncertainty (+)
Insurance		Slow Legislation (+)
Manufacturing/Trade		Solution Costs (–)
Public Safety/Defense		Standards Saturation (+)
Retail/Hospitality		
Telecommunications		
Transportation		
Workplace		

7.4 Capability Maturity Model Integration (CMMI)

CMMI aims to develop an organization's software quality by targeting the various processes related to software and service development. It is often used in large-scale international organizations, especially those involved in Department of Defense contracts and financial operations, such as Lockheed Martin, Northrop Grumman IT, and JPMorgan Chase & Co.[7] It involves five maturity levels for certification, and each includes a set of required processes that represent specific service-oriented goals.

7.4.1 Effectiveness

The five maturity levels are operationalized across eight focus areas:[104]

1. Project and work management: enables teams to accelerate performance and complete strategic initiatives more efficiently and effectively.
2. Supporting infrastructure: ensures organizations control costs while defining and delivering reliable products and services.
3. Product engineering development: enables competitive-advantage by developing the right products and processes.
4. Data management: enables competitive advantage by finding the most effective use of today's massive amounts of data and optimizing the use of data assets.
5. Process management: enables efficient use of an organization's assets.
6. People management: Develops skills, builds teams, manages performance, and shapes the workforce to ensure organizational growth.
7. Service delivery and management: Ensures service delivery improvements and effective service performance.
8. Supplier management: Builds procurement capabilities in order to manage suppliers efficiently and effectively.

While information privacy and security is not an explicit category, it is incorporated in almost all of the focus areas. **Focuses 1, 3, 5, 6, 7 and 8** all address the challenge *Solution Costs* by creating value through efficiency and constant process improvements. **Focus 2** addresses the challenge *Device Capability* by targeting the actual products and services offered by a company. **Focus 4** has the potential to either improve or damage the challenges *Business Models* and *Data Aggregation* depending on the organization and domain by allowing for broad uses of data and expanding the scope of data use needed to maintain competitive advantage. **Focus 7** addresses the challenge *Economic Incentives* by emphasizing the service and, therefore, the desires, goals, and needs of the service consumers.

Further, CMMI also utilizes a “Security By Design” framework.[36] This additional framework includes processes such as product security risk management, security requirements engineering, security reviews, security testing, defect management, security validation, and secure coding.[36] Further, it addresses the challenge *Accountability* by describing an organization’s responsibility towards data privacy and proper information management. CMMI’s security standards are comprehensive, clear, and narrowly drawn to the design, development, use, and evolution of secure technology services like those offered by IoT. Further, CMMI is already utilized by companies within the IoT space such as Cognizant Technology Solutions, Neoway Technology, Brillio LLC, SolvIT Networks, Lockheed Martin, Honeywell, Booz Allen Hamilton, Minacs, and Kalkitech. These companies represent operations within the following IoT domains: telecommunications, manufacturing, finance, transportation, domestic, education, infrastructure, defense, retail, and government. Therefore, CMMI is applicable to nearly all IoT operational domains.

On a similar note, one study compared organizations’ perceptions of various IT compliance frameworks. It showed that not only is CMMI the best-known of such frameworks, it is also considered the most important instrument for providing business models, standards, and best practices for private organizations.[60] Therefore, between this fact and the “Security by Design” framework, it also improves the challenge *Business Models*.

CMMI has also been shown to benefit a company’s costs, schedules, productivity, service quality, customer satisfaction, and return-on-investment. For example, a technical report published in 2006 showed a median improvement over time of 34% for costs, 61% for productivity, 14% for customer satisfaction, and a median return-on-investment of 4:1.[82] Therefore, it addresses the challenges *Solution Costs* and *Economic Incentives*.

However, individual training for CMMI costs roughly $19k, organizational appraisal costs roughly $36-60k depending on the maturity of the organization, and full process development from start to finish costs roughly $125k in a single year.[37][38] These costs represent a significant barrier to improving IoT privacy and security since it negatively impacts the challenge *Solution Costs*. While long-term costs are shown to benefit the organization, short-term costs may be prohibitive for smaller organizations.

Table 7.3 maps CMMI to the MoC analysis framework. As a compliance framework, CMMI is focused on business management concerns. In doing so, it addresses a number of key IoT privacy and security challenges from the perspective of private stakeholders like developers and service providers. It creates an effective framework that applies to many areas of IoT privacy and security. However, there are two major effectiveness limitations. First, the framework is not domain-focused and also does not provide direction for any domain best practices. This structure has the potential to limit the effectiveness of the framework by requiring the compliant organization to develop their own privacy and security solutions. In practice, it seems that such a structure leads to a preemptive adoption of general best practices and de facto norms without much thought given to more advanced standards.[7]

Second, CMMI derives its value from improving existing business practices. It includes a "Security by Design" framework, but also balances those values with status quo operations. While this balancing is important for private enterprises to derive value from IoT systems and business models, it can also lead to potential privacy and security issues such as those derived from the challenges *Business Models* and *Data Aggregation*. Without directly addressing those challenges, such continuation of the IoT ecosystem status quo can lead to privacy and security risks and harms.

Table 7.3: Domains covered, stakeholder power, and challenges impacted by CMMI.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Data Brokers (+)	Accountability (+)
Domestic	Developers/ Manufacturers (+)	Business Models (+/–)
Education	SDOs (++)	Data Aggregation (+/–)
Entertainment	Service Providers (+)	Device Capability (+)
Finance	Testing/Cert. Vendors (+++)	Economic Incentives (+)
Government		Solution Costs (+/–)
Healthcare		
Infrastructure		
Insurance		
Manufacturing/Trade		
Public Safety/Defense		
Retail/Hospitality		
Telecommunications		
Transportation		
Workplace		

7.5 The Open Group Architecture Framework (TOGAF)

TOGAF is designed to help organizations develop enterprise software architectures and services. The body of the framework is centered on the *Architecture Development Method*, which is a continuous process that involves modularization, standardization, and the use of pre-existing and proven technologies. TOGAF is the de facto enterprise architecture standard available on the market today.[83] It is also generic enough to be tailored to most domains. For example, TOGAF has been used as 1) a dependability model for cloud-computing services [3]; 2) a security planning framework for enterprise architectures that maps technical and design decisions to business and policy decisions [59]; and 3) an operational efficiency, risk management, and IT governance framework for the use of IT services by local governments.[128]

7.5.1 Effectiveness

TOGAF functions on four operational levels: business, application, data, and technology.[103] **The business level** impacts the methods a company uses to meet strategic goals. **The application level** impacts the process by which specific technical applications and services are engineered, including information transfer and processing. **The data level** impacts the management and oversight of a company's digital and physical data resources. Finally, **the technology level** impacts the design, development, and oversight of the hardware and software infrastructure relied upon by a company's applications and data systems.[5]

TOGAF's intent is to operationalize industry norms and best practices across each of the four levels. While it does provide standard best practice guidance for architecture security, the set of goals contained by this guidance focus on the security of the organization and its business models.[59] Further, TOGAF does not provide any such guidance for privacy practices. These structural choices suggest that the framework is more focused on internal business practices than on consumer-oriented concerns. Therefore, it has a positive impact on the challenges *Accountability* and *Business Models*, and has minimal impact on any consumer-oriented challenges such as *User Knowledge*, *Information Asymmetry*, and *Psychological Biases*.

TOGAF accomplishes its goals through a process with nine recursive stages. As one can see, these stages rely on the specific organization's concerns and strategies. Therefore, it is an adaptable framework that can apply across domains and stakeholders.

1. **Preliminary:** Identify context, guidelines, standards, and goals.
2. **Architecture Vision:** Expand stage (1) into a strategic plan that includes guiding organizational principles.
3. **Business Architecture:** Use stages (1) and (2) to develop the business architecture.
4. **Information Systems Architecture:** Use stages (1) and (2) to develop the

[5] It is important to note the connection between these four levels and the standard four levels of the IoT reference architecture discussed in Chapter 1.2.2.

information systems architecture.

5. **Technology Architecture:** Use stages (1) and (2) to develop the technology architecture.
6. **Opportunities and Solutions:** Use stages (3-5) to identify business and operational services.
7. **Migration Planning:** Develop strategic and operational plan to apply stages (3-5) to resolve stage (6).
8. **Implementation Governance:** Develop operational plan to provide oversight mechanisms for new architectures and solutions/services.
9. **Architecture Change Management:** Ensure stages (3-5) are continually updated to match stage (6).

Translating these stages into an IoT domain is straightforward. Stage (1) defines domain-specific contexts and functions. For example, in the healthcare domain it would identify an IoT service such as autonomous diagnosis and important regulations and guidelines such as HIPAA. Stage (2) allows the inclusion of domain-specific best practices and policies for IoT privacy and security into the business strategy, such as declaring a policy of not sharing individual health-related data with an insurance provider. Stage (3-5) operationalizes those best practices and policies for IoT privacy and security, such as providing end-to-end encryption on all datalinks, requiring consent for the collection of new types of data, allowing a user to audit and edit their own data, and providing consistent and reliable data services. Stage (6) encourages the company to explore the use of the service and architecture to meet new marketable opportunities. For example, the IoT healthcare service provider or developer could adapt their services to include emergency care notifications, create boutique healthcare plans, or transfer their analytical tools and architectures into a separate IoT domain such as finance. Stage (7-9) relate to the operational oversight and management processes needed in any domain that includes both regulatory expectations and market competition.

As of 2015, TOGAF was implemented in 60% of Fortune 500 companies, including Cognizant, HP, Cisco, Oracle, IBM, and SPARX Systems.[85] Further, TOGAF members include Fujitsu, HP Enterprise, Huawei Technologies, IBM, Oracle, Philips, American Express, and Boeing, all of which are companies involved in various IoT domains.[86] However, there is one clear trend in the marketing and actual use of TOGAF. Like the other compliance frameworks already discussed, TOGAF has the highest adoption rate among large international companies. This trend suggests that TOGAF compliance is costly and negatively impacts the challenge *Solution Costs*. While TOGAF will impact privacy and security in domains such as finance, manufacturing, commerce, entertainment, and perhaps retail, it is less likely to impact domains such as domestic, education, and government.

Another potential issue with applying TOGAF to IoT is the fact that TOGAF relies on pre-established best practices and policies. As has already been discussed, the market for best practices is overbroad and saturated. Therefore, TOGAF has the potential to exacerbate the challenge *Standards Saturation*. While a number of broad best practice frameworks exist for IoT, few discuss domain-specific considerations. This fact diminishes the effectiveness of TOGAF applied to IoT domains. Further, since TOGAF is a fluid and open framework that adapts to business-specific issues, TOGAF's impact on many IoT privacy and security challenges is uncertain. Table 7.4 attempts to map TOGAF to the effectiveness framework. While the domains covered and the stakeholder power are clear, the impact on challenges is mostly non-obvious.

However, TOGAF has been proven to be operationally sound and widely adopted. If nothing else, it is an accepted industry standard with a massive following that has the industry power to influence the privacy and security of data-driven services. Since IoT will be a key component of robust and effective data-driven services, IoT companies will find themselves in markets and domains that already use TOGAF. Therefore, TOGAF has the potential to provide privacy and security protections within some IoT domains once those domains develop specific best practices.

Table 7.4: Domains covered, stakeholder power, and challenges impacted by TOGAF.

Domains	**Stakeholder Power**	**Impact on Challenges**
Agriculture	Data Brokers (+)	Accountability (+)
Entertainment	Developers/ Manufacturers (+)	Business Models (+)
Finance	SDOs (++)	Solution Costs (–)
Healthcare	Service Providers (+)	Standards Saturation (–)
Infrastructure	Testing/Cert. Vendors (+++)	
Insurance		
Manufacturing/Trade		
Retail/Hospitality		
Telecommunications		
Transportation		

7.6 Compliance Frameworks Conclusion

These case studies reveal that the compliance frameworks ecosystem requires two improvements to better control privacy and security. First, there must be accepted best practices that address IoT risks and harms by domain. This process requires focused standards for each IoT domain. For example, in order for ITIL and TOGAF to be effective, both require normative design standards and industry best practices.

Second, compliance frameworks must be created that work for IoT domains that 1) are not consumer- or profit-centric and 2) do not have the ability to dedicate large capital expenditures on process and system improvements. Most of the compliance frameworks discussed in this chapter have limited applicability to non-profit-centric domains such as government, infrastructure, and defense. Further, most of the compliance frameworks discussed in this chapter are costly and time-consuming. Therefore, they are not effective in domains such as domestic, education, and workplace where firms maintain small enterprise and capital expenditures on compliance frameworks.

For the compliance framework MoC to improve IoT privacy and security, we must 1) design privacy and security standards specific to IoT domains, and 2) tailor those standards for domains that are not consumer- or profit-centric, or domains that cannot rely on large capital expenditures to achieve compliance.

Nothing to see here. Move along.

Chapter 8

Federal Authorities

8.1 Introduction

The final MoC discussed in this thesis is the control available to and currently applied by federal authorities. This section will reveal that this MoC currently has the most power to influence IoT privacy and security. It has also avoided acting on the full extent of that power. Instead of wielding the full weight of federal authority, the groups discussed in this section have all taken an approach that involves broad multistakeholder discussions and the subsequent publishing of reports and recommendations. The efficacy of such an approach is suspect in the context of improving IoT privacy and security.

Within this section, I analyze the various frameworks proposed by and the practices of the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the legislative branch, the executive branch, the Department of Homeland Security (DHS). Each of these members has provided some degree of input or control to the IoT ecosystem. Each of them has followed the trend of multistakeholder discussions and industry self-regulation.

8.2 Federal Trade Commission

8.2.1 Introduction

The following section will analyze the FTC's ability to provide control and improve IoT privacy and security. First, I will discuss the recent events and enforcement activities disclosed in a recent FTC report. Then, I will dive into the efficacy of the three tenets the FTC uses to guide their views and enforcement of IoT privacy and security. The FTC is the most widely cited source of regulatory authority and control within the IoT privacy and security ecosystem. The FTC derives its power to enforce consumer protection through Section 5(a) of the FTC Act that states, "Unfair or deceptive acts or practices in or affecting commerce [. . .] are [. . .] declared unlawful." This same section was amended to include foreign commerce acts or practices that cause or may cause injury within the U.S.. Additionally, the FTC enforces a number of codified consumer protection statutes such as the FCRA, GLBA, and COPPA.[1] Therefore, the FTC sets the national tone in regards to controlling IoT privacy and security.[2] That tone is currently one of broad industry self-regulation with limited guidance on privacy and security standards or rules.

8.2.2 Privacy & Data Security Update: 2016

Each year since 2013, the FTC releases a report titled "Privacy & Data Security Update." These reports are meant to convey how the FTC goes about protecting consumer privacy and ensuring data security. The 2016 report clearly states the mechanisms by which the FTC can enforce privacy and security:

> "The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful

[1] For a complete history of the FTC and its rise as the de facto data privacy protector in the U.S. through a common law approach, see [199].

[2] There is legitimacy to the claim that other federal agencies also set this tone, such as the FDA for IoT healthcare and the DOT for IoT transportation. However, recent work demonstrates that these other agencies look to the FTC for partnership and guidance, such as a joint FTC–FDA endeavor to guide the development of mobile health services [184] and a joint FTC–NHTSA workshop on the privacy and security issues facing connected and autonomous vehicles [183].

> behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules."[77]

As one can see, the FTC's enforcement mechanisms for privacy and security are broad and have the potential to affect every IoT stakeholder. The FTC uses those tools to protect "personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace."[77] In 2016, the FTC used its authority to enact privacy and security controls through eleven **General Privacy** actions and five **Data Security** actions.[3]

These specific actions demonstrate that the FTC's authority in the space of consumer information privacy and security is active and far reaching across domains such as education, telecommunications, healthcare, manufacturing, commerce, and entertainment, and across stakeholders such as data brokers, developers, manufacturers, and service providers.[77] It is also clear that the FTC's approach has engaged an *on the ground* style of developing information privacy and security law. For example, the 2015 *FTC v. Wyndham Worldwide Corp.* case created a new precedent that failure to implement reasonable security is now considered a violation of the FTC act.[11] The case also proved that the FTC is now directly regulating data security best practices.

The FTC has applied its authority in the IoT ecosystem across domains, from finance and insurance to healthcare and domestic. For example, in 2013 the FTC took action against an IoT developer for the very first time when it settled an order against TRENDnet, an IP camera manufacturer who harmed consumers by failing to adhere to their own claims regarding the security of their cameras.[171] Therefore, the FTC has proven and operationalized its control authority in the domain of IoT

[3] For a list of specific FTC actions taken in 2016 to enforce data privacy and security, see Appendix F.

privacy and security. The question remains whether its inherent philosophy and guiding tenets improve the key IoT privacy and security challenges.

8.2.3 The FTC's Privacy and Security Philosophy

In 2012, the FTC released its guiding document for businesses and policymakers in the data-driven world titled *Protecting Consumer Privacy in an Era of Rapid Change*. This report outlines a privacy framework and provides specific recommendations based on discussions with IoT stakeholders. The recommendations include:[72]

1. The privacy framework "does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties."[4]
2. The privacy framework declares the following information collection and use practices exempt from needing consumer consent: product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing. Further, companies do not need to receive consent for collection and use practices "consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law."
3. The FTC urges Congress to enact legislation that provides improved transparency for, and control over, the practices of data brokers.

Further, the report also states that "as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework."[72] These statements and recommendations suggest that the FTC is attempting to solve a number of key privacy and security challenges, including *Economic Incentives*, *Information Asymmetry*, *Solution Costs*, *Accountability*, *Slow Legislation*, and *Regulation Saturation*.

[4] The complex issue of what constitutes sensitive (PII) and non-sensitive data is beyond the scope of this thesis. Please see [32], [81], [150], [154], [161], [171], [191], and [198] for criticisms, recommendations, and analysis all related to the PII problem.

Further, the final recommendation suggests that the FTC is looking to the legislative branch for guidance on the issues of IoT privacy and security. As the previous section noted, that guidance does not currently exist and it is unclear when or if it ever will. At the same time, these statements and recommendations also seem to miss or potentially worsen a few key challenges such as *Information Scope*, *Business Models*, *Device Ubiquity*, *Dynamic Context*, and *Data Aggregation*.

The 2012 FTC report and its privacy framework declares the FTC's guiding philosophy in regards to protecting data privacy and security. The philosophy aligns directly with the discussion in Chapter 3.2 regarding FIPs.[5] These guiding tenets are: **Privacy by Design**, **Simplified Consumer Choice**, and **Transparency**.

Privacy By Design

In an attempt to resolve the challenges *Device Capabilities*, *Business Models*, and *Data Aggregation*, the framework calls on companies to incorporate data security, collection limits, reasonable retention practices, data accuracy mechanisms, and full life-cycle data management support for all products and services. In practice, these tenets provide mechanisms to resolve the targeted challenges. For example, the 2015 *FTC v. Wyndham Worldwide Corp.* case demonstrated that the FTC is willing to practice some degree of control regarding lax privacy and security capabilities, while also offering some definition of reasonable privacy and security practices.[11]

Simplified Consumer Choice

In an attempt to resolve the challenges *Information Scope*, *Information Asymmetry*, *Dynamic Context*, and *User Knowledge*, the framework calls for companies to institute simplified consumer choice mechanisms that do not inundate users in unnecessary information, and consumer consent mechanisms at a time and context that corresponds to data-related decisions. The NaC mechanism, the application of this principle in the marketplace, was already discussed in depth in Chapter 3. In brief, that case study

[5] This alignment makes sense considering the fact that the NaC mechanism is a direct application of the FTC's guiding privacy and security philosophy.

demonstrated how the NaC mechanism exacerbates the challenges *Business Models*, *Economic Incentives*, *Negative Externalities*, *Information Scope*, *Accountability*, *Data Aggregation*, *Psychological Biases*, and *Solution Costs.* Therefore, this specific tenet of the FTC's philosophy is, in practice, at odds with its own purpose.

Transparency

In an attempt to resolve the challenges *Economic Incentives*, *Business Models*, *User Knowledge*, *Device Ubiquity*, and *Dynamic Context*, the framework calls for increased transparency in companies' data practices. This transparency includes the use of privacy notices, access control mechanisms, and consumer education efforts. The challenge with this tenet is that it contradicts the tenet **Simplified Consumer Choice** by increasing the amount of information provided to the user. In practice, it exacerbates the IoT privacy and security challenge *Information Scope* because companies are rarely judicial with the amount and type of information they disclose to users, how they frame the information, and how they share it.

8.2.4 The FTC and IoT

These tenets were reaffirmed in the context of IoT privacy and security in a 2015 FTC report titled, "IoT Privacy & Security in a Connected World."[75] However, this 2015 report also acknowledges that the IoT represents a set of challenges that their framework cannot fully address, including the fact that no one-size-fits-all approach will work for the broader IoT ecosystem because the domain applications are so diverse. For example, in the context of **Simplified Consumer Choice** and **Transparency**, this report states that in the IoT context, different approaches "include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard [. . .] companies may want to consider using a combination of approaches."[75]

Further, this report also demonstrates the FTC's view that the IoT industry is an emerging domain and "does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time."[75] Instead, the report encourages "self-regulatory programs designed for particular industries [. . .] as a means to encourage the adoption of privacy- and security-sensitive practices."[75] Unfortunately, numerous researchers have demonstrated that the self-regulatory approach has and will continue to result in market failure.[62][143][162][190] The reasons for this market failure are the exact privacy and security challenges discussed in Chapter 2.3 and demonstrated in Chapter 3.[6]

8.2.5 Conclusion

Of all the federal authorities, the FTC's authority and mandate represents the most obvious MoC that influences IoT privacy and security. The FTC's use of this authority has impacted the broadest set of domains, stakeholders, and challenges as compared to the other federal authorities analyzed below. Finally, it is clear that the FTC has routine and continuing efforts to investigate IoT privacy and security challenges and solutions, as well as engage the various IoT stakeholders. Table 8.1 represents the domains covered, the stakeholder power, and the IoT privacy and security challenges impacted by the FTC's authority. As one can see, the FTC's authority in this space is broad, their philosophies too general, and their practices and recommendations contradictory. Therefore, the effectiveness of the FTC's current approach to controlling IoT privacy and security is suspect.

8.3 Federal Communications Commission

The FCC has limited authority in the IoT ecosystem. The traditional role of the FCC is to regulate radio, television, wire, satellite and cable communications.[106] In this way, various aspects of IoT technology fall under their purview, as do the domains of

[6] One of the most interesting events regarding the FTC and IoT occurred in 2016 at the Consumer Electronics Show in Las Vegas. The Chairwoman of the FTC at the time, Edith Ramirez, directly acknowledged her own beliefs regarding IoT healthcare services such as those offered by Fitbit. She revealed that she only uses non-internet-connected pedometers to track exercise activity and specifically avoids Fitbit because of privacy fears regarding her sensitive health information and lack of disclosure regarding how that data is used and shared.[223]

Table 8.1: Domains covered, stakeholder power, and challenges impacted by the FTC's control authority and privacy framework.

Domains	Stakeholder Power	Impact on Challenges
Domestic	Consumers (+)	Accountability (+/–)
Education	Data Brokers (+++)	Business Models (+/–)
Entertainment	Developers/ Manufacturers (+++)	Data Aggregation (+/–)
Finance	Government Agencies (++)	Device Capability (+)
Government	Privacy/Security Advocates (+)	Device Ubiquity (+/–)
Healthcare	SDOs (+)	Dynamic Contexts (+/–)
Insurance	Service Providers (+++)	Economic Incentives (+/–)
Manufacturing/Trade	Testing/Cert. Vendors (+)	Info Asymmetry (+)
Retail/Hospitality		Info Scope (+/–)
Telecommunications		Negative Externalities (–)
Transportation		Psychological Biases (–)
Workplace		Regulation Uncertainty (+)
		Slow Legislation (+)
		Solution Costs (+/–)
		User Knowledge (+)

infrastructure, manufacturing, and transportation. Insofar as the FCC can write IoT privacy and security rules, they can only do so for stakeholders who are considered common carriers under Title II of the Communications Act of 1934. Since the 2015 decision on network neutrality, the FCC has begun to play a more significant role in the development of privacy standards for internet-related services.

The FCC derives its primary authority from the Communications Act of 1934 and the Telecommunications Act of 1996. The FCC's powers were expanded in a way that could impact ICT privacy and security in 1996 by title II subsection 202 of the Communications Act of 1934. This subsection granted the FCC rule-making authority on "common carriers" in order to protect against "unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services."[41] By enforcing this authority (e.g. in the 2015 network neutrality case), the FCC can prescribe data privacy and security controls to internet service providers. A recent example of such rule-making was a document released in November, 2016 titled *Protecting the*

Privacy of Customers of Broadband and Other Telecommunications Services. This document represented a set of prescriptive rules to establish baseline consumer privacy protections for telecommunication services.[64]

Before diving into the specifics of this document, it is important to acknowledge a few facts about the FCC and IoT privacy and security. These facts suggest the FCC does not have enough political capital or goodwill to develop effective rules in the IoT ecosystem. First, it is unclear how IoT services will interact with Title II common carriers. It is conceivable that IoT service providers might not even fall under the common carrier label. The FCC's authority, similar to the 3GPP technical standards, might not go beyond the actual spectrum needed for IoT devices to communicate.[7]

Second, the FCC's recent history in the space of IoT privacy and security has been tumultuous. In March, 2016, the FCC Chairman released a proposal to give broadband consumers increased choice, transparency, and security with respect to their data.[63] This proposal was followed in June, 2016, by formal remarks from the FTC Commissioner directly criticizing the FCC's proposed approach to protecting consumer privacy and security.[8] In October, 2016, the FCC issued the formal privacy rules for ISPs mentioned above. These rules define "sensitive" information (such as mobile app data, search engine data, and health data), require opt-in methods for consumers to provide consent, and was intended to go into full effect in 2017.[150][64] Following the 2016 general election, the FCC canceled a plan to pursue the creation of specific IoT security rules yet urged the incoming administration to continue the plan, which endeavored to "empower and educate consumers."[215] Then, in late December, 2016, the FCC announced a new plan to pursue 5G spectrum rules as a way to regulate IoT device security.[9][216] Finally, in January, 2017, the new FCC Chairman began work to fully block the *Protecting the Privacy of Customers of Broadband and Other*

[7] It is important to note that under this perspective, the FCC has no authority over the domestic, workplace, retail, and many aspects of the infrastructure domains since many systems broadcast on un-licensed frequency bands.[58]

[8] It is important to note that the FTC is seen as the traditional federal agency with the responsibility and regulatory authority to protect consumer privacy and security. The FTC authority and approach is discussed in Section 8.2.

[9] The 5th Generation Mobile Network, or 5G, is one proposed telecommunication standard for future IoT networks and services.

Telecommunications Services rules published in October, 2016.[29]

Despite the fact that the FCC privacy rules have been discarded, and that the FCC might cede any claimed regulatory authority in this space back to the FTC, it is still worthwhile to consider the rules. They can be considered briefly because they target a single IoT domain, telecommunications, two specific IoT stakeholders, service providers and consumers, and do so using only three tenets:[64]

1. Choice: Consumers have the right to exercise meaningful and informed control over what personal data their broadband provider uses and under what circumstances it shares their personal information with third parties or affiliated companies.
2. Transparency: Consumers deserve to know what information is being collected about them, how it's being used, and under what circumstances it will be shared with other entities. Broadband providers must provide accurate disclosures of their privacy practices in an easily understandable and accessible manner.
3. Security: Broadband providers have a responsibility to protect consumer data, both as they carry it across their networks and wherever it is stored.

Based on these factors, we can conclude that these rules attempt to solve the IoT privacy and security challenges of *Information Asymmetry*, *Business Models*, *Accountability*, and *Slow Legislation.* However, in doing so they also potentially worsen the challenges of *Information Scope* by forcing service providers to inundate users in more information about the services, *Psychological Biases* by creating a system that relies heavily on personal choice control mechanisms, *Solution Costs* by admittedly creating "up-front costs for small providers," *Standards Saturation* by creating a privacy and security standard that is unclear about which specific providers it requires to do what tasks, and *Negative Externalities* by creating a system in which one person's choices could affect the privacy or security of another person.[64][167] Table 8.2 represents the domains covered, stakeholder power, and challenges impacted if *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* rules had been fully adopted. The potential effectiveness of such a set of rules is suspect and prone to damaging an excessive number of IoT privacy and security challenges.

Table 8.2: Domains covered, stakeholder power, and challenges impacted by complete FCC ISP Privacy Rules adoption.

Domains	**Stakeholder Power**	**Impact on Challenges**
Telecommunications	Consumers (++)	Accountability (+)
	Government Agencies (++)	Business Models (+)
	Service Providers (+)	Info Asymmetry (+)
		Info Scope (–)
		Negative Externalities (–)
		Psychological Biases (–)
		Slow Legislation (+)
		Solution Costs (–)
		Standards Saturation (–)

8.4 U.S. Legislative Branch

There have been no IoT-specific regulations or rules codified by the legislative branch. However, recent congressional hearings suggest that both the House of Representatives and the Senate have begun to consider their role in the future of IoT privacy and security. These hearings are fact-finding and due-diligence processes prior to unilateral action on the part of the legislative branch. This section will review four recent hearings and one recent resolution, the stakeholders involved, and what each hearing represents in terms of the legislative branch's evolving perspective.[10]

8.4.1 Senate Hearing – February, 2015

On February 11, 2015, the Senate Committee on Commerce, Science, and Transportation held the hearing, "The Connected World: Examining the Internet of Things." It focused on how the IoT will change the impact of technology across domains. The multistakeholder witness panel included representatives from the following stakeholder groups: **Privacy/Security Advocates**, **Developers/Manufacturers**, **Ser-**

[10] An interesting future study would be to take the raw-text from each of these hearings and conduct text analysis to determine sentiment and common themes. In this way, one could rigorously and empirically characterize the perspectives, beliefs, and desires of each stakeholder represented at the hearings.

vice Providers, and **Academia/Research Labs**.[91]

Overall, the purpose of the hearing was best summed by the opening statements of Senator John Thune: “By engaging early in this debate, Congress can ensure that any government efforts to protect consumers are tailored for actual problems and avoid regulatory overreach.”[91] Later in his opening statements, Senator John Thune also noted that the industry is “standing on the cusp of technological innovations that will improve both the safety and convenience of everyday items,” and warned against “government needlessly slow[ing] the pace of new development.”[91] These quotes demonstrate that the legislative branch wants to take action to protect consumers while also avoiding negative impacts on technology innovation.

The witness panel testimonies and question-answer session during this hearing demonstrated that the developers, manufacturers, and service providers hold significant concerns that *any* federal regulation will stifle IoT growth and innovation.[91] That being said, it was also clear through the testimony of Douglas Davis (Vice President and General Manager,Internet of Things Group, Intel), that large industry stakeholders such as Intel are interested in creating public-private partnerships to develop sector-specific rules.[91]

8.4.2 Senate Resolution – March, 2015

On March 24, 2015, the 114th Congress published Senate resolution 110 “about a strategy for the Internet of Things to promote economic growth and consumer empowerment.”[66] It declared five individual resolutions that demonstrate the Senate’s perspective on the future of IoT technologies and uses:[66]

1. The United States should develop a strategy to incentivize the development of the Internet of Things in a way that maximizes the promise connected technologies hold to empower consumers, foster future economic growth, and improve our collective social well-being.
2. The United States should prioritize accelerating the development and deployment of the Internet of Things in a way that recognizes its benefits, allows for future innovation, and responsibly protects against misuse.

3. The United States should recognize the importance of consensus-based best practices and communication among stakeholders, with the understanding that businesses can play an important role in the future development of the Internet of Things.
4. The United States Government should commit itself to using the Internet of Things to improve its efficiency and effectiveness and cut waste, fraud, and abuse whenever possible.
5. Using the Internet of Things, innovators in the United States should commit to improving the quality of life for future generations by developing safe, new technologies aimed at tackling the most challenging societal issues facing the world.

These resolutions demonstrate a few key trends. First, the legislative branch recognizes the significant impact that IoT technologies will have on every domain of social and economic life. Second, the legislative branch recognizes the need to foster IoT innovation and growth in order to maintain competitiveness in the world's markets. Third, the legislative branch recognizes the need for industry standardization. Fourth, the legislative branch recognizes the potential for data harms and misuse related to the development of IoT technologies. These resolutions do not convey an intent to conduct further legislative proceedings or codify privacy and security rules.

8.4.3 Congressional Hearing – March, 2015

On March 24, 2015, the House Energy and Commerce Committee held a hearing titled, "The Internet of Things: Exploring the Next Technology Frontier." The focus of the hearing was the multi-domain and broad consumer impact of IoT technologies. The multistakeholder witness panel included representatives from the following stakeholder groups: **Privacy/Security Advocates**, **Developers/Manufacturers**, and **Service Providers**.[89]

Testimonies from the witness panel made it clear that the perspectives on regulating IoT privacy controls and regulating IoT security controls are contradictory. The stakeholders fear that *privacy* regulation will limit the usefulness and effectiveness of

IoT technologies. For example, in calling for continued industry self-regulation one stakeholder said, "Privacy principles designed for a small data world might not work in a big data world."[89] Meanwhile, the same stakeholders also advocated that Congress directly incentivize the IoT industry to adopt better *security* practices. Daniel Castro (Vice President, Information Technology and Innovation Foundation) said, "Congress should pass data breach notification legislation that preempts state laws and reduces the legal compliance costs companies face from abiding by multiple rules. This will allow them to focus more resources on proving the security of their products."[89] Thus, it is clear these stakeholders feel that the current security regulation environment is plagued by *Regulation Uncertainty*.

The difference between the stakeholders' perspectives on *privacy* regulation and *security* regulation are an interesting contradiction. In the context of *privacy*, they are adamant that any regulation will stifle innovation. In the context of *security*, they are adamant that regulation will ensure innovation. It is unclear what these stakeholders believe is different between the two regulatory goals.

8.4.4 Senate Hearing – June, 2016

On June 28, 2016, the Senate Committee on Commerce, Science, & Transportation held a hearing titled, "How the Internet of Things (IoT) Can Bring U.S. Transportation and Infrastructure into the 21st Century." The multistakeholder witness panel included representatives from the following stakeholder groups: **Government Agencies**, **Service Providers**, and **Developers/Manufacturers**.[92]

The hearing explored how businesses and the government use IoT to enhance the efficiency of infrastructure and transportation. It is the only IoT-related legislative hearing that even acknowledges the fact that different IoT domains might require different analysis, rules, and standards. The witness panel was directed to provide their individual successes and challenges in adopting IoT technology for the transportation and infrastructure domains. Further, they were also asked for their perspective on government's appropriate role in promoting innovation, adopting new technologies, and protecting safety in transportation and infrastructure.

It is clear from the witness comments that the stakeholders in the transportation and infrastructure domains desire standardization, open and interoperable systems, private-public partnerships, a national IoT strategy, and that there is a common industry-stakeholder belief that regulation lags behind innovation and stifles growth.[92] This hearing also represented a clear shift in stakeholders' tone regarding federal regulation. Many of the stakeholders acknowledged the current IoT ecosystem requires more clear standards and controls, that various State-specific rules and international standards have created *Regulation Uncertainty* and *Standards Saturation*, and that the federal government is obligated to correct such market failures.[11][92]

8.4.5 Congressional Hearing – November, 2016

On November 16, 2016, the House Energy and Commerce Committee held a hearing titled, "Understanding the Role of Connected Devices in Recent Cyber Attacks." The focus of the hearing was the multistakeholder steps needed to make the IoT ecosystem more secure without sacrificing innovation and growth, and was motivated by the Mirai botnet attack on October 21, 2016. The witness panel included representatives from the following stakeholder groups: **Service Providers** and **Academia/Research Labs**.

It is interesting to note the difference between this witness panel and the panels of the other IoT-related hearings. While the other hearings focused (with exceptions) on industry-stakeholders like developers, manufacturers, and service providers, this hearing centered around academic researchers considered to be privacy, security, and technology experts. This change might be a sign of shifting perspectives in the legislative branch in regards to their authority and obligation to implement national IoT privacy and security regulations.

The testimonies by Bruce Schneier and Kevin Fu, the academics at this hearing, were more nuanced in considering IoT privacy and security controls than the testi-

[11] Some of the witnesses expressed the desire to work with the National Highway Traffic Safety Administration in order to resolve the need for common federal IoT standards and rules in the transportation domain.

monies in the other hearings above. Most notably, at no point in their testimonies did either dispose of an entire control method such as command and control regulations. Conversely, in each prior hearing almost every panel member made a point of disposing of command and control regulation as a reasonable MoC. The testimonies in this hearing, by both the witnesses and the committee members, demonstrated a growing interest in command and control regulation, particularly in the context of security and IoT ecosystem risks.[90] Further, this hearing discussed a few specific IoT privacy and security challenges that need to be addressed such as *Economic Incentives*, *Standards Saturation*, and *Device Capabilities*.[90] Finally, the witnesses also offered specific means by which the legislative branch could regulate without sacrificing the benefits of an open, free, and innovative market. For example, Kevin Fu specifically observed that regulations that champion desired outcomes and principles, and not the mechanisms to achieve them, are often beneficial for innovation.[90]

8.4.6 Conclusion

While there has only been four legislative hearings related to IoT, there is a growing trend towards discussing common federal standards and regulations for IoT privacy and security. Further, there is also a potential trend towards the realization that separate IoT domains require separate standards and regulations.[12]

This section did not discuss, and the legislative branch has not provided, any concrete recommendation, regulation, standard, or framework in regards to IoT privacy or security. Therefore, this section on legislative control does not include a mapping of the IoT domains, stakeholder power, and impact on challenges. However, the legislative branch has the potential and the authority to clearly affect every IoT domain and improve upon each IoT privacy and security challenge if it operates with purposeful intent as per the suggestions of the most recent congressional hearing.

[12] It is also interesting to note that the two congressional IoT-related hearings and the two senate IoT-related hearings were conducted by the same committees: The House Energy and Commerce Committee, and the Senate Committee on Commerce, Science, & Transportation. Therefore, if one is interested in tracking the legislative branch's efforts as related to the IoT ecosystem, one should track these two committees, their membership, and their statements.

8.5 U.S. Executive Branch: National Privacy Research Strategy (NPRS)

The NPRS, published in 2016, describes the executive branch's strategy for enhancing privacy in the ICT realm through federally-funded research and guidance for federal agencies. It is concerned with the *mosaic effect* of data privacy. The mosaic effect is the point where analysis across multiple datasets reveals private information or generates inaccurate and harmful inferences.

The NPRS describes the following three privacy challenges that face the ICT domain. One can see how these three challenges match directly to the IoT privacy and security challenges described in Chapter 2.3.

1. **Influence of Context on Privacy** - matches *Dynamic Contexts* and *Device Ubiquity*.
2. **Transparency in Data Collection, Use, and Retention** - matches *Information Asymmetry*, *Information Scope*, *Solution Costs*, and *Accountability*.
3. **Data Aggregation, Analysis, and Release** - matches *Information Scope*, *Business Models*, *Solution Costs*, and *Data Aggregation*.

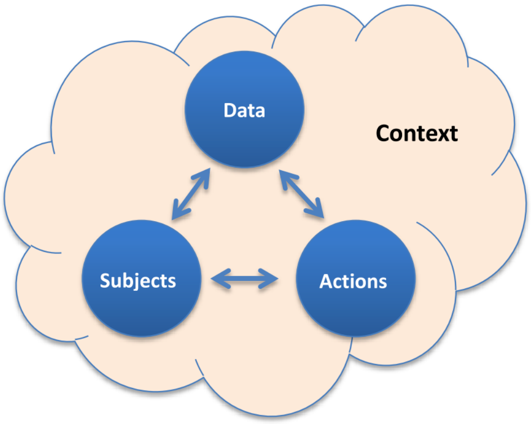


Figure 8-1: The NPRS privacy system.[13]

NPRS also provides a framework that describes the privacy system (Figure 8-1). This framework is useful because it provides stakeholders with common definitions

[13] Found in [157].

and a common system to discuss privacy concerns and research. It defines *subjects* as individuals, groups, the identity of individuals or groups, their rights, autonomy, and their privacy thresholds. It defines *data* as the information derived about individuals and groups. It defines *actions* as data collection, processing, analysis, and retention, controls that constrain such practices, and the impact on subjects and society of such practices. Finally, it defines context as what influences the interpretation and the interactions between subjects, data, and actions.

Finally, NPRS proposes the following priorities for privacy research:[14]

1. Foster a multidisciplinary approach to privacy research and solutions.
2. Understand and measure privacy desires and impacts.
3. Develop system design methods that incorporate privacy desires, requirements, and controls.
4. Increase transparency of data collection, sharing, use, and retention.
5. Assure that information flows and use are consistent with privacy rules.
6. Develop approaches for remediation and recovery.
7. Reduce privacy risks of analytical algorithms.

The three NPRS parts – privacy challenges, privacy system framework, and research priorities – encompass the entirety of the contributions that this report provides for improving IoT privacy and security. It is useful for sparking conversation, and little else. In a sentence, this endeavor has no teeth.

The only mechanism that the executive branch has for implementing such a strategy is through funding research and coordinating between the various executive branch agencies. In 2014, the U.S. Government provided $3.9 billion in networking and information technology research.[185] Of that total, only $80 million was allocated for privacy research.[185] The executive branch could provide broad directives meant to impact IoT privacy and security. As of yet, no such directives exist.

Therefore, while the strategy outlined by this report is admirable, the report itself does not improve IoT privacy and security. There is benefit in declaring the values

[14] All priorities include a set of key research questions that must be addressed. I have copied these questions in Appendix E for convenience since many apply directly to future work in the realm of IoT privacy and security.

and intent of the executive branch in regards to data privacy research, and the NPRS does so. This report also offers a number of key research questions, available in Appendix E, that should be pursued by academic research.

Since this work is a statement of strategic goals and not a functional standard, framework, or architecture, I have not mapped it to the MoC analysis framework.

8.6 The Department of Homeland Security: Strategic Principles for Securing the IoT

The DHS Strategic Principles are similar to the NPRS in the sense that the report describes a high-level strategy for enhancing privacy and security. However, there are a few key differences between the two strategies. First, the DHS report is tailored to the IoT ecosystem, while NPRS only alludes to IoT in its mission and strategies. Second, the DHS Strategic Principles targets industry stakeholders, whereas NPRS targets academic researchers and government agencies. Third, DHS's strategy focuses on security and emphasizes the technical aspects of IoT security. Finally, the result of DHS's Strategic Principles is not a research agenda, but rather a set of high-level recommendations for IoT systems and service development and deployment.

The report includes a section on its intended audience and how each stakeholder can operationalize the principles. This characteristic is unique and useful since it provides a clear stakeholder analysis for DHS's IoT security strategies. The intended audience, and their responsibilities, are:[50]

- **IoT Developers** - Consider security when designing or developing a device, sensor, service, or IoT component (also called security by design).
- **IoT Manufacturers** - Expand security controls for consumer devices and vendor-managed devices.
- **Service Providers** -Provide IoT services, consider the service security and functional security of those IoT devices, develop the security of the infrastructure that enables IoT services.

- **Industrial and Business-level Consumers** - Engage manufacturers and service providers regarding the security of IoT devices and services (includes the federal government and critical infrastructure owners and operators).

The actual principles are a set of general and non-binding concepts meant to improve IoT security through design, manufacturing, and deployment processes. Further, the report includes suggested best practices to implement each principle. The principles represent an initial yet formalized attempt to initiate IoT security conversations between IoT developers, manufacturers, service providers, and users. The strategic principles are:[50]

1. Incorporate security at the design phase.
2. Advance security updates and vulnerability management.
3. Build on proven security practices.
4. Prioritize security measures according to potential impact.
5. Promote transparency across IoT.
6. Connect carefully and deliberately.

For each principle, the report identifies a current endeavor that exemplifies the principle in practice. For example, the report identifies NIST's "Cybersecurity Risk Management Framework" as a starting point for principle 3. The report also provides suggested practices for the targeted stakeholders to apply each principle. For example, the report suggests "coordinating software updates among third-party vendors to address vulnerabilities and security improvements" as an application of principle 2.[50] The report intends to address the IoT privacy and security challenges *Economic Incentives*, *Information Asymmetry*, *Business Models*, *Accountability*, *Slow Legislation*, and *Device Capabilities*. The report does not provide any domain-specific considerations in terms of these challenges, nor a framework for doing so. However, it does provide some clear stakeholder-specific recommendations as suggested practices.

The report is basic and to the point. It does not provide a panacea to address IoT security challenges. What it provides is a clear and simple set of principles that *may* lead to better privacy and security practices for developers, manufacturers, service providers, and consumers.

The report itself, similar to the NPRS, has no teeth and therefore will not prove effective at addressing IoT privacy and security. The report suggests four "lines of effort [. . .] to fortify the security of the IoT."[50] However, these lines of effort are all soft-power attempts at improving IoT security such as "build awareness of the risks associated with IoT across stakeholders," and "contribute to international standards development processes for IoT."[50] Without the use of hard-power to enforce these principles, specific standards, and risk frameworks, there is little hope that this strategy can improve the IoT privacy and security challenges it purports to correct.

Similar to NPRS, this work is a statement of strategic goals and not a functional standard or framework. Therefore, it is not mapped to the MoC analysis framework

8.7 Federal Authorities Conclusion

The federal authorities MoC for IoT privacy and security varies greatly in terms of practical effectiveness. The FTC is the most active federal authority MoC for IoT privacy and security. Not only does it have a broad mandate to protect data privacy and security, but it also routinely practices that mandate and attempts to represent all stakeholders and domains while doing so. Unfortunately, the effectiveness of the FTC's current approach to IoT privacy and security, self-regulation, is suspect. In fact, the FTC's entire philosophy regarding data privacy and security fails to capture many aspects of the IoT ecosystem that require control. Therefore, the FTC's current approach to controlling IoT privacy and security cannot be considered effective. The FCC has attempted to enact narrow control in order to improve consumer data privacy and security in the telecommunications domain, but its authority has recently been questioned and dismissed. The legislative branch has begun the process of enacting controls for IoT privacy and security, but it is yet to implement any tangible control. If it does so, the resulting effects are unclear. Many stakeholders claim that command and control regulation from the legislative branch will destroy IoT innovation. Some stakeholders claim that it will ensure innovation. This dichotomy explains the legislative branch's reluctance to proceed with any command and control regulation. The executive branch has enacted minimal effective control meant to improve IoT privacy and security. DHS has enacted control, though the mechanism and implementation of said control will likely not improve IoT privacy and security due to its generality and broad nature. Therefore, the current application of the federal authority MoC is ineffective at improving IoT privacy and security.

Part III

Conclusions and Recommendations

Nothing to see here. Move along.

Chapter 9

The Course Ahead

9.1 Introduction

The series of case studies that comprise the body of this work, while not exhaustive, reveal key trends among the available IoT privacy and security MoCs. By identifying the primary challenges that these MoCs exacerbate or improve, we can determine the most important targets for research into IoT privacy and security solutions. Further, by tracking the common MoC trends from each case study, we can also determine the trends that require paradigm shifts. Using these two methods, this final chapter seeks to provide a navigable course for improving IoT privacy and security.

In this chapter, I first explain the most important findings derived from the MoC case studies. These results include both MoC-specific observations as well as common trends. From these results, I build a case for the two fundamental faults in current IoT privacy and security controls. The faults can be distilled into two veins, both related to specificity. First, current IoT privacy and security controls lack domain focus. Domain focus is the narrow scope in which a MoC applies. It relates to the IoT system *context*. Second, current IoT privacy and security controls lack a risk and harms focus. Risk and harms focus is the specific IoT privacy and security implication that a MoC targets. It relates to the *use* of IoT systems. These faults lead to a market failure that must be addressed if IoT stakeholders wish to internalize effective privacy and security as driving tenets.

Next, I present two specific and tangible scenarios where the MoCs discussed in this work have failed to provide reasonable privacy and security controls – the recent TRENDnet and the D-Link cases. Both cases were adjudicated by the FTC, and neither has led to increased privacy or security controls in the IoT ecosystem. These brief case studies serve as a tangible application of the meta-analysis in the body of this thesis that can serve as specific examples for policymakers.

Finally, I recommend three major paradigm shifts to address this market failure. First, the Federal Trade Commission must acknowledge that its current adjudicative approach that controls *business practices* without addressing more fundamental *business models* has failed and will continue to fail to improve IoT privacy and security. Second, the Notice and Choice framework must undergo a thorough redesign or be discarded as the primary IoT privacy and security MoC. The structure of the current Notice and Choice framework is at odds with the realities of the IoT ecosystem. This conclusion is derived from a detailed analysis in Chapter 3 as well as the results of an IoT consumer study included in Appendix A. Personal choice control mechanisms like Notice and Choice should not be relied upon to improve IoT privacy and security. Third, new IoT privacy and security standards must be developed that embody the tenets of specificity and provide baseline privacy and security controls. The MoC case studies demonstrate that the extensive market for IoT operational and technical standards fails to control the fundamental IoT privacy and security challenges due to lack of specificity. The realization of these paradigm shifts will navigate the IoT ecosystem towards more effective privacy and security control.

In order to encourage this realization, I present the initial strategy and proposal for an IoT Lab research endeavor. The IoT Lab will serve to analyze and categorize IoT systems and services for the purpose of developing domain-specific operational and technical privacy and security standards.

9.2 Conclusions

9.2.1 MoC-specific Conclusions

The following conclusions are drawn from each specific MoC case study and research conducted for this thesis.

Individual Choice Mechanisms

Individual choice mechanisms like the Notice and Choice framework have led to, and will continue to lead to, significant privacy and security market failure in the IoT ecosystem. The market failure is caused by a number of key IoT privacy and security challenges that actively work against its effectiveness, such as *Business Models*, *Economic Incentives*, *Information Scope*, *Negative Externalities*, *Device Capabilities*, *Device Ubiquity*, *Solution Costs*, *Psychological Biases*, and *User Knowledge*. It is a MoC designed for webpages with an incomplete and damaging extrapolation to the realities of IoT systems and services. A major finding from this chapter is that the de facto IoT privacy and security norms and status quo MoC is ineffective.

Command and Control Regulations

Command and control regulations for IoT privacy and security comprise an immature market in the sense that there are no IoT-specific command and control regulations.[1] However, there are a number of command and control regulations with collateral IoT impact that appear to provide effective privacy and security controls. HIPAA, the most obvious of such regulations, has already had an impact on IoT privacy and security by encouraging IoT developers and service providers like Fitbit to implement HIPAA privacy and security controls. Further, these controls are effective in the sense that firms have *volunteered* to implement them, so their negative impact on innovation and economic growth must be limited, and they have created a domain-specific set

[1] In this context, market maturity relates to how many of the type of MoC exist within the market. Therefore, a mature MoC market would be one in which there exists many example MoCs to analyze.

of privacy and security norms that firms can expand. Therefore, it is conceivable that future direct domain-specific regulations for IoT privacy and security can be an effective MoC. A major finding from this chapter is that for a MoC to be effective, it must have a narrow domain focus.

Operational and Technical Standards

Standards that impact IoT privacy and security comprise a vast and mature market, and the only MoC category that actually has IoT-specific controls. However, the vastness of the market has led to saturation and subsequent confusion regarding industry best practices and the specific controls provided by individual standards. While there are a number of key popular standards, it is unclear which of the hundreds of IoT standards is the most effective in specific domains and use-contexts. Standards rarely present themselves in regards to which risks, harms, and challenges they address and improve. This uncertainty leads to confusion and ineffectiveness in developing IoT privacy and security controls because firms might choose a suboptimal standard for their IoT domain. Therefore, the current IoT standards market is ineffective in its adoption and, ironically, requires clearer standardization. A major finding from this chapter is that for a MoC to be effective, it must have a clear risk and harm framing.

Compliance Frameworks

Compliance frameworks that impact IoT privacy and security also comprise a vast and mature market. However, the market is less mature than the operational standards market in the sense that IoT-specific controls are just now being developed. Further, the existing compliance frameworks that impact IoT privacy and security tend to be expensive and lack focus on informational privacy and security. The existing compliance frameworks fail in their specificity towards specific IoT privacy and security challenges, stakeholders, and domains. The compliance framework MoC is an effective IoT privacy and security control for large developers and service providers in specific domains such as finance, insurance, telecommunications, retail, and manufacturing. However, it is less effective for smaller developers and service providers, and those in domains such as domestic, workplace, and education. A major finding from this chapter is that for a MoC to be effective, it must be specific regarding which IoT uses, domains, and risks it seeks to address.

Federal Authorities

Federal authorities that can impact IoT privacy and security have demonstrated themselves to be either inconsistent between their statements and actions, or committed to the current status quo. Recent events suggest that the FCC will avoid writing regulations that impact the ecosystem for the foreseeable future. Recent statements from the FTC suggest that the organization is committed to the status quo controls such as the Notice and Choice framework. Recent hearings suggest that Congress has interest in future IoT privacy and security controls, but is yet to demonstrate any coalition to develop such controls. A major finding from this chapter is that the current federal authorities MoC is ineffective for two reasons. First, recent statements suggest that federal authorities are committed to current status quo MoC norms. Second, it is unlikely that federal authorities will provide much future control for IoT privacy and security without significant prodding.

9.2.2 General MoC Conclusions

The following conclusions are drawn from a holistic consideration of the MoC case studies and research conducted for this thesis. Each conclusions demonstrates the fact that a market failure currently exists in terms of IoT privacy and security.

Domain Conclusions

Most MoCs are too inclusive and generic. With the exception of the FCC authority and HIPAA rules, all other MoCs analyzed in this thesis covered nearly every domain. This structure decreases MoC effectiveness because it leads to uncertainty and broad privacy and security solutions that fail to address domain-specific technologies and use-contexts. Further, it tends to lead to a system that does not address specific risks, harms, or challenges. In a sentence, generic MoCs lead to generic solutions, and generic solutions do not always solve specific privacy and security failures. Therefore, a market failure exists.

Stakeholder Conclusions

The current status quo for IoT privacy and security MoCs grants the greatest power and autonomy to developers and manufacturers, service providers, data brokers, and standards developing organizations. More clearly, this system is best characterized by the term "self-regulation." The IoT privacy and security challenge *Economic Incentives* explains why a market failure occurs when these stakeholders retain so much power. These stakeholders' incentives are not always aligned with increased privacy and security.[12][13][151] Therefore, a self-regulatory MoC that grants the most power to these stakeholders is an ineffective control for IoT privacy and security.

Challenges Conclusions

Table 9.1 shows which key privacy and security challenges are most damaged and improved by the current IoT privacy and security MoCs.

Table 9.1: Challenges most damaged and improved by current MoCs.

	Challenges Damaged	**Challenges Improved**
1.	Solution Costs	Accountability
2.	Standards Saturation	Business Models
3.	Psychological Biases	Slow Legislation
4.	Negative Externalities	Device Capability
5.	Information Scope	Economic Incentives
6.	Business Models	Information Asymmetry
7.	Data Aggregation	Regulation Uncertainty

It is interesting to note that both lists include *Business Models*. This fact is further evidence of an IoT privacy and security market failure and the MoC faults discussed below in more detail. The current MoCs create a system characterized by uncertainty, confusion, and inconsistency. Therefore, it makes sense that some MoCs improve the

Business Models challenge while others aggravate it. Further, because the challenge *Business Models* relates to how IoT developers and manufacturers, service providers, and data brokers embrace IoT privacy and security, this tumultuous relationship is further evidence that a self regulatory MoC system may be ineffective.

9.2.3 Specificity and the MoC Faults

For convenience, I have synthesized the above conclusions into common interrelated faults that impact the effectiveness of current IoT privacy and security MoCs. The common faults both relate to the systemic lack of MoC specificity and manifest as a general lack of **domain** or **risk and harms** focus.

Domain Focus

Domain focus is the narrow scope in which a MoC applies. It relates to the IoT system *context*, and can apply to every stakeholder.

Risk and Harms Focus

Risk and harms focus is the specific IoT privacy and security implication(s) that a MoC targets. It relates to the *use* of IoT systems, and can apply to every stakeholder.

9.3 Recommendations

In terms of a practical application of these conclusions, one common thread permeates this entire thesis: the current MoCs for IoT privacy and security are insufficient and the IoT community must undergo a paradigm shift if it wishes to embody strong privacy and security values. The paradigm shift requires three focuses: 1) A full practical evaluation and overhaul of the federal government's regulatory authority and its privacy and security enforcement actions; 2) A full practical evaluation and overhaul of the NaC framework as applied to IoT systems; and 3) A research endeavor for the purpose of developing context-specific IoT operational and technical standards to influence policymakers, device manufacturers, and service providers. We can establish the veracity of that claim through a brief and concrete policy scenario. For this scenario, I will consider the IoT domestic domain.

9.3.1 Practical Evidence: Grounding the Meta

Privacy and security in the IoT domestic domain is controlled by the NaC framework, the FTC's rule-making authority, and the numerous operational and technical standards available within the market. Two recent FTC cases exemplify the market failure of the current MoCs as applied to the IoT domestic domain. The first was the 2014 FTC order against TRENDnet, Inc., a device manufacturer and service provider that sells IoT devices such as routers and IP security cameras for the home and for businesses. The second was the 2017 FTC charges against D-Link, a device manufacturer and service provider that sells IoT devices such as routers and IP security cameras for the home and for businesses. Both lawsuits were brought against the companies for lax security practices and deceptive security claims in regards to their IP cameras (TRENDnet and D-Link) and routers (D-Link).

TRENDnet

TRENDnet's cameras relied on software called "Securview." Securview advertises that it helps organizations adhere to the security best practices of ITIL and ISO-27001, as well as compliance under the Payment Card Industry Data Security Standard, HIPPA, GLBA, the Federal Information Security Management Act, and SOX.[192] According to the FTC, TRENDnet implemented insecure software security practices in their cameras "that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address."[73] Therefore, despite the industry best practices, and security and compliance standard certifications, TRENDnet's software was insecure. In this case, the technical standards, operational standards, and compliance frameworks failed to provide reasonable privacy and security controls.

TRENDnet is now required to submit security assessments to the FTC every two years. The first of these assessments, released in 2014, has a number of issues:[96]

1. TRENDnet's system assessment did not appear to be certified.
2. The company hired to test TRENDnet's system is listed only as the "Institute for Information Industry."
3. TRENDnet's CEO states that Certified Information System Security Professionals developed their compliance system. No experts are identified.
4. The FTC called for Certified Secure Software Lifecycle Professional (CISP) or CISSP-performed evaluations. The evaluation was completed by someone who claims to be a "security specialist" who holds "Certified Ethical Hacker CEH and ISO 27001 Lead Auditor certificates."
5. The report includes pages of training materials and policies, but no explanation for how these meet the risk identification and mitigation obligations of the FTC consent decree.

Since this initial 2014 assessment, the FTC has taken no additional actions against TRENDnet. It appears that the FTC enforcement actions may have had less of a controlling impact on TRENDnet's system privacy and security than intended. Finally, even though the consent decree related specifically to TRENDnet's IP security cameras, one would assume that such intense scrutiny would lead to company-wide changes in security practices. However, recent work publicized by Jan Hoersch, an IT security consultant at Securai GmbH, at Kaspersky Lab's Security Analyst Summit demonstrated significant and persistent security flaws in TRENDnet routers.[30]

D-Link

The second case involves the IoT device manufacturer D-Link. D-Link collects alliances and industry-accreditation's like trading cards. On their website, they flaunt partnerships and memberships under five different categories: **Internet Service Cloud**, **Software**, **Multimedia and Digital Home**, **Connectivity and Security**, and **Standards and Regulations**. In total, D-Link advertises 19 industry partnerships and 18 industry memberships, including with major security standards such as the IEEE technical standards, software security solutions such as OnSSI, OpenDNS, and Milestone Systems, popular security certification vendors such as ICSA Labs, and IoT technical standards groups such as the zWave Alliance.[54]

The FTC lawsuit noted specific issues with D-Link's systems. First, D-Link advertised their routers as "Easy to Secure" and containing "Advanced Network Security," while failing to address simple and preventable security flaws such as:[79]

1. "Hard-coded" login credentials integrated into D-Link camera software – such as the username "guest" and the password "guest" – that could allow unauthorized access to the cameras' live feed.
2. A software flaw known as "command injection" that could enable remote attackers to take control of consumers' routers by sending them unauthorized commands over the Internet.
3. The mishandling of a private key code used to sign into D-Link software, such that it was openly available on a public website for six months.
4. Leaving users' login credentials for D-Link's mobile app unsecured in clear, readable text on their mobile devices, even though there is free software available to secure the information.

Therefore, despite the industry best practices, industry collaborations and partnerships, and security and compliance standard certifications, D-Link's systems still contain major privacy and security faults. In this case, the technical standards, operational standards, and compliance frameworks MoCs all once again failed to provide reasonable privacy and security controls, even for well-established best practices such as not hard-coding simple login credentials for routers.

While the D-Link case is yet to be settled, few suspect that the FTC's enforcement actions will prove to be any more effective than they did for the TRENDnet case. For such recent cases regarding the claimed privacy and security practices of digital services and device manufacturers, the settlements amount to a slap on the wrist and a warning to stop lying, and only require submitting privacy or security assessments to the FTC every few months for 20 years – few and insignificant fines (if any), and no restrictions or course-changing controls are imposed.[26]

The D-Link case is also evidence for the failure of individual choice MoCs like

NaC. A study I conducted with two fellow researchers that investigates consumer's privacy and security considerations regarding various IoT devices looked at 87 different devices, including two D-Link products (see Appendix A). This study concluded that there was no correlation between publicized privacy or security vulnerabilities in IoT devices and the presence of consumer discourse regarding privacy or security of the device. Further, it also concluded that few consumers even consider privacy or security issues when reviewing IoT devices. In terms of the two D-Link devices, one had a rate of privacy or security discussion in consumer reviews of 7.43% while the other had a rate of 1.27%. The low prevalence of privacy and security discourse, even in devices with well-known and publicized privacy and security flaws, suggests that the IoT ecosystem should not rely on consumer control mechanisms like individual choice to encourage better privacy and security practices.

Implications of These Scenarios

While the majority of this thesis evaluated the faults and limitations of IoT privacy and security MoCs at a meta level, these two scenarios ground the conclusions of this thesis in practical reality. Both cases demonstrate that the current IoT privacy and security MoCs fail not only "on the books" but also "on the ground." Therefore, the IoT ecosystem requires new and better-designed privacy and security controls predicated on three fundamental paradigm shifts.

9.3.2 Necessary Paradigm Shifts

1. The FTC must address the fact that its enforcement actions could be more effective at considering organizations' privacy or security faults by evaluating and taking actions against organizations' actual business models and not just business practices. The practices are only a symptom of the fundamental privacy and security issues that originate with an organization's business model. The framework provided in Appendix G is an effective approach to analyzing an organization's business model as represented by business practices. It re-

quires a detailed evaluation of an organization's controlling documents (terms of use, privacy and data policies, contracts, etc) as well as an analysis of specific devices in use. This framework can be used to enhance the FTC's enforcement against unfair and deceptive practices. Further, since the FTC's authority does not cover every IoT domain, authorities such as the Food and Drug Administration, the Federal Aviation Administration, and the National Highway Traffic Safety Administration must conduct similar analyses of their enforcement actions regarding the privacy and security of IoT systems and applications within their specific domains. This work can be informed, supported, and improved by the third paradigm shift.

2. If the FTC intends to champion the NaC framework as the primary privacy and security MoC for the IoT ecosystem, then NaC requires a significant reboot. The majority of evidence in Chapter 3, as well as the results from the study in Appendix A, supports the notion that NaC will continue to result in an IoT privacy and security market failure. While a 2009 study demonstrates that consumers make privacy-enhancing decisions in a marketplace *if* clear, understandable, and salient information about the implications of data use is presented to them [209][210], the study in Appendix A demonstrates that such information is not part of the open discourse regarding IoT devices, and the analysis presented in Chapter 3 demonstrates that the current NaC framework is not equipped to present such information for IoT systems and services. Given the poor applicability of the current NaC framework to the IoT ecosystem, a new IoT NaC framework would benefit from two developments. First, analyzing and accepting the limits of effective privacy and security notices in IoT use-contexts. Second, acknowledging the fact that consumer choice is vulnerable to trading reasonable but immeasurable privacy and security for tangible functionality and immediate usefulness. Given these facts, the privacy and security of the IoT ecosystem, and the effectiveness of the NaC framework, would benefit from the third paradigm shift.

3. Parties with controlling power like policymakers, regulators, and federal authorities must acknowledge that relying on the current IoT standards market will not address major IoT privacy and security issues. The current market, while extensive, is saturated with broad operational and technical standards that lack the needed specificity to improve IoT privacy and security. The current approach is to allow the free market to establish its own winners. However, this approach has led to an overabundant standards market that does not lead to better IoT privacy and security practices. Instead, narrow technical and operational standards must be written that apply to specific use-contexts for IoT technologies and that apply best practices designed from risk and harm assessments. Further, base-line or minimum domain standards must be enforced.

Research groups can make immediate progress on paradigm shift 3. Current operational and technical standards fail to address major IoT privacy and security risks and harms by use-context and domain. Therefore, research groups should design technical and operational standards to accomplish that goal. By analyzing and categorizing IoT systems and services based on a domain and harms framework, a research group can publish a body of IoT privacy and security standards that establish the foundation for effective policy making, functional systems engineering, and usable privacy and security controls for the entire IoT ecosystem. Such a research endeavor requires the creation of an IoT Lab designed to evaluate the technical and operational factors of IoT systems, as well as the controlling business models and regulatory environment for the IoT system and parent organization.

9.4 IoT Lab Proposal

The following section outlines a proposal for MIT's Internet Policy Research Initiative to build an IoT laboratory. The idea for this laboratory derives from the MoC case studies on operational standards, technical standards, and compliance frameworks

(Chapters 5, 6, and 7 respectively). The investigation of MoCs led to the conclusion that the current market for IoT operational and technical standards is extensive yet incomplete. The current IoT standards market is extensive in the sense that there are hundreds, if not thousands, of available standards. However, the market is incomplete in the sense that the available standards fail to embody the tenets of specificity. In particular, current standards fail to consider the *contextual uses* of IoT systems and services, and the *risks and harms* that derive from those specific contexts and uses.

Further, due to the market failure of the current de facto IoT privacy and security MoCs – the Notice and Choice framework (Chapter 3) and the FTC's application of its regulatory authority (Chapter 8.2) – the IoT ecosystem will benefit from a research endeavor that defines IoT privacy and security risks, harms, and baseline standards. Such work can be used by policymakers to improve the de facto IoT privacy and security MoCs. This proposal seeks to resolve paradigm shift 3 by developing and publishing such specific baseline IoT privacy and security standards.

The IoT Lab will serve to analyze and categorize IoT systems and services for the purpose of developing domain-specific operational and technical privacy and security standards. The Lab should endeavor to define context-specific risks and harms, and the functional standards to alleviate them. These standards should be published and distributed throughout the IoT community. Further, they can serve a secondary purpose: to inform policymakers regarding the specific risks and harms associated with IoT use-contexts and domains, and the steps necessary to limit those risks and harms. In doing so, this body of clear, narrow, and specific IoT standards can provide effect control for both operational IoT privacy and security as well as the larger policy and regulatory environment.

Three existing endeavors can serve as potential models for this IoT Lab: Microsoft's IoT & AI Insider Lab, the OneLab Federation's FIT-IoT Lab and NITLab, and University of New Hampshire's InterOperability Laboratory. These labs will be particularly useful models for designing the **Technical Analysis** process described in Subsection 9.4.3

9.4.1 Purpose

The IoT Lab has three primary goals.

1. To design a process that evaluates IoT technologies, systems, and services in order to define …
   - … contextual privacy and security risks.
   - … harms that derive from the use of IoT technologies, systems, and services.
   - … harms that derive from the use of the data associated with IoT technologies, systems, and services.
   - … baseline privacy and security requirements for IoT technologies, systems, and services.
   - … domain-specific IoT privacy and security requirements.
2. To create a taxonomy for IoT technologies, systems, and services based on …
   - … device function.
   - … how devices network or communicate.
   - … how devices use data.
   - … privacy or security risks or harms.
3. To contribute to the global IoT privacy and security policy discussion by …
   - … providing policymakers with specific recommendations to improve IoT privacy and security in narrow domains, whether by altering existing policies and regulations or engineering new policies and regulations.
   - … providing device manufacturers and service providers with concrete technical and operational steps and business models to improve IoT privacy and security for specific use-contexts.
   - … developing a series of publications related to IoT technology and policy.

9.4.2 Topics

The IoT Lab will involve the following technical topics:

1. IoT device, system, and service security (*security by design*).
2. IoT data privacy (*privacy by design*).

3. IoT system architecture.
4. Computer networks.
5. Network topology.
6. Network communications.
7. Network traffic analysis.

The IoT Lab will involve the following operational topics:

1. IoT business models and organizational policies.
2. Data and information regulations and national/international policies.
3. Legal frameworks that define liability and risk in the IoT ecosystem.
4. IoT technology use-contexts and scenarios.

9.4.3 Process

I recommend a six stage process for analyzing IoT systems and services: **Contextual Analysis**, **Technical Analysis**, **Operational Analysis**, **Risk and Harms Analysis**, and finally **Develop Standards**. The first three endeavors can be completed simultaneously for a single IoT system or service. The **Risk and Harms Analysis** will derive from the first three endeavors for a single IoT system or service. Finally, the **Develop Standards** process should emerge from the combined analyses of multiple IoT systems or services. I suggest that these standards fit within the contextual domain framework in Chapter 2.1; however, in operating the Lab there may emerge a more functional way to categorize IoT systems and services. In such a case, the high-level categories should serve as the differentiating factor for the IoT operational and technical standards.

There is a final process that will emerge from these endeavors: **Privacy and Security Enhancing IoT Business Models**. The IoT Lab should publish such business models alongside the operational and technical standards. These business models should be categorized by IoT system and service use-context, and should include technical as well as operational business considerations.

P1. Contextual Analysis

The contextual analysis for an IoT system or service should include a domain analysis and a complete stakeholder analysis (See Chapter 2). It should also include a case study regarding how the system or service is operationalized, as well as a review of the existing regulatory and policy environment that impacts the IoT system or service.

P2. Technical Analysis

The technical analysis for an IoT system or service should involve a full technical study of the system or service in operation. This process involves using the system in an environment that reveals the technical aspects of the system functions. For most IoT systems, this means creating a physical lab that can conduct network and traffic analysis, penetration testing, and reverse engineering. Further, it is important to conduct this technical testing in both an isolated scenario (i.e. a control test), a partial connected scenario (i.e. a LAN with other lab-controlled systems), and an open-connected scenario (i.e. full system operation connected to external/uncontrolled networks).

P3. Operational Analysis

The operational analysis for an IoT system or service should involve a study of how each system function operates, how the system networks with other systems or services, how the system collects data, how the system processes data internally, how the system transmits the data, what data the system transmits, and what is done with that data. Further, the operational analysis should also involve an analysis of the business operations of the device manufacturer and service provider as it relates to the specific system (See Appendix G).

P4. Risk and Harms Analysis

Once the contextual, technical, and operational analyses are completed, the IoT system in question must undergo a risk and harms analysis.

Risk assessments are notorious for their challenging application to socio-technical domains such as those inhabited by many IoT systems. However, there are a few popular risk frameworks that the Lab could adjust for use in IoT systems.[2]

1. **Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)** – Includes the following assets in risk assessments: people, hardware, software, information and systems. While it is meant for organizational risk assessments, it can be modified to address socio-technical IoT systems.[35]
2. **Factor Analysis of Information Risk (FAIR)** – Designed to assess information risk and information security vulnerabilities. It provides a common taxonomy for risk, can be applied to single systems or entire organizations, and demonstrates how resources (time and money) impact information security.[105]
3. **National Institute of Standards and Technology's Risk Management Framework (NIST RMF)** – While NIST RMF is focused on risk mitigation, it does offer a framework to analyze organization risk factors and risk impacts. It can therefore be used to conduct a risk assessment of IoT business models.[203]
4. **National Institute of Standards and Technology's Internal Report 8062** – This new NIST internal report is titled "An Introduction to Privacy Engineering and Risk Management in Federal Systems" and provides a perspective on privacy risk analysis.[202]
5. **The Threat Agent Risk Assessment (TARA)** – Provides a perspective on the risks most likely to occur and includes a common taxonomy of information security threats.[208]
6. **The Social Amplification of Risk Framework (SARF)** – Because many IoT systems tend to be integrated socio-technical systems, this framework provides a perspective on the impacts that societal factors play on risk perception and communication.[174]
7. There are also IoT-specific risk assessment frameworks that should be reviewed including a risk-based information security framework for healthcare systems

[2] Analyzing existing risk frameworks and designing a functional IoT privacy and security risk assessment framework would be a beneficial research project and could serve as a reasonable Masters thesis topic for a future student.

[4], a threat taxonomy and security model for IoT systems [20], and an IoT security vulnerability threat model [55].

A harms analysis should be completed once the IoT system risk analysis is finalized. A harm is the effect of a vulnerability. A harms analysis answers the question, "What is the impact of this specific risk?" Harms can be realized through both malicious and benevolent actions, and tend to be framed in the context of a specific stakeholder. The Lab should develop its own harms analysis framework.[3]

P5. Develop Standards

The creation of functional IoT privacy and security standards requires multiple iterations of processes 1–4 for different IoT systems. I suggest the Lab chooses a single domain focus in order to develop contextual IoT privacy and security standards. For example, the Lab should start with the IoT domestic domain and choose a sample of IoT systems and services intended to be used in the home.[4] Then, the **Contextual Analysis**, **Technical Analysis**, **Operational Analysis**, and **Risk and Harms Analysis** should be completed for each system or service. Once each of these analyses is complete, the results can be compiled and refined into a context-specific IoT standard that includes operational, technical, and policy recommendations.

P*. Privacy and Security Enhancing IoT Business Models

An additional benefit of the IoT Lab processes is the results of such a comprehensive investigation into current IoT systems and services. Individual system and service analyses can be compared to find the most effective and privacy and security enhancing practices within specific IoT domains. Therefore, the IoT Lab can publish and champion a set of well-defined and specific business models that 1) are based in actual IoT case studies, 2) are proven to be operational and effective, and 3) encourage privacy and security enhancing activities in the IoT ecosystem.

[3] Designing a functional IoT harm framework would be a beneficial research project and could serve as a reasonable Masters thesis topic for a future student, and could be included in the IoT privacy and security risk assessment framework project.

[4] The study found in Appendix A includes a convenient list of IoT domestic devices worth investigating, as well as some IoT healthcare and IoT transportation devices.

Part IV

Appendices

Appendix A

Insights into Unsolicited Consumer Thoughts on IoT Device Privacy and Security: A Study[1]

Nathaniel H. Fruchter[2]
Brandon A. Karpf[2]
Ilaria Liccardi[2]
MIT CSAIL, Cambridge, MA, 02139

Abstract

With the growing popularity of internet-capable devices known as the Internet of Things (IoT), and the risks these devices pose for consumer data privacy and security (P&S), it is worthwhile to examine how consumers relate P&S risks. By understanding how IoT consumers conceptualize and communicate P&S concerns, researchers and developers can better decide how to secure risks and limit harms. We consider P&S together because privacy and security risks both result in similar harms to a consumer using IoT in the home–our study's subject.

In this study, we seek to understand how IoT consumers conceptualize and communicate their P&S concerns with home-IoT devices such as connected thermostats, security systems, smart watches, and personal assistant hubs. Our approach seeks to

[1] Submitted for acceptance to the 44th Research Conference on Communications, Information, and Internet Policy – TPRC 2017.

[2] Nathaniel H. Fruchter, Brandon A. Karpf and Ilaria Liccardi were supported by the William and Flora Hewlett Foundation grant.

specifically understand if and how consumers advertise P&S concerns as they interact with devices in a modern marketplace. In this way, we can better understand the potential efficacy of consumer control mechanisms for P&S.

We collected a corpus of 160,000 consumer posts about 87 popular IoT products on Amazon.com. We analyzed the corpus with a combination of natural language processing techniques [25] and qualitative human-based methods [170]. Our analysis seeks to **(i)** determine if P&S is a common discussion topic; and **(ii)** identify what types of P&S issues are salient to consumers and whether that classification is impacted by device category or other factors. We can conclude that, for the most part, consumers who discuss these devices online tend to not discuss privacy or security. Among the subset of consumers who do discuss P&S concerns, we find that discussions tend to occur in relation to healthcare and tracking devices, and discourse centers around three themes: consumer knowledge, tradeoffs and thresholds, and the scope of data collection.

A.1 Introduction

Computing and sensing devices have become ubiquitous within our homes, vehicles, consumer products, and workplaces. The adoption of such devices will only increase given the value that they create for users and developers.[39][148] However, these devices have been shown to lack reasonable privacy and security controls and/or features.[75] These shortcomings are due in part to ill-defined standards [75], often compounded by fundamental characteristics of IoT devices, e.g. *the integration of networked sensing into everyday things, the difficulty of de-identifying or anonymizing data, the propensity for devices to hold security vulnerabilities, and the challenge of obtaining meaningful consent for data usage and collection.*[171]

In this work we seek to determine if consumers consider or report on privacy or security concerns when they review, investigate, or discuss an IoT device. We are interested in understanding and identifying people's opinions, possible concerns, and views about their own IoT devices. To do this, we explore several questions:

1. Do users discuss privacy and/or security factors when reviewing or asking about a product?
2. When privacy and/or security factors are present, what are people's major concerns? Can we determine trends or patterns in these concerns?

3. More broadly, how do these findings influence the future privacy and security landscape of IoT?

First, we provide an overview of how we created a realistic corpus to analyze, including product selection and categorization. Second, we outline data collection and analysis. Third, we present our results. Finally, we discuss potential outcomes for regulators, developers and consumers. The outcome of this work has the potential to provide insights for policy and standards creation for device manufacturers, regulators, and consumers of IoT devices. It will also further the privacy and security research agenda by analyzing realistic concerns of current and active users of these devices.

A.1.1 Background and prior work

There is a clear and growing concern within the technical and policy communities regarding privacy and security implications of IoT devices.[127] Past privacy and security research has shown consumers to be unaware, uninterested, or uninformed when it comes to privacy and security issues [5, 179], whether due to misconceptions [214] or lack of expertise [181, 179]. In fact, some consumers even choose to use or add device features that infringe upon their privacy and security rights in order to gain functionality.[132] However, much of the prior research and studies in this domain involve what consumers say, not necessarily how they act in their private lives. Further, little work has been completed that explores how consumers interact with the market of IoT devices in the context of privacy and security. It is important to start this exploration by examining consumer's primary IoT privacy and security concerns. In doing so, the research community can engineer usable privacy and security controls for the IoT ecosystem.

A.2 Study Design and Methodology

In order to investigate the presence and the substance of privacy and security issues in IoT devices, we chose to use and analyze data from Amazon.com. For this study, we use Amazon reviews, along with question and answer threads from Amazon's product

Table A.1: List of the fifteen IoT device categories defined for this study.

IoT Device Categories		
Health–Scale	Health–Watch	Hub–Router
Light–Bluetooth	Light–WiFi	Light–Zigbee
Media–Audio	Media–TV	Security
Sensor	Thermostat	Tracker–Car
Tracker–Items	Utilities–Irrigation	Utilities–Switch

Q&A forums, to investigate the following research questions:

A.2.1 Research Questions

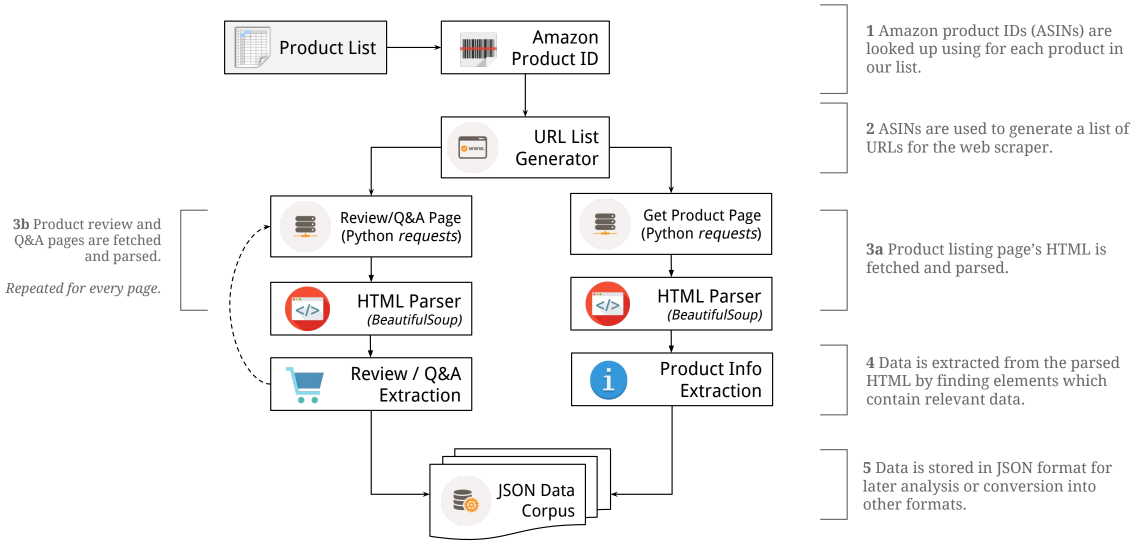
RQ1: Do users consider privacy and/or security factors when reviewing a recently purchased IoT device? Do users consider privacy and/or security factors when asking questions about IoT devices?

RQ2: When privacy and/or security factors are present, what are people's major concerns?

Product Information

We selected products in a multistage process. Our device search was limited to consumer-facing products that provide a service or functionality to a person or group in the home. We first found all products from iotlist.co that were posted for sale on Amazon.com. We combined this list with devices found under Amazon's *Electronics* category. We narrowed the resulting list to those products with 100 or more reviews, except in categories where most products had fewer than 100 Amazon reviews. Once this process was complete, we had a list of 87 IoT devices (see Table A.5).

We categorized the 87 devices using a combination of factors such as device function, Amazon category, and manufacturer description. We developed fifteen device categories based on these factors (Table A.1). Finally, we conducted an online search for news reports on each of the 87 devices to determine which have had publicized privacy or security faults, incidents, or vulnerabilities since 2010. 42 of the devices


Product List
Amazon Product ID
URL List Generator
Review/Q&A Page (Python *requests*)
Get Product Page (Python *requests*)
HTML Parser (*BeautifulSoup*)
HTML Parser (*BeautifulSoup*)
Review / Q&A Extraction
Product Info Extraction
JSON Data Corpus

1 Amazon product IDs (ASINs) are looked up using for each product in our list.

2 ASINs are used to generate a list of URLs for the web scraper.

3b Product review and Q&A pages are fetched and parsed.

Repeated for every page.

3a Product listing page's HTML is fetched and parsed.

4 Data is extracted from the parsed HTML by finding elements which contain relevant data.

5 Data is stored in JSON format for later analysis or conversion into other formats.

Figure A-1: Block diagram for the Amazon.com reviews and Q&A scraper. The scraper takes in a product list, generates a list of URLs to scrape, and then parses each page's HTML to extract relevant data for this study.

have had such a publicized event (see Table A.5). For each product, we collected basic metadata (name, vendor, listed category, availability date, and star rating), price, and when the product was first made available on Amazon.com.

A.2.2 Gathering a Realistic Data Corpus

We initially gathered the entire corpus of reviews, questions, and answers from each of the 87 devices. For the purpose of this study we only used reviews which were tagged as *verified purchase* so to analyze reviews based on real purchases. All Q&As were used as we wished to include both existing and potential consumers for a product. In total, we created a dataset with n = 119,414 reviews and n = 40,618 Q&A threads.

Review Data

We collected the complete set of Amazon reviews for our list of 87 devices. The metadata collected about each review included the review text, title, reviewer's name, and review type (verified purchaser), review ID, review date, and review score (1 to 5 stars). A web scraping system based on Python's *requests* HTTP client and *BeautifulSoup* HTML parser was used to locate each product's description page based on its *Amazon Standard Identification Number* (or ASIN; see Figure A-1).

Q&A Data

Amazon also offers a Q&A forum that allows potential customers to ask questions about products. Experts, owners, and vendors are able to answer these questions in a bulletin board-like format. Therefore, where available[3], we used our scraping system in Figure A-1 to scrape Q&A threads for the 87 devices. The system functioned in parallel to the review scraper and downloaded pages of questions based on each product's ASIN. As this data may provide insight into consumers' pre-purchase concerns and lines of thinking, it could serve as a valuable resource to gauge whether privacy and security are pressing concerns for those thinking of buying into the home-IoT market.

A.2.3 Data Processing and Analysis

We used a combination of natural language processing techniques and human-based methods to identify a subset of our review/Q&A corpus that reported privacy and security issues. The natural language processing first involved identifying only those reviews and Q&As that contained at least one privacy and security keyword. Then, a subset of the resulting corpus was read to determine which keywords were ambiguous by device category. Any review or Q&A thread with only the ambiguous keywords was also discarded. Once data processing was complete, a subset of privacy and/or security related reviews and Q&As remained called the P&S Reviews (n = 3,448) and the P&S Q&As (n = 649). Finally, these P&S subsets were manually read and tagged to determine common topics and trends.

[3] For products with more than 1000 posted Q&As, Amazon only allows access to the 1000 most recent questions.

Table A.2: Keywords used to identify potential privacy or security related reviews and Q&A threads.

Privacy and Security Keyword Dictionary

abuse
access
breach
confidential
control
creepy
crime
cyber
damage
data
ethic
fbi
fear
freedom
government
hack
harm
individual
information
insurance
law
leak
legal
loss
malware
monitor
nsa
permission
personal
physical
police
privacy
protection
rights
secret
security
snowden
spy
state
storage
surveillance
technology
terrorism
third party
threat
track
unauthorized
violate
violence
virus
vulnerability

Privacy and Security Tailored Keywords

We created a dictionary with 51 keywords to be used to identify P&S reviews and Q&A threads. These keywords, found in Table A.2, are a broad set of privacy and security related terms. Several iterations were used to create the appropriate set of keywords included in Table A.2. The authors discussed and identified common terms used often associated with privacy or security concern, opinions and attitudes. A set of keywords generated from prominent privacy and security related events and media coverage were also included in the dictionary.[4]

This keyword dictionary was designed to be over-broad. Given that each review and Q&A thread that contained a keyword would be read by at least two researchers, the false positives that were erroneously tagged could later be discarded. We were more interested in identifying *possible* privacy and security-related discussions rather than discarding relevant ones in the tagging process. False negatives would impact the validity of our research.

[4] The words from prominent privacy and security related events were: breach, confidential, crime, cyber, FBI, hack, malware, NSA, security, snowden, surveillance, third party, unauthorized, virus, and vulnerable.

In some categories, common privacy and security keywords could be used to refer to a fundamental function and/or feature of the device itself. For example, the keyword *leak* in the category *Utilities-Irrigation* is a word often used to describe a specific factor of the device, i.e. a water leak. This resulted in an ambiguity with certain keywords for some categories. Therefore, we chose to tailor the keywords to each device category. We call these category-specific keywords the *unambiguous keywords*. We removed the keywords *damage* or *leak* from the Utilities-Irrigation category, the words *individual, personal* or *loss* from the Health-Scale category, the words *control* or *monitor* from the Media-TV category, the word *security* from the Security-Camera category, and the word *track* from the Tracker-Car and Tracker-Item categories. This was done in order to isolate discussions that do not contain their categories' ambiguous keywords.

A.2.4 Automated Language Analysis

The text of each captured item – review and Q&A thread – was processed through stemming and lemmatization functions to ensure that all derivative forms of the privacy and security keywords were considered during the tagging process. We then used part-of-speech tagging functions to identify the subset of reviews and Q&As that had at least one privacy and security keyword reported in their own body. We searched for the 51 keywords within the 119,414 captured reviews and the 40,618 Q&As. We then applied the category-tailored set of *unambiguous keywords*, removing possible ambiguous category-specific terms. The result consisted of 3,448 reviews and 649 Q&A threads that did not contained their category's ambiguous privacy and security keywords. We call these subsets the P&S Reviews and the P&S Q&As. By identifying the P&S Reviews and the P&S Q&As dataset, we minimized the appearance of false negatives and increased the probability that every manually coded review reported privacy and security opinions, concerns, and views.

Table A.3: Topic tags used to manually code the P&S Reviews.

Tag	Definition
Personal Experience	Discusses a personal experience with the device related to privacy or security.
News Related	Reference to a publicized privacy or security event in the media.
Knowledgeable	Demonstrates technical knowledge beyond what might be considered average.
Security Threshold	Discusses the user's threshold for acceptable security violations.
Privacy Threshold	Discusses the user's threshold for acceptable privacy violations.
Setup	Discusses the setup procedures of the device.
Data Scope	Discusses the scope of data collection.
Perpetual Collection	Discusses the perpetuity with which the device collects data.
Interface	Discusses the device's or service's user interface.
Usability	Discusses the device functions ease of use or data accessibility.
Security Usability	Discusses systems security and the use of security products with the device.
Security Feature	Discusses security features as part of the device.
Physical Security	Discusses security concerns in the context of physical security.
Functionality Tradeoff	Discusses product features as important features for the device's functionality, but which might also decrease the privacy or security of the device.
Consumer Harm	Discusses potential consumer harms created by the device.
Product Reviews	Discusses other online product reviews or the product reviewing system.
Customer Service	Discusses an experience with the company's customer service department.
App Concern	Discusses concerns with privacy or security in related smartphone applications.

Manual Topic Analysis

We first manually read a small pseudo-random subset of P&S Reviews (n = 100) and P&S Questions (n = 100) in order to establish a common protocol for tagging different topics. Table A.3 is the complete list of topics we used to tag the P&S Reviews. In addition to the coding tags in Table A.3, we tagged each review as *Positive* or *Negative* in terms of its dominant emotion.[5] We also noted the presence of any of the following secondary emotions: *uncomfortable, pleased, comical, frustrated, fearful, excited, and angry.* We then read the P&S Reviews in order to tag each body of text. This step also ensured the removal of false positives given the broad keyword dictionary. It is important to note that a single review could have multiple tags. In fact, most of the P&S Reviews have at least three different tags.

In reading the pseudo-random P&S Q&A subset, we determined that Q&A data is less conducive to fitting common topic tags than the P&S Reviews. This fact is because Q&A threads tend to be a single sentence that lacks detail, whereas a device review tends to be a paragraph that includes many specifics. This lack of detail led to a far greater number of false positives in the P&S Q&A dataset (88.90%) than in the P&S Reviews dataset (17.02%). Further, our manual topic analysis revealed that the reviews proved to be a far more information-rich body of data than the Q&As. We found that the most effective approach to the P&S Q&As was to simply verify that the Q&A thread did relate a privacy or security concern. In doing so, we could still answer RQ1: P&S consideration. We chose to not do a more comprehensive topic analysis on the P&S Q&A dataset.

A.3 Results

A.3.1 RQ1 - Presence of privacy or security discussions

Privacy and security is not a topic often reported in Amazon IoT device reviews or Q&A threads. Of the 119,414 captured reviews, only 3,448 (2.89%) contained at least one unambiguous keyword with a false positive rate of 17.02%. Of the 40,618 captured Q&A threads, only 649 (1.60%) contained at least one unambiguous keyword with a large false positive rate of 88.90%. Overall, these results suggest that IoT device privacy or security concerns are rarely expressed, questioned, or *openly* considered by consumers in an IoT marketplace. Future work needs to be completed to determine

[5] Positive reviews relate to a 4-5 star rating, Negative reviews relate to a 1-2 star rating, and neutral reviews relate to a 3 star rating.

Table A.4: Number of P&S Reviews and P&S Q&As, and percentage of total collected reviews and Q&As, by device category.

Device Category	**Reviews**	**% P&S**	**Q&As**	**% P&S**
Health–Scale	8,918	17.45%***	1,357	4.27%*
Health–Watch	12,648	0.87%	6,968	3.76%
Hub–Router	26,035	1.77%	4,990	0.70%
Light–Bluetooth	1,629	1.66%	615	0.49%
Light–WiFi	1,163	4.64%	990	0.81%
Light–Zigbee	1,697	1.30%	1,450	0.69%
Media–Audio	1,663	1.74%	998	0.60%
Media–TV	8,051	0.53%	5,146	0.16%
Security	33,382	2.00%	8,242	1.04%
Sensor	680	1.18%	406	3.94%
Thermostat	13,504	1.98%	4,169	0.58%
Tracker–Car	631	8.87%***	703	7.68%***
Tracker–Items	1,145	1.40%	509	10.41%***
Utilities–Irrigation	1,877	2.18%	912	0.77%
Utilities–Switch	6,391	1.41%	3,163	0.60%
All Devices	119,414	2.89%	40,618	1.60%

*Statistically significant to the 0.05 probability level.

** Statistically significant to the 0.01 probability level.

*** Statistically significant to the 0.001 probability level.

if consumers still consider P&S issues and just push them aside, or if most consumers do not even consider P&S issues to begin with.

We did find that certain device categories and specific devices have statistically significant incidences of P&S Reviews and P&S Q&As. Table A.4 shows these numbers by device category and Table A.5 shows these numbers by individual device. For example, the Health-Scale category had by far the highest occurrence of P&S Reviews at 17.45% (significant to the 0.001 probability level). In fact, each of the six devices within the Health-Scale category had statistically significant occurrences of P&S Reviews to the 0.001 probability level, while only one of the six devices has ever had a publicized privacy or security incident (see Table A.5). The devices that have statistically significance occurrences of P&S discussion are those in the Health-Scale, Tracker-Car, and Tracker-Item categories.

42 of the 87 devices have had publicized privacy or security incidents (Table A.5). However, we found no correlation between which devices have had publicized privacy or security incidents and those devices or categories with statistically significant numbers of P&S Reviews or P&S Q&As. Therefore, we suspect that the general absence of P&S discussion in device reviews and Q&As demonstrates two factors. First, insofar as consumers *are* concerned with P&S issues, those issues do not relate to actual events. Instead, they relate to personal perceptions of risk. For example, the devices in the Health-Scale category collect data that people perceive to be particularly private, such as weight, and devices in the Tracker-Car category collect data that people perceive to be particularly sensitive, such as location.

Second, these results and findings demonstrate a broad lack of significant consumer concern with or understanding of common privacy or security issues. Even though nearly half of the devices studied have had publicized privacy or security issues, consumers appear to be relatively unaware or unconcerned with these issues. Previous research has reported this same effect when consumers interact with mobile devices [193] and in social media networks [133]. Further, the time distribution of the P&S Reviews and P&S Q&As matched the time distributions of the entire set of normal reviews and Q&As for each device category – suggesting that there is no relationship for when consumers discuss P&S concerns. For example, neither the 2014 Sony hack, the 2015 Samsung Smart TV privacy policy scandal, nor the 2016 Mirai botnet correlated with any increase in the number of P&S Reviews or Q&As for any device category (all of these events had a statistical significance below the 0.95 probability level).

We can conclude that, for the most part, consumers who purchase, consider purchasing, or openly discuss these IoT devices online tend to not discuss privacy or security concerns. Insofar as these consumer do discuss privacy or security concerns, they mostly do so in regards to devices in the Health-Scale and Tracker categories.

Table A.5: The 87 IoT devices, organized by device category, with their total number of reviews, percentage of total reivews that are P&S reviews, total number of Q&A threads, and percentage of total Q&A threads that are P&S Q&As.

Category	**Device**	**Reviews**	**% P&S**	**Q&As**	**% P&S**
Health–Scale	Easy@Home Smart Scale	550	16.73%***	111	3.60%**
	Fitbit Aria Smart Scale†	4,680	17.41%***	416	5.53%***
	Taylor Smart Scale	217	12.90%***	50	4.00%***
	Weight Gurus Bluetooth	1,381	15.79%***	420	4.05%***
	Weight Gurus Digital	1,412	19.33%***	100	5.00%***
	Yunmai	678	19.17%***	260	2.69%
Health–Watch	Apple Watch Sport†	776	2.06%	1,459	3.63%**
	Generic Smartwatch	306	0.98%	481	0.83%***
	Fitbit Surge†	5,996	0.50%	1,051	9.61%
	LEMFO	610	0.16%	524	0.57%
	Misfit Wearables Shine 2	195	2.56%	60	10.00%***
	Padgene DZ09†	993	0.60%	1,189	0.50%
	Pebble†	2,819	1.21%	1,051	4.85%***
	Samsung Gear S†	360	2.78%	472	1.69%
	Smart Watch GT08	88	1.14%	240	0.83%
	Sony SWR50	505	0.79%	441	6.35%***
Hub–Router	Amazon Echo†	20,769	1.65%	1,960	0.41%
	CUJO Smart Firewall	115	25.22%***	30	10.00%***
	eero Home WiFi System	910	0.44%	731	0.55%
	Panasonic KX-HNB600W	7	0.00%	–	–
	Samsung SmartThings†	753	3.72%	651	0.92%
	Securifi Almond+†	1,746	0.52%	567	0.71%
	singlecue Gen 1	90	4.44%	30	0.00%
	TP-Link OnHub AC1900	571	3.15%	560	0.54%
	Wink Connected Home†	915	2.40%	271	2.21%
	Wink Relay†	159	1.89%	190	0.53%
Light–Bluetooth	Flux	204	3.43%	100	0.00%
	MagicLight	1,094	1.19%	434	0.69%
	MIPOW E26	148	4.05%	61	0.00%

Continued on next page

Table A.5 – *Continued from previous page*

Category	Device	Reviews	% P&S	Q&As	% P&S
	SunLabz	183	0.55%	20	0.00%
Light–WiFi	emberlight	57	0.00%	20	5.00%***
	LIFX†	170	1.76%	60	0.00%
	Philips 426353 Hue†	775	5.03%*	460	1.52%
	TP-Link Smart Wi-Fi A19†	161	7.45%***	450	0.00%
Light–Zigbee	GE Link Wireless A19†	1,143	0.87%	517	0.19%
	Philips 259945 Hue†	147	0.68%	93	1.08%
	Philips Hue LED†	407	2.70%	840	0.95%
Media–Audio	SONOS CONNECT†	513	2.92%	278	0.00%
	SONOS PLAY:1†	1,150	1.22%	720	0.83%
Media–TV	LG Electronics 43LH5700	129	0.00%	265	0.00%
	Samsung UN40J5200†	2,037	0.69%	1,384	0.22%
	Sony KDL40R510C	546	0.37%	746	0.00%
	TCL 32S3800	4,838	0.54%	1,676	0.18%
	VIZIO D40-D1†	501	0.20%	1,075	0.19%
Security	Amcrest 960H†	1,434	1.19%	1,149	0.70%
	Amcrest IP2M-841†	4,300	1.21%	1,206	1.82%
	ANNKE HD	43	4.65%*	40	0.00%
	Chamberlain MYQ-G0201†	913	0.99%	540	0.74%
	D-Link DCS-960L HD†	202	7.43%***	80	0.00%
	EZVIZ Home Security	82	2.44%	325	1.54%
	Foscam FI8910W†	7,330	3.12%	982	1.43%
	Foscam FI9821PB†	1,067	2.53%	430	1.16%
	Logitech Circle	173	2.89%	241	1.24%
	Nest Cam†	4,109	2.21%	710	1.41%
	Netatmo Welcome†	68	5.88%***	52	0.00%
	Ring Doorbell†	11,948	1.41%	1,258	0.48%
	Schlage Connect BE469NX	1,357	1.25%	937	0.75%
	Zmodo Greet Doorbell	62	1.61%	60	0.00%
	Zmodo Pivot	294	9.86%***	232	0.86%
Sensor	D-Link DCH-S160†	158	1.27%	91	4.40%***

Continued on next page

Table A.5 – *Continued from previous page*

Category	**Device**	**Reviews**	**% P&S**	**Q&As**	**% P&S**
	Aeotec ZW100-A MultiSensor	119	1.68%	120	0.83%
	Samsung SmartThings Arrival†	139	2.88%	30	0.00%
	Samsung SmartThings Multi†	164	0.00%	102	0.00%
	Samsung SmartThings Leak†	100	0.00%	63	17.46%***
Thermostat	Allure EverSense	26	0.00%	10	0.00%
	ecobee3	2,175	3.40%	651	0.61%
	Honeywell Lyric†	30	3.33%	60	0.00%
	Honeywell RTH9580WF1005†	2,179	1.33%	982	0.51%
	Honeywell Wi-Fi Thermostat†	93	4.30%	102	0.98%
	Nest Learning Thermostat†	6,810	1.73%	1,124	0.36%
	Sensi UP500W	2,191	1.92%	1,240	0.81%
Tracker–Car	Automatic AUT-350C	27	3.70%	371	5.93%***
	Automatic: 3G Connected Car	442	5.20%**	92	6.52%***
	Carlock OBD	29	0.00%	44	11.36%***
	Vyncs Connected OBD	21	0.00%	163	11.04%***
	Zubie ZK30012M†	112	28.57%***	33	9.09%***
Tracker–Items	MYNT Smart Tracker	491	0.61%	180	10.00%***
	Tagg Pet GPS Plus	322	1.86%	120	11.67%***
	Tile Slim	120	1.67%	155	7.74%***
	XY3 Finder	212	2.36%	54	16.67%***
Utilities–Irrigation	Blossom Smart Watering	216	0.93%	62	0.00%
	Orbit 57946 B-hyve Sprinkler	189	1.59%	140	0.00%
	Rachio Smart Sprinkler	904	1.99%	310	0.97%
	RainMachine HD-16	568	3.17%	400	1.00%
Utilities - Switch	TP-Link Smart Plug†	1,785	1.85%	1,812	0.39%
	Wemo Light Switch†	816	1.84%	1,351	0.89%
	Wemo Switch Plug†	3,790	1.11%	–	–

*Statistically significant to the 0.05 probability level.

** Statistically significant to the 0.01 probability level.

*** Statistically significant to the 0.001 probability level.

† Devices that have had privacy or security issues publicized by popular media since 2010.

A.3.2 RQ2 - Main P&S concerns and popular topics

Once we established that consumers typically do not discuss privacy or security concerns in relation to IoT devices, we wanted to determine if there exists any trends or patterns in the limited set of discussions that do involve privacy or security concerns. As mentioned above, the Q&A threads proved to be a shallow dataset that lacked significant detail, so we focused our efforts to determine P&S discussion trends exclusively on the P&S Reviews dataset.

We discovered several common privacy and security concerns, views and opinions within the Amazon reviews for the 87 IoT devices. These common trends relate to user knowledge, privacy or security tradeoffs and thresholds, and data collection.[6]

Overall Sentiment: Of the 3,448 P&S Reviews, half (50%) ultimately rated the device negatively when speaking about privacy and security, while 45.5% reported a positive sentiment of reassurance and safeguard. The remainder (4.5%) did not report any clear feeling.

Knowledge and Understanding: 38.6% of the P&S Reviews showed a high level of technical understanding of the devices. While these reviews reported privacy or security concerns about the product, in some cases they also provided suggestions on how to address possible privacy or security issues. R45 suggests *"[. . .] if you use public wifi your password can be "sniffed" out [. . .] I personally plan on setting up the camera for viewing through a VPN."*

Among the P&S Reviews that expressed technical knowledge, 47.1% were negative and 41.2% were positive. Those that were positive often gave reasons to be positive, such as the fact that the device uses a function or feature that was developed to safeguard their privacy or security. For example, R3 reports the fact *"[. . .] that Eero is actively updating the router software gives me hope that this router will be resistant to malware"*. The remainder (11.7%) did not express a clear sentiment.

Tradeoffs and Thresholds: 27.3% of the P&S Reviews discussed a tradeoff between device functionality and the reviewer's own privacy or security. In these,

[6] It is important to note that a review could receive a combination of tags, the only mutually exclusive tags are *Positive* and *Negative*

the reviewer viewed the trade for functionality as primarily a positive factor (75.0% positive and only 25.0% negative). For example, R16 identified a possible breach to their own privacy and security when reviewing a D-Link camera, stating, *"not sure about the security and [. . .] the risk that others can accidentally access your feed"*. Despite these concerns, R16 reported satisfaction (*"[. . .] this camera earned these five stars"*) and continued use. This kind of reaction may be due to a lack of knowledge and understanding of possible repercussions resulting from the breach of one's own privacy or security. R16 reported knowledge gaps by admitting not to be *"techy enough to know the ins and outs"*. When the same product was reviewed by an individual (R25) with a technical background, the item not only scored a low star rating but was also flagged as a vulnerable product, citing how *"firmware in the camera [needs] a MANDATORY web browser plugin"* which doesn't with *"the Chrome browser nor with Firefox [. . .] [and] will not work behind a proxy server"*.

While 27.3% of the P&S Reviews discussed a functionality tradeoff, an additional 15.9% of the P&S Reviews reported a specific privacy or security threshold in relation to this tradeoff, and that the devices had breached the threshold of a reasonable compromise for their own privacy or security. For example R41 reported that the Flux Smart Light Bulb *"[. . .] requires access to personal files and media on the device as well as location [. . .] a BT light bulb should not need access to these types of sensitive information"* This unreasonable tradeoff led R41 to purchase another device that *"[. . .] will continue to function if you deny access"*. Only 28.6% of these reviews that specifically described a privacy or security threshold were positive.

Data Collection: 20.5% of the P&S Reviews reported concerns related to data collection. 9.1% of the P&S Reviews had concerns with the *kind* of data collected and the *purpose* of use (all were rated negatively). 11.4% of the P&S Reviews reported concerns with *perpetual collection* of data. Different from the reviews that reported concern over *type* and *purpose* of data, these review that discussed *perpetual collection* had a majority with positive sentiment (83.3%).

This result may indicate that people would recommend and are happy with devices that engage in perpetual data collection, even though these devices might infringe upon their own privacy and security. For instance R40 reports, *"I really don't like the idea of it [Echo] always listening [. . .] how do we know it's truly muted and it's not still recording in some way?"*. Despite these concerns R40 concludes with *"[. . .] very happy [. . .] Alexa is the pleasant and helpful side of AI."* For R40, the concerns inherent in perpetual data collection were not significant enough to alter use of the device.

In another example, while R14 was *"disturbed"* by the prospects of perpetual collection by the Amazon Echo, this review still considered the device positively: *"[. . .] it's a little creepy that it records and you can play back everything you say [. . .] but I can get past that [. . .] Overall, this is a fantastic product"*. However, there were some who viewed perpetual collection negatively. For example, the perpetuity of collection by the Nest Cam device led R730 to declare *"This is a complete invasion of privacy initiated by one company to sell your behavior and habits to third parties!"*.

Discomfort: 11.4% of the P&S Reviews demonstrated some discomfort with privacy or security features. Of those reviews tagged as demonstrating discomfort, 60.0% were positive and 40.0% were negative.

Satisfaction: 15.9% of the P&S Reviews voiced a high degree of satisfaction with the device. All reviews tagged as voicing pleasure were also tagged as positive.

Excitement: 13.6% of the P&S Reviews voiced a high degree of excitement with the device. All reviews tagged as voicing excitement were also tagged as positive.

Harms: 25.0% of the P&S Reviews discuss consumer harms related to privacy or security. Of those reviews tagged as discussing a consumer harm, 36.3% were tagged as positive and 63.7% were tagged as negative.

P&S Discourse

We also observed that when users discuss the same issues, they tend to discuss them in the same way using similar words. For example, reviews that only contained the keywords *creepy* and *access* also mention tradeoffs between functionality and privacy. Similarly, 17 P&S Reviews contain the keyword *creepy* as well as the word *cool.* 13 of the *creepy-cool* reviews discuss perpetual data collection. These reviews describe the functions related to perpetual data collection as both *creepy* and *cool*. Therefore, this finding supports the result above that found most P&S Reviews related to perpetual data collection to also be positive. Further, these results align with Shklovski et al.'s analysis of privacy perceptions in the mobile app space – specifically those related to the perceived creepiness yet simultaneous continued use of mobile applications that conduct perpetual data collection.[194] They conclude that the better alignment of user and engineering values requires value-sensitive engineering design and deliberately changing informational norms.[194] Our initial result supports an expansion of their conclusions beyond the mobile app space and into the consumer-device and IoT ecosystem.

A.4 Discussion

Our study reveals that few consumers discuss IoT P&S concerns online when reviewing the actual devices that often embody those P&S issues. This result suggests that consumers are either not concerned or not informed about IoT device P&S. Why this is the case–and what it tells us about consumers' role in securing the IoT ecosystem–is relevant for P&S policy. Consumer control mechanisms for improving IoT P&S–like the notice and choice framework–may not secure risks or limit harm. If the market cannot rely on consumers to act in a P&S enhancing way, the development of more private and secure IoT devices should not be left solely to consumer influence. Prior work in the domain shows that consumers tend to be unaware, uninterested, or uninformed [5] of P&S harms, whether due to risk perception [214] or level of expertise [179]. These results combined with our findings have implications for policy makers, standards organizations, and P&S advocates since it demonstrates a consumer control limitation in the IoT domain.

We draw additional conclusions about common P&S concerns, the time series nature of these discussions, the relationship between P&S discussions and devices or device types, and the correlations between P&S discussions and publicized P&S events such as the Mirai Botnet. This paper represents the first steps in an endeavor that includes consumer interviews and surveys to draw more definitive conclusions on IoT product demand and consumer P&S concerns.

Consumers' opinions, views, and concerns over home-IoT devices are varied and depend on 1) knowledge and understanding of possible privacy and security repercussions and 2) an individual‘s own balance between (and limits on) invasion of privacy or degradation of security compared with convenience and necessity. While some consumers reported privacy or security vulnerabilities with several devices, and while 42 of the 87 devices in this study have had serious publicized privacy or security failures, few consumers actually discussed these issues and even fewer seemed willing to alter their use of the devices.

We acknowledge that our study involves a significant selection bias. By collecting online device reviews and Q&As, we have limited the extent to which we can extrapolate our results to a larger population. However, the results of this study still hold great relevance. Online device reviews serve as a way for other consumers to evaluate devices for purchase, and for manufacturers and developers to receive feedback on their systems. Further, while our study subjects represent only those consumers who have purchased the IoT devices, and other consumers may have been deterred from purchasing the IoT devices for P&S concerns, the size of our sample demonstrates that there exists significant demand for these devices by consumers that rarely express any P&S concerns. Such significant demand, and a lack of open discourse regarding P&S concerns, suggests two major issues. First, that IoT device manufacturers and developers might lack the market incentives to improve the privacy or security of their systems. Second, that potential IoT device consumers might lack the information needed to make privacy- or security-enhancing market decisions. Such a misalignment of incentives leads to market failure.

A.4.1 Creating More Informed Policy

It is important to consider our study results within the broader context of the policymaking and regulatory communities. Calls to examine the impact of IoT trends on public policy domains – including privacy, security, and consumer protection –

have increased over the past few years. For example, congressional representatives have introduced bills that mandate P&S provisions in connected devices.[152][159] Further, agencies such as the Federal Trade Commission (FTC) [75][78], Department of Commerce [47], and the Department of Homeland Security [48] have signalled their intent to tackle IoT P&S risks.

Within these environments, understanding consumer sentiment is a powerful tool for policymakers who intend to create a more usable and secure IoT ecosystem. A recent request for comment from the FTC and National Highway Traffic Safety Administration (NHTSA) highlights the importance of developing such consumer sentiment analysis tools for IoT contexts.[183] This request inquires about a variety of vehicular IoT-related concerns, including several in regards to consumer behavior and perceptions. The request asks about consumer perception and the intersection of vehicular and home-IoT systems: *"What privacy and security issues might arise from consumer operation of connected vehicles, including use of third-party aftermarket products [. . .] [and what] evidence exists regarding consumer perceptions of connected vehicles?"*

While this direct inquiry about consumer behavior and perception is rare from the FTC (the authors were able to locate one other similar request, and only in the the food-safety realm [76]), attention to issues of consumer behavior and sentiment by regulators and policymakers will benefit the policy process. Insights driven by our investigation into IoT consumer sentiment – such as the relative sensitivity that consumers express for their vehicular tracking data, or consumers' willingness to trade data privacy for increased functionality in IoT systems – are able to directly address the questions posed by the FTC and NHTSA. In this vein, we see our project as relevant to the broader policy discussion on addressing IoT P&S challenges. Increased consideration of consumer behavior and sentiment in these policymaking discussions will serve to benefit consumers, regulators, and policymakers; doing otherwise would ignore a wealth of real-world evidence on how to address privacy, security, and consumer protection challenges in the IoT ecosystem.

A.4.2 Future work

We are interested in secondary sources of P&S concern. Work by Shih et al. reviews instances where smartphone apps can be a source of unmanaged data leaks.[193] These fears are shared by a subset of consumers in our study. To analyze these concerns, we have begun to collect smartphone apps associated with the devices on our list to characterize the apps' use of permissions and personal data. This analysis will allow us to examine the relationship between sentiment and legitimate P&S threats. Combined with our coded P&S datasets, we believe that this data can contribute to ongoing discussions about the usability of privacy and security in IoT systems.

A.5 Conclusion

In this study, we sought to understand how IoT consumers communicate P&S concerns with home-IoT devices. By leveraging a corpus of consumer product reviews and Q&A threads from Amazon.com, we were able to provide one of the first pictures of how consumers discuss P&S concerns as they interact with devices in a modern marketplace.

We can conclude that, for the most part, consumers who discuss these devices online tend to not discuss privacy or security concerns. Insofar as these consumer do discuss privacy or security concerns, they mostly do so in regards to devices in the *Health–Scale* and *Tracker* categories. This finding shows that concerns may stem from personal perceptions of risk instead of a risk assessment of a broader scope.

Among the subset of consumers who openly discuss P&S concerns, we find that discussion centers around three themes: consumer knowledge, tradeoffs and thresholds, and data collection. Our analysis of the P&S Reviews corpus demonstrates that consumers with a high level of technical knowledge do comprehend more nuanced P&S challenges and discuss them openly in reviews. We also show that this subset of consumers is mindful of tradeoffs made between device functionality and P&S harms. These tradeoffs are framed in terms of personal harms, as well as harms related to the scope and purpose of data collected by the device.

Appendix B

HIPAA Criteria for PHI

According to HIPAA, protected health information (PHI), also known as individually identifiable health information, is ...

> "information, including demographic data, that relates to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number)
>
> ...
>
> The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer
>
> ...
>
> There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways

> to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual."

The 18 types of information that must be removed from individually identifiable health information for it to be considered de-identified (From the Human Research Project Program at the University of California San Francisco) are:

1. Names
2. All geographical subdivisions smaller than a state, including street address, city, county, precinct and zip code
3. All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date and date of death
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate and license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web URLs
15. IP address numbers
16. Biometric identifiers, including fingerprints and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code

Appendix C

ISO/IEC 27k Series Standards Related to IoT

Table C.1: The IoT-relevant ISO/IEC 27k series standards.[1]

Standard: Year Written	Title and Topic
ISO/IEC 27000:2016	Information security management systems - Overview and vocabulary
ISO/IEC 27001:2013	Information security management systems - Requirements
ISO/IEC 27002:2013	Code of practice for information security controls
ISO/IEC 27003:2010	Information security management system implementation guidance
ISO/IEC 27004:2009	Information security management - Measurement
ISO/IEC 27005:2011	Information security risk management
ISO/IEC 27006:2015	Requirements for bodies providing audit and certification of ISMS
ISO/IEC 27007:2011	Guidelines for information security management systems auditing
ISO/IEC 27008:2011	Guidelines for auditors of information security controls
ISO/IEC 27009:2016	Sector-specific application of ISO/IEC 27001 - Requirements
ISO/IEC 27010:2015	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011:2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013:2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014:2013	Governance of information security
ISO/IEC 27015:2012	Information security management guidelines for financial services
ISO/IEC 27016:2014	Information security management - Organizational economics
ISO/IEC 27017:2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2014	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27019:2013	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
ISO/IEC 27799:2016	Health informatics - Information security management in health using ISO/IEC 27002

[1] List was adapted from a publication titled "Protecting Information Assets Using ISO/IEC Security Standards."[61]

Nothing to see here. Move along.

Appendix D

oneM2M Release 2 Standards

Table D.1: oneM2M Release 2 Standards

Reference	Version	Title	Date
TS 0001	2.10.0	Functional Architecture	Aug-16
TS 0002	2.7.1	Requirements	Aug-16
TS 0003	2.4.1	Security Solutions	Aug-16
TS 0004	2.7.1	Service Layer Core Protocol	Aug-16
TS 0005	2.0.0	Management Enablement (OMA)	Aug-16
TS 0006	2.0.1	Management Enablement (BBF)	Aug-16
TS 0007	2.0.0	Service Components	Aug-16
TS 0009	2.6.1	HTTP Protocol Binding	Aug-16
TS 0010	2.4.1	MQTT Protocol Binding	Aug-16
TS 0011	2.4.1	Common Terminology	Aug-16
TS 0012	2.0.0	oneM2M Base Ontology	Aug-16
TS 0014	2.0.0	LWM2M Interworking	Aug-16
TS 0015	2.0.0	Testing Framework	Aug-16
TS 0020	2.0.0	Websocket Protocol Binding	Aug-16
TS 0021	2.0.0	oneM2M and AllJoyn Interworking	Aug-16
TS 0023	2.0.0	Home Appliances Information Model and Mapping	Aug-16
TS 0024	2.0.0	OIC Interworking	Aug-16
TR 0001	2.4.1	Use Cases Collection	Aug-16
TR 0007	2.11.1	Study of Abstraction and Semantics Enablements	Aug-16
TR 0008	2.0.0	Security	Aug-16
TR 0012	2.0.0	oneM2M End-to-End Security and Group Authentication	Aug-16
TR 0016	2.0.0	Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies	Aug-16
TR 0017	2.0.0	Home Domain Abstract Information Model	Aug-16
TR 0018	2.0.0	Industrial Domain Enablement	Aug-16
TR 0019	2.0.0	Dynamic Authorization for IoT	Dec-16
TR 0022	2.0.0	Continuation & integration of HGI Smart Home activities	Aug-16
TR 0024	2.0.0	3GPP Release 13 Interworking	Aug-16

Nothing to see here. Move along.

Appendix E

National Privacy Research Strategy Research Questions[1]

E.1 NPRS Challenge 2

Research questions for Challenge 2: "Understand and measure privacy desires and impacts."

1. What research methods most reliably and validly sample, measure, and represent people's privacy desires, expectations, attitudes, beliefs, and interests in one or more communities?
2. To what extent do privacy desires, expectations, attitudes, beliefs, and interests vary by generation, by cultural subgroup, by national interest, by socioeconomic status, or by other demarcations?
3. How and why do privacy desires, expectations, attitudes, beliefs, and interests change? Among groups or subgroups, do certain factors influence the emergence of privacy expectations and beliefs regarding privacy more than others, and if so, why?
4. What incentives can effectively promote privacy and the adoption of privacy-enhancing technologies, policies, and practices?
5. What impacts have privacy incentives had on the full range of social values such

[1] There are no research questions associated with Challenge 1: "Influence of Context on Privacy"

as social justice, economic growth and security, and innovation?

6. To what extent do incentives, such as sharing personal data for access to “free” services, modulate privacy expectations, attitudes, beliefs, and interests?
7. What methods and technologies could identify privacy events and other privacy impacts effectively and efficiently? What methods would be effective for disclosing this information to affected parties and systems?
8. How do privacy events become regarded as privacy harms by individuals or groups? How can privacy harms be recognized, measured, and assessed?
9. How do privacy events affect peoples’ behavior? How can the “chilling effects” of privacy events be measured?
10. What information and methods can effectively inform and enable decisions regarding people’s privacy desires in the policy, regulatory, and legislative domains?
11. To what extent does the public understand how technological and economic factors affect their privacy, and to what extent do people understand power and information asymmetries between individuals and data collectors/users?
12. How do different privacy desires, expectations, attitudes, beliefs, and interests in other countries (if they exist) drive any differences in privacy laws and regulations?
13. What kinds of formalisms could define privacy objectives and impacts, and what techniques and metrics could be used to measure how information processing systems meet those objectives?
14. How can the relationship of privacy objectives and other objectives of individuals, organizations, and society be understood and assessed?
15. How can the effects of privacy policy approaches on privacy incidents and markets, both domestically and internationally, be evaluated?

E.2 NPRS Challenge 3

Research questions for Challenge 3: “Develop system design methods to incorporate privacy desires, requirements, and controls.”

1. How can privacy risk be modeled to support privacy risk identification and management?
2. What kinds of system properties can be associated with privacy to support the implementation of privacy principles and policies?
3. How should privacy properties be characterized, and how can they be assessed or quantified?
4. What privacy design patterns and use cases describe common solutions that would assist system designers, particularly in emerging areas such as smart cyber-physical systems and the Internet of Things?
5. How can privacy-enhancing cryptographic technologies be developed to scale, as well as be integrated into the functional requirements and standards that are already widely adopted in systems?
6. What metrics can be used to assess the effectiveness of privacy controls?
7. How can privacy risk be considered and controlled in concert with system and data utility needs?
8. What metrics and measurements can measure both privacy and system utility, to understand the tradeoffs between the two, and to support the development of systems that can maximize both?

E.3 NPRS Challenge 4

Research questions for Challenge 4: “Increase transparency of data collection, sharing, use, and retention.”

1. What type(s) of experimental studies and field trials should be used to discover information asymmetry?
2. Can tools or automated systems be built to measure and report information

flows? Is it possible to measure such flows without inherently producing more privacy risk?

3. What techniques could be effective in informing individuals about the information practices of data collectors/users, and in informing data collectors/users about the desires and privacy preferences of individuals?
4. How can the format and lexicon for describing data practices across industries be standardized, taking into account the inevitability of changes in technology over time? What other measures could improve individuals' ability to compare data practices across the range of data collectors/users, thereby encouraging competition on privacy issues?
5. What might be the appropriate level of transparency and choice for prospective changes to data-handling practices? How can the impact of these changes be measured?
6. How can individuals be provided with notice about the practices of data collectors that collect and use data without directly interacting with individuals?
7. How can notice and choice be standardized and conveyed in ways that facilitate automation and reduce transaction costs for users and stakeholders?
8. How can privacy policies be improved to ensure reader comprehension, including examination of the efficacy of disclosure attributes such as text, font, and icons or graphics?
9. How can data collectors/users provide meaningful notice of their data practices on mobile and similar devices? How effective are "just-in-time" disclosures?
10. In what situations is the traditional notice-and-choice approach ineffective without other types of protections?
11. How should the effectiveness of transparency mechanisms be evaluated?

E.4 NPRS Challenge 5

Research questions for Challenge 5: "Assure that information flows and use are consistent with privacy rules."

1. What are usable methods for specifying and managing information-flow based controls?
2. How can hardware or software methods for establishing trustworthy execution environments support secure management of information flows and compliance with privacy policies?
3. Can methods for tracking, assuring, and archiving the provenance of data and software components be used to assure privacy compliance?
4. Can data provenance be implemented in a way that does not itself violate privacy?
5. What program analysis methods can be developed for various kinds of information flow properties and privacy policy languages that are meaningful to legal experts, yet have precise semantics that system developers can use to restrict and provide accountability for how their code operates on personal information of users?
6. Are there effective methods for understanding the flow of personal data through systems of computer programs?
7. In what ways can privacy rules for the results of data processing be derived from privacy rules of the inputs, processing, and context?
8. How can the change in value or sensitivity of data, as they are combined with other information, be accounted for and properly acted upon by information processing systems?
9. Can access control systems that incorporate usage-based and purpose-based constraints be adapted to the range of privacy issues now faced by system designers?
10. Are there effective information disclosure controls, methods for de-identifying data, and means for assessing these de-identification methods?
11. Can anonymous and pseudonymous computing, computing with obscured or encrypted data, and management of multiple identities be made efficient and practical?
12. Can existing Internet infrastructure and protocols be redesigned to better sup-

port privacy (i.e., support anonymous, censorship-resistant, and metadata-hiding communications)? Can privacy be built into core Internet services without adversely affecting cybersecurity?

E.5 NPRS Challenge 6

Research questions for Challenge 6: "Develop approaches for remediation and recovery."

1. What technological mechanisms would effectively remediate a privacy event?
2. How can the effectiveness of remediation and recovery mechanisms be evaluated in terms of their financial, psychological, and societal impact?
3. What effect does the existence of remediation and recovery mechanisms have on the likelihood of privacy events?
4. What effect does the use of remediation and recovery have on the investment in more robust privacy technologies?
5. How could privacy-protecting and privacy-recovery technologies be integrated to create more effective and efficient solutions?

E.6 NPRS Challenge 7

Research questions for Challenge 7: "Reduce privacy risks of analytical algorithms."

1. In what ways do analytical algorithms and systems that act upon the results of the algorithms adversely affect individuals or groups of people?
2. What types of concerns do individuals have with respect to analytical and predictive algorithms, and what information do they need to address these concerns? How can this information be effectively conveyed to an individual?
3. How can the provenance, accuracy, and quality of data used in making a decision or a prediction about an individual or groups be assessed?
4. How can the compatibility between datasets and analytical algorithms be assessed?

5. What are the impacts on individuals or groups when analytical algorithms use erroneous or inaccurate data?
6. How can the decisions or predictions made by analytical algorithms be measured and assessed for compliance with legal requirements?
7. How can analytical algorithms be designed to provide increased transparency, accountability, and auditing, and to minimize adverse effects on individuals or groups? What are practicable algorithm discovery and intervention mechanisms for individuals, the government, and industry?
8. What are the impacts of analytical algorithms on individuals' autonomy and agency (i.e., the ability to make independent and free choices)? In what ways do analytical algorithms create a structure that determines, affects, or limits decisions by individuals?
9. How can new technologies and algorithms, and combinations of technologies and algorithms, provide practical and theoretical privacy-preserving data analysis?

Nothing to see here. Move along.

Appendix F

2016 FTC Privacy and Security Enforcement Actions[1]

F.1 Information Privacy

1. Settlement against the operators of *Ashley Madison*, a dating site that lured users with fake profiles, had lax data security practices, misrepresented the effects of a "full delete" service, and falsified a "Trusted Security Award."
2. Settlement against *Turn Inc.*, a mobile ad network who misrepresented their ability and operations that tracked users' mobile internet traffic, as well as had opt-out mechanisms that were not effective.
3. Settlement against *Gigats.com*, an education lead generator who misrepresented how they utilized private user data.
4. Settlement against *Practice Fusion*, a cloud-based electronic health record company who misrepresented how they utilized patient information and publicly disclosed private patient health data (to include full name, medications, health conditions, and treatments received).
5. Settlement against *InMobi*, a Singapore-based mobile advertising company who tracked the locations of hundreds of millions of consumers without their consent, including when users specifically denied permission to use location information.

[1] Adapted from [77].

6. Settlement against *Vulcun*, a technology company who essentially used their acquisition of a web browser game to install applications directly to consumers' mobile phones without consent.
7. Charged *Tachht Inc.*, a marketing operation, with illegally spamming consumers with fake products and false endorsements.
8. Issued twelve warning letters to app developers who use software that monitors television use through audio beacons that consumers cannot hear but the software can detect. The letters stated that the app developers must clearly notify consumers that they are collecting and transmitting viewing data.
9. Order against *Sequoia One*, a data broker who falsely obtained consumer information and sold that data to a scam that manipulated users' bank accounts and credit cards without their consent. The order effectively executed the operation.

F.2 Data Security

1. Settlement against the operators of *Ashley Madison*, a dating site that had lax data security practices, falsified a "Trusted Security Award," failed to have a written information security policy, had no reasonable access controls, no security training of employees, and no knowledge of how third party services used their data.
2. Order against *LabMD*, a medical testing lab that had unreasonable data security practices and shared sensitive user medical information.
3. Order against *ASUS*, a Taiwan-based computer hardware maker whose routers had major security flaws that compromised the networks of hundreds of thousands of consumers, and used insecure cloud services that compromised consumer devices and exposed personal information.
4. Settlement against *Henry Schein Practice Solutions*, an office management software provider for dental practices who falsely advertised the encryption its software used to protect patient data.
5. Order against *Oracle* who failed to update a security flaw in its Java Platform

that allowed malware to access usernames and passwords for financial accounts and allowed hackers to obtain information through phishing attacks.

F.3 Rule Creation

Since the year 2000, the FTC has created the following information privacy and security rules:

1. **The Health Breach Notification Rule** – Web-based businesses must notify consumers when the security of their electronic health information is breached.
2. **The Red Flags Rule** – financial institutions and creditors must utilize identity theft prevention programs to identify, detect, and respond to patterns, practices, or activities that indicate possible identity theft.
3. **The COPPA Rule** – websites and apps must obtain parental consent before collecting personal data from children under 13.
4. **The GLBA Privacy Rule** – car dealerships must provide consumers with a privacy policy and practices and allow consumers to opt out of information sharing with third parties.
5. **The GLBA Safeguards Rule** – financial institutions must develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards.
6. **The Disposal Rule** – (Under FACTA, the FCRA amendment) companies must dispose of credit reports and the information derived from them in a safe and secure manner.

Nothing to see here. Move along.

Appendix G

IoT Business and Systems Operational Analysis Framework

The following framework should be used in conjunction with the IPRI IoT Lab in order to analyze the business models and service structures associated with a device's use context. Each category includes suggested standards and associated scores. The term "controlling documents" refers to the terms of use, privacy and data policies, and contracts that control the use of the system or service.

G.1 Focus 1 – Business Model

Readability

5. Controlling documents use no jargon or legalease and are easy to comprehend by the configured user. Sets the industry standard.
4. Controlling documents are user friendly. Might include some industry jargon but does not include legalease. Easy to comprehend by the configured user.
3. Controlling documents incorporate some industry jargon and legalease. Still possible to comprehend with some extra digging required.
2. Controlling documents include a lot of industry jargon and legalease. Requires extra reading and searches to fully comprehend.

1. Controlling documents are full of jargon and legalease. Impossible for the intended user to understand OR information is unavailable.

Accessibility

5. User is directed to the controlling documents. Documents are exceptionally easy to navigate. Sets industry standard.
4. User is directed to the controlling documents. Documents include table of contents, but navigation of the documents could be improved.
3. User is not directed to the controlling documents. Documents are available with searching
2. User is not directed to the controlling documents. Documents available with searching. Navigation of the documents is not user friendly.
1. User is not directed to the controlling documents. Documents are not available.

Responsibility

5. Controlling documents explicitly state the responsibility and liability of the company and product. Sets industry standard.
4. Controlling documents include some discussion of responsibility and liability and how the company and product address user concerns.
3. Controlling documents include some discussion of either responsibility or liability, and how the company and product address user concerns.
2. Controlling documents make some mention of either responsibility, liability, or user concerns.
1. Controlling documents do not mention responsibility, liability, functions, or user concerns OR information is unavailable.

Legitimacy

5. Controlling documents clearly state the product's P&S practices and attempt to fully disclose its functions. Details are verifiable. Sets industry standard.

4. Controlling documents state the product's P&S practices and functions. Not all details are verifiable.
3. Controlling documents make some attempt to state P&S practices and functions of the product. Not verifiable.
2. Controlling documents make marginal attempt to state P&S practices and functions of the product. Not verifiable.
1. Controlling documents make no attempt to state P&S practices and functions of the product. OR information is unavailable.

Notification

5. Company has detailed, planned, and published notification and incident response procedures. Sets industry standard.
4. Company has published notification and incident response procedures. Not quite to industry standard.
3. Company claims to have notification and incident response procedures. They are not published but are available when asked.
2. Company claims to have notification and incident response procedures. They are not published and are unavailable when asked.
1. Company does not claim to have any notification or incident response procedures even when asked. OR information is unavailable.

Information Sharing

5. Controlling documents detail all types and amounts of collected data that are shared, who it is shared with, and why, and what data would be exchanged if the product or company were to change ownership. Sets industry standard.
4. Controlling documents discuss the types and amounts of data that are shared, who it is shared with, and what data would be exchanged if the product or company were to change ownership.
3. Controlling documents make some mention what data is shared, who it is shared with, and what data will be transferred if the product or company were to

change ownership, but do not provide more detail.

2. Controlling documents mention that data is shared and will be transferred if the product or company were to change ownership, but does not describe specific types of data.
1. No mention that data will be transferred if the product or company were to change ownership.

G.2 Focus 2 – Privacy Practices

Scope

5. Product only collects data as required by its purpose. Sets industry standard.
4. Product provides some limitations to its collection, storage, usage, and distribution of data. Collects slightly beyond what its purposes require.
3. Product provides some limitations to its collection, storage, usage, and distribution of data. Collects far beyond what its purposes require.
2. Product provides marginal limitations to its collection, storage, usage, and distribution of data. Collects far beyond what its purposes require.
1. Product does not provide limits to the type and quantity of collected data. Product does not limit usage, distribution, or storage of data. OR information is unavailable.

User-defined

5. Obvious mechanisms are provided for the user to actively manage the mode of data collection and communication (on/off, limited, etc). Sets the industry standard.
4. Some mechanism is provided to change the mode of data collection and communication. Mechanism may not be obvious, simple, or effective and may diminish the functionality of the device.
3. Some mechanism is provided to change the mode of data collection and communication. Mechanism is not obvious, simple, and effective, and may diminish

the functionality of the product.

2. Limited mechanism provided to change the mode of data collection and communication. Mechanism is not obvious, simple, or effective and diminishes the functionality of the product.
1. Product does not provide any mechanism for the user to manage the mode of data collection and communication.

Product-defined

5. Product itself is designed to actively manage what types of data it collects, communicates, stores, when those actions take place, and in what contexts. Engineered specifically to protect the privacy of the user. Sets the industry standard.
4. Product has some form of inherent ability to manage what types of data it collects, communicates, stores, when those actions take place, and in what contexts.
3. Product has some limited ability to manage what types of data it collects, communicates, stores, when those actions take place, or in what contexts.
2. Product has some marginal ability to either manage what types of data it collects, communicates, or stores, or when those actions take place, or in what contexts.
1. Product has no inherent ability to manage the types of data it collects, communicates, stores, and when.

Data Accessibility

5. All data collected and stored as a function of the product is accessible, amendable, and able to be eliminated by the user in its entirety. The method to accomplish this task is well defined and easy to follow relative to the function of the product. Sets the industry standard.
4. Most data collected and stored as a function of the product is accessible, amendable, and able to be eliminated by the user. The method is well defined and

somewhat easy to follow.

3. Current data collected and stored as a function of the product is accessible, amendable, and able to be eliminated by the user. The method is defined and somewhat easy to follow.
2. Some data collected and stored as a function of the product is accessible, amendable, and able to be eliminated by the user. The method is not easy to follow.
1. No data, or limited data, collected and stored as a function of the product is accessible, amendable, and able to be eliminated by the user. Any method is highly challenging to follow.

Consent

5. Product requests and requires user consent prior to storing and transporting new forms of data, exchanging ownership of new forms of data, altering policies and the controlling documents, and prior to the installation of updates. Sets the industry standard.
4. Product requests consent or provides clear notification prior to storing and transporting new forms of data, exchanging ownership of new forms of data, altering policies and the controlling documents, and prior to the installation of updates.
3. Product provides clear notification prior to storing and transporting new forms of data, exchanging ownership of new forms of data, altering policies and the controlling documents, or prior to the installation of updates.
2. Product provides some type of notification prior to storing or transporting new forms of data, exchanging ownership of new forms of data, altering policies or the controlling documents, or prior to the installation of updates.
1. Product does not request consent or provide notification prior to storing and transporting new forms of data, exchanging ownership of new forms of data, altering policies or the controlling documents, or prior to the installation of updates.

G.3 Focus 3 – Security Practices

Update

5. Company publishes and maintains an update plan (either reactive or planned), clearly adheres to that plan, and includes known security patches in those updates. Sets the industry standard.
4. Company maintains an update plan and clearly adheres to that plan. Not as robust as the industry standard, but still effective in provided known security patches.
3. Company claims to have an update plan, does not publish said plan but does adhere to some type of update schedule.
2. Company does not publish an update plan and does not clearly adhere to any plan. Updates are sporadic.
1. Company does not publish or maintain an update plan, does not clearly adhere to any set plan or schedule, or does not include known security patches in its updates OR information is unavailable.

User-defined

5. Product or company provides the user with a detailed risk and harm assessment as it relates to specific settings and functions of the product. Security settings are easily adjusted by the user. Sets the industry standard.
4. Product or company provides some type of risk or harm assessment as they relate to the product. Product security settings are adjustable within reasonable limits.
3. Product or company may provide risk or harm assessments. Product security settings are somewhat adjustable within reasonable limits.
2. Product or company does not provide risk or harm assessments. Product security settings are somewhat adjustable within reasonable limits.
1. Product or company does not provide any risk or harm assessments. Settings are not adjustable.

Product-defined

5. Product clearly incorporates in its settings, and suggests and explains to the user in its documentation, the use of best-practice security techniques. Sets the industry standard.
4. Product incorporates in its settings and attempts to explain to the user the best-practice security techniques, as applicable to its functions.
3. Product incorporates in its settings and provides some explanation to the user about the best-practice security techniques, as applicable to its functions.
2. Product incorporates in its settings or explains to the user a few best-practice security techniques, as applicable to its functions.
1. Product does not incorporate in its settings or explain to the user any best-practice security techniques, as applicable to its functions.

Support

5. Company openly commits to and declares its plan to support the product for a defined life cycle. Company has a history of adhering to those commitments. Lifecycle is comparable to the industry standard for products with a similar purpose. (90-100%)
4. Company openly commits to and declares its plan to support the product for a defined life cycle. Lifecycle is somewhat shorter than the industry standard for products with a similar purpose.
3. Company commits to a plan to support the product for a defined life cycle. Lifecycle is shorter than the industry standard for products with a similar purpose. (50-75%)
2. Company has a plan to support the product for a defined life cycle. Lifecycle is much shorter than the industry standard for products with a similar purpose. (25-50%)
1. Company has either not committed to a life cycle support plan for the product, company fails to adhere to the support plan for the product, or the life cycle is a

great deal shorter than products with a similar purpose (0-25%) OR information is unavailable.

Setup

5. The product's initialization procedures and default settings require the creation of individualized security features, as applicable, and limit the architecture's reliance on false trust assumptions. Sets the industry standard.
4. The product's initialization procedures and default settings incorporate individualized security features, as applicable, but may rely on a few false trust assumptions in its architecture.
3. The product's initialization procedures and default settings incorporate a few individualized security features, as applicable, and rely on a few false trust assumptions in its architecture.
2. The product's initialization procedures and default settings incorporate limited individualized security features, as applicable, and rely on a number of false trust assumptions in its architecture.
1. The product's initialization procedures and default settings do not incorporate individualized security features and does not limit the architectures reliance on false trust assumptions or information is unavailable.

Nothing to see here. Move along.

Bibliography

[1] 360is. *ISO 27001, how do we prepare and what does it cost?* 2015. URL: https://360is.blogspot.com/2015/02/iso-27001-how-do-we-prepare-and-what.html (visited on 02/15/2017).

[2] *A Reference Architecture for the Internet of Things.* 2016. URL: https://www.infoq.com/articles/internet-of-things-reference-architecture (visited on 02/21/2017).

[3] Wiem Abderrahim. "The Multi-Dimensional Model for Dependability Assurance in Cloud Computing". In: *Proceedings of the Wireless Communications and Mobile Computing Conference* (2016), pp. 133–138.

[4] Habtamu Abie and Ilangko Balasingham. "Risk-based Adaptive Security for Smart IoT in eHealth". In: *Proceedings of the 7th International Conference on Body Area Networks.* 2012, pp. 269–275.

[5] Alessandro Acquisti and Jens Grossklags. "Privacy and Rationality in Individual Decision Making". In: *IEEE Security & Privacy* 2.2005 (2005), pp. 24–30.

[6] Ahmed Banafa. "Securing the Internet of Things (IoT)". In: *Issues in Information Systems* 17.4 (2016), pp. 21–28.

[7] Ziyad Alshaikh et al. "Process Improvement in Governmental Agencies: Toward CMMI Certification". In: *2015 IEEE International Symposium on Software Reliability Engineering Workshops* (2015), pp. 168–173.

[8] Tariq Alshugran and Julius Dichter. "Extracting and Modeling the Privacy Requirements from HIPAA for Healthcare Applications". In: *IEEE Systems, Applications and Technology Conference* (2014).

[9] Tariq Alshugran, Julius Dichter, and Miad Faezipour. "Formally expressing HIPAA Privacy Policies for Web Services". In: *IEEE International Conference on Electro/Information Technology* (2015), pp. 295–299.

[10] Rajeev Alur et al. “Systems Computing Challenges in the Internet of Things”. In: *Computing Community Consortium* (2015).

[11] Thomas L. Ambro. *Federal Trade Commission v. Wyndham Worldwide Corporation.* 2015.

[12] Ross Anderson and Tyler Moore. “The Economics of Information Security: A Survey and Open Questions”. In: *Science* 314 (2006), pp. 610–613.

[13] Ross Anderson and Tyler Moore. “Information Security Economics – and Beyond”. In: *Advances in Cryptology.* 2008.

[14] Juhani Anttila et al. “Integrating ISO/IEC 27001 and Other Managerial Discipline Standards with Processes of Management in Organizations”. In: *Proceedings - 7th International Conference on Availability, Reliability and Security* (2012), pp. 425–436.

[15] Taylor Armerding. *NIST’s Finalized Cybersecurity Framework Receives Mixed Reviews.* 2014. URL: http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html (visited on 02/20/2017).

[16] David G Armstrong et al. “Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of “Medjacking””. In: *Journal of Diabetes Science and Technology* 10.2 (2016), pp. 435–8.

[17] AT&T. *The CEO’s Guide to Securing the Internet of Things.* Tech. rep. 2016.

[18] Secretary’s Advisory Committee on Automated Personal Data Systems. *Records, Computers and the Rights of Citizens.* 1973. URL: https://epic.org/privacy/hew1973report/default.html (visited on 03/02/2017).

[19] Axelos. *The Key Benefits of ITIL: For the Organization and the Professional.* Tech. rep.

[20] Sachin Babar et al. “Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)”. In: *Recent Trends in Network Security and Applications: Third International Conference.* Ed. by Natarajan Meghanathan et al. 2010, pp. 420–429.

[21] G. Baldini et al. “Ethical Design in the Internet of Things”. In: *Science and Engineering Ethics* (2016).

[22] Kenneth A. Bamberger and Deidre K. Mulligan. “Privacy on the Books and on the Ground”. In: *Stanford Law Review* 63 (2011), pp. 247–316.

[23] C.J. Bennett. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press, 1992.

[24] Kathy Bergen. *Chicago seeking 'smart-city' tech solutions to improve city life*. 2016. URL: `http://www.chicagotribune.com/news/globalcity/ct-chicago-smart-city-global-city-20160421-story.html` (visited on 04/12/2017).

[25] Steven Bird, Edward Loper, and Ewan Klein. *Natural Language Processing with Python*. O'Reilly Media Inc., 2009.

[26] Violet Blue. *FTC vs D-Link: All bark, no bite*. 2017. URL: `https://www.engadget.com/2017/01/13/ftc-vs-d-link-all-bark-no-bite/` (visited on 05/08/2017).

[27] Alessio Botta et al. "Integration of Cloud computing and Internet of Things: A Survey". In: *Future Generation Computer Systems* 56 (2016), pp. 684–700.

[28] Alina Bradford. *Why smart toilets might actually be worth the upgrade*. 2016. URL: `https://www.cnet.com/how-to/smart-toilets-make-your-bathroom-high-tech/` (visited on 02/15/2017).

[29] Russell Brandom. *FCC Chairman Pai Rushes to Block New Privacy Rules*. 2017. URL: `http://www.theverge.com/2017/2/24/14727418/fcc-privacy-rules-stay-ajit-pai-net-neutrality` (visited on 03/07/2017).

[30] Chris Brook. *Travel Routers, NAS Devices Among Easily Hacked IoT Devices*. 2017. URL: `https://threatpost.com/travel-routers-nas-devices-among-easily-hacked-iot-devices/124877/` (visited on 05/08/2017).

[31] Mary Butler. "Is HIPAA Outdated? While Coverage Gaps and Growing Breaches Raise Industry Concern, Others Argue HIPAA is Still Effective". In: *Journal of AHIMA* 88.4 (2017), pp. 14–17. URL: `http://bok.ahima.org/doc?oid=302073#.WQDEh1PyuAw` (visited on 04/26/2017).

[32] Fred H. Cate. "The Limits of Notice and Choice". In: *IEEE Security and Privacy* 8.2 (2010), pp. 59–62.

[33] Aileen Cater-Steel, Wui-Gee Tan, and Mark Toleman. "Challenge of Adopting Multiple Process Improvement Frameworks". In: *14th European Conference on Information Systems*. 2006.

[34] Vinton G Cerf et al. "IoT Safety and Security as Shared Responsibility". In: *Journal of Business Informatics* 1.35 (2016), pp. 7–19.

[35] CERT. *OCTAVE*. 2017. URL: `https://www.cert.org/resilience/products-services/octave/index.cfm` (visited on 05/09/2017).

[36] CMMI. *Security by Design with CMMI for Development, Version 1.3*. Tech. rep. May. CMMI Institute, 2013.

[37] CMMIFAQ. *How Long Does It Take?* 2014. URL: `http://www.cmmifaq.info/#16` (visited on 02/20/2017).

[38] CMMIFAQ. *How Much Does It Cost?* 2014. URL: `http://www.cmmifaq.info/#17` (visited on 02/20/2017).

[39] Louis Columbus. *Roundup Of Internet Of Things Forecasts And Market Estimates*. 2016. URL: `https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016`.

[40] Privacy Protection Study Commission. *Personal Privacy in an Information Society*. 1977. URL: `https://epic.org/privacy/ppsc1977report/` (visited on 03/02/2017).

[41] 73rd Congress. "Communications Act of 1934". In: *Pub. LA. No. 73–416, 48 Stat. 1064* (1934).

[42] ISO 27001 Consultant. *How Much Does ISO 27001 Certification Cost?* 2016. URL: `http://iso27001guide.com/blog/how-much-does-iso-27001-certification-cost/` (visited on 02/15/2017).

[43] Xavier Costa-Pérez et al. "Latest Trends in Telecommunication Standards". In: *Computer Communications Review* 43.2 (2013), pp. 64–71.

[44] Andy Crabtree and Richard Mortier. *Personal Data, Privacy and the Internet of Things: The Shifting Locus of Agency and Control*. Tech. rep. 2016.

[45] Lorrie F. Cranor. "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice". In: *Journal on Telecommunications and High Technology Law* 10 (2012), pp. 273–307.

[46] Lorrie F. Cranor et al. *Are They Worth Reading? An In-Depth Analysis of Online Trackers' Privacy Policies*. 2015.

[47] Department of Commerce. *U.S. Department of Commerce Releases Green Paper Proposing Approach for Advancing Growth of Internet of Things | NTIA*. 2017. URL: `https://www.ntia.doc.gov/press-release/2017/us-department-commerce-releases-green-paper-proposing-approach-advancing-growth` (visited on 05/10/2017).

[48] DHS. *Securing the Internet of Things*. 2016. URL: `https://www.dhs.gov/securingtheIoT`.

[49] DHS. *Strategic Principles for Securing the Internet of Things: Introduction and Overview*. 2016.

[50] DHS. *Strategic Principles for Securing the Internet of Things (IoT)*. 2016.

[51] Amadou Diallo. *Do Smart Devices Need Regulation? FTC Examines Internet Of Things*. 2013. URL: `https://www.forbes.com/sites/amadoudiallo/2013/11/23/ftc-regulation-internet-of-things/#5f3830628015` (visited on 02/15/2017).

[52] Georg Disterer. "ISO/IEC 27000 , 27001 and 27002 for Information Security Management". In: *Journal of Information Security* 4.April (2013), pp. 92–100.

[53] D-Link. *Npower Launches Smart Home Trial with D-Link and Other Leading Manufacturers*. 2016. URL: `http://www.dlink.com/uk/en/press-centre/press-releases/2016/february/25/npower-launches-smart-home-trial-with-dlink` (visited on 04/12/2017).

[54] D-Link. *Alliances and Accreditations*. 2017. URL: `http://us.dlink.com/us/en/service-provider-solutions/why-d-link/alliances-and-accreditations.html#Standards` (visited on 05/08/2017).

[55] Bruno Dorsemaine et al. "A New Approach to Investigate IoT Threats Based on a Four Layer Model". In: *13th International Conference on New Technologies for Distributed Systems*. 2016.

[56] Tony Doyle. "Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life". In: *The Journal of Value Inquiry* 45.1 (2011), pp. 97–102.

[57] Françius Ennesser and Yogendra Shah. *Security Solutions and Services for the IoT*. Tech. rep. oneM2M IoThink Series, 2016.

[58] EPIC. *Comments of the Electronic Privacy Information Center to the Federal Trade Commission on the Privacy and Security Implications of the Internet of Things*. 2013.

[59] L. Ertaul, A. Movasseghi, and S. Kumar. *Enterprise Security Planning with TOGAF-9*. 2011, pp. 2–7.

[60] Rodrigo Santos De Espindola, Edimara Mezzomo Luciano, and Jorge Luis Nicolas Audy. "An Overview of the Adoption of IT Governance Models and Software Process Quality Instruments at Brazil - Preliminary Results of a Survey". In: *Hawaii International Conference on System Sciences*. 2009.

[61] Lois Evans. *Protecting Information Assets Using ISO/IEC Security Standards*. Tech. rep. 2016.

[62] Karim Farhat. *Docket No. 160331306–6306–01: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*. Tech. rep. 2016. URL: https://www.ntia.doc.gov/files/ntia/publications/k_farhat_ntia_iot.pdf.

[63] FCC. "FCC proposes to give broadband consumers increased choice, transparency and security for their personal data". In: *FCC press releases* (2016).

[64] FCC. *Report and Order: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*. Tech. rep. 2016, pp. 13911–14129.

[65] Susan Feinstein. *What you need to know about medical privacy: HIPAA explained*. 2015. URL: http://www.consumerreports.org/cro/news/2008/12/hipaa/index.htm (visited on 02/15/2017).

[66] Senator Deb Fischer et al. *114th Congress, 1st Session, S. Res. 110: A resolution expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment*. 2015.

[67] Fitbit. *Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Capabilities*. 2015. URL: https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx (visited on 03/16/2017).

[68] National Science Foundation. *Cyber-Physical Systems (CPS)*. Tech. rep. Program Solicitation NSF 17-529, 2017.

[69] FTC. *Privacy Online: A Report to Congress*. Tech. rep. 1998, p. 63.

[70] FTC. *A Report To Congress – Privacy Online: Fair Information Practices in the Electronic Marketplace*. Tech. rep. 2000.

[71] FTC. *Preliminary FTC Staff Report – Protecting Consumer Privacy in an Era of Rapid Change*. Tech. rep. December. 2010.

[72] FTC. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policymakers*. Tech. rep. 2012.

[73] FTC. *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.* 2014. URL: https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc (visited on 05/08/2017).

[74] FTC. *IoT Privacy, Data Protection, Information Security*. Tech. rep. 2015.

[75] FTC. *IoT Privacy & Security in a Connected World*. Tech. rep. January. 2015.

[76] FTC. *FTC and USDA to Host Roundtable in Washington, D.C. on October 20, 2016, to Examine Consumer Perceptions of "Organic" Claims for Non-Agricultural Products.* 2016. URL: https://www.ftc.gov/news-events/press-releases/2016/08/ftc-usda-host-roundtable-washington-dc-october-20-2016-examine (visited on 05/10/2017).

[77] FTC. *Privacy & Data Security Update: 2016.* Tech. rep. December. 2016.

[78] FTC. *FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices | Federal Trade Commission.* 2017. URL: https://www.ftc.gov/news-events/press-releases/2017/01/ftc-announces-internet-things-challenge-combat-security (visited on 05/10/2017).

[79] FTC. *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras.* 2017. URL: https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate (visited on 05/08/2017).

[80] Vangelis Gazis. "A Survey of Standards for Machine to Machine (M2M) and the Internet of Things (IoT)". In: *IEEE Communications Surveys & Tutorials* (2016).

[81] Robert Gellman. *Fair Information Practices: A Basic History.* Tech. rep. 2016. URL: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[82] Diane L Gibson, Dennis R Goldenson, and Keith Kost. *Performance Results of CMMI®-Based Process Improvement.* Tech. rep. August. 2006.

[83] Danny Greefhorst. *TOGAF® & Major IT Frameworks - Architecting the Family.* May 2014. URL: https://www.slideshare.net/dannygreefhorst/togaf-cobit-itil-pmbok-10 (visited on 02/20/2017).

[84] Neil Gross. "The Earth Will Don An Electronic Skin". In: *Business Week* (1999). URL: https://www.bloomberg.com/news/articles/1999-08-29/14-the-earth-will-don-an-electronic-skin.

[85] The Open Group. *TOGAF® Usage Worldwide.* 2015. URL: http://www.opengroup.org/subjectareas/enterprise/togaf/worldwide (visited on 02/20/2017).

[86] The Open Group. *The Open Group Membership.* 2017. URL: http://reports.opengroup.org/membership_report_all.pdf.

[87] U.S. Department of Health and Human Services. *Covered Entities and Business Associates.* URL: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (visited on 02/15/2017).

[88] U.S. Department of Health and Human Services. *The HIPAA Privacy Rule*. URL: `https://www.hhs.gov/hipaa/for-professionals/privacy/` (visited on 02/15/2017).

[89] Congressional Hearing. *The Internet of Things: Exploring the Next Technology Frontier*. 2015.

[90] Congressional Hearing. *Understanding the Role of Connected Devices in Recent Cyber Attacks*. 2016.

[91] Senate Hearing. *The Connected World: Examining the Internet of Things*. 2015.

[92] Senate Hearing. *How the Internet of Things (IoT) Can Bring U.S. Transportation and Infrastructure into the 21st Century*. 2016.

[93] Alexander Hoerbst et al. "The Status of IT Service Management in health care – ITIL® in Selected European Countries". In: *BMC Medical Informatics & Decision Making* 76.11 (2011).

[94] Chris J. Hoofnagle. *Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems*. 2014. URL: `https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/` (visited on 03/02/2017).

[95] Chris J. Hoofnagle. *Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems*. Tech. rep. Berkeley Center for Law & Technology, 2014.

[96] Chris J. Hoofnagle. *Assessing the Assessments*. 2015. URL: `https://hoofnagle.berkeley.edu/2015/09/28/assessing-the-assessments/` (visited on 05/08/2017).

[97] Privacy Rights Clearing House. *Mobile Health and Fitness Apps: What Are the Privacy Risks?* 2013. URL: `https://www.privacyrights.org/blog/privacy-rights-clearinghouse-releases-study-mobile-health-and-fitness-apps-what-are-privacy` (visited on 02/15/2017).

[98] White House. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. Tech. rep. 2012.

[99] Carol Hsu, Tawei Wang, and Ang Lu. "The Impact of ISO 27001 Certification on Firm Performance". In: *Hawaii International Conference on System Sciences*. Vol. 49. 2016, pp. 4842–4848.

[100] Zhitao Huang, Pavol Zavarsky, and Ron Ruhl. “An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002”. In: *Proceedings of the IEEE International Conference on Computational Science and Engineering*. 2009, pp. 386–391.

[101] Syed Husain et al. “Recent Trends in Standards Related to the Internet of Things and Machine-to-Machine Communications”. In: *Journal of Information and Communication Convergence Engineering* 12.4 (2014), pp. 228–236.

[102] Syed Husain et al. “Optimisations in Machine Type Communications for Sensor Data Networking”. In: *IET Wireless Sensor Systems Special Issue: Use of Cellular Technologies in Sensor Networking* 6.4 (2016), pp. 102–108.

[103] CTE Solutions Inc. *Business and ITSM on the Same Page at Last! ITIL, TOGAF and COBIT Working Together.* 2013. URL: `https://www.slideshare.net/CTESolutions/business-and-itsm-on-the-same-page-at-last-itil-togaf-and-cobit-working-together` (visited on 02/15/2017).

[104] CMMI Institute. *Building Organizational Capability.* 2017 . URL: `http://cmmiinstitute.com/build-organizational-capability` (visited on 02/20/2017).

[105] FAIR Institute. *FAIR.* 2017. URL: `http://www.fairinstitute.org/` (visited on 05/09/2017).

[106] *Internet of Things: A Framework for the Next Administration.* Tech. rep. November. 2016, pp. 49–60.

[107] iotlist. *Discover the Internet of Things.* 2017. URL: `http://iotlist.co/` (visited on 02/24/2017).

[108] ISACA. *COBIT 5 for Information Security.* URL: `http://www.isaca.org/cobit/pages/info-sec.aspx` (visited on 02/20/2017).

[109] ISACA. *COBIT 5 for Risk.* URL: `http://www.isaca.org/cobit/pages/risk-product-page.aspx` (visited on 02/20/2017).

[110] ISACA. *Cybersecurity: Based on the NIST Cybersecurity Framework.* 2017.

[111] ISO. *The ISO Survey of Management System Standard Certifications.* Tech. rep. ISO/IEC, 2015.

[112] *ISO Survey 2015.* `http://www.iso.org/iso/iso_27001_iso_survey2015.xls`. Accessed: 2017-02-15.

[113] ISO/IEC. *Study Report on IoT Reference Architectures / Frameworks.* Tech. rep. 2014.

[114] ISO/IEC. *Annexes to the Internet of Things Preliminary Report*. Tech. rep. 2015. URL: https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-annexes.zip.

[115] ISO/IEC. *Internet of Things (IoT) Preliminary Report*. Tech. rep. 2015. URL: https://www.iso.org/isoiec-jtc-1.html.

[116] ISO/IEC. *ISO/IEC JTC 1: Information Technology*. 2017. URL: http://www.iso.org/iso/jtc1_home.html (visited on 02/20/2017).

[117] ITU. *The Internet of Things*. Tech. rep. 2005.

[118] ITU. *Overview*. 2017. URL: http://www.itu.int/en/about/Pages/overview.aspx (visited on 02/24/2017).

[119] ITU-T. *Y.2060 Overview of the Internet of Things*. 2012.

[120] ITU-T. *Y.2066 Common Requirements of the Internet of Things*. 2014.

[121] Ieuan Jolly. *Data protection in the United States: overview*. 2016. URL: http://us.practicallaw.com/6-502-0467#a747828 (visited on 02/15/2017).

[122] HIPAA Journal. *FDA Confirms Muddy Waters' Claims that St. Jude Medical Devices Can be Hacked*. 2017. URL: http://www.hipaajournal.com/fda-confirms-muddy-waters-claims-st-jude-medical-devices-can-hacked-8642/ (visited on 03/20/2017).

[123] Ved P. Kafle, Yusuke Fukushima, and Hiroaki Harai. "Internet of Things Standardization in ITU and Prospective Technologies". In: *IEEE Communications Magazine* 54.7 (2016), pp. 40–47.

[124] Patrick Gage Kelley et al. "Standardizing Privacy Notices: An Outline Study of the Nutritional Label Approach". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010).

[125] John B. Kennedy. "When Woman is Boss – An Interview with Nikola Tesla". In: *Collier's Magazine* (1926). URL: http://www.tfcbooks.com/tesla/1926-01-30.htm.

[126] Robin Kester. "Demystifying the Internet of Things: Industry Impact, Standardization Problems, and Legal Considerations". In: *Elon Law Review* 1 (2014).

[127] Brian Krebs. *KrebsOnSecurity Hit With Record DDoS*. 2016. URL: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (visited on 12/17/2016).

[128] Haryo Laksono and Yose Supriyadi. "Design and Implementation Information Security Governance Using Analytic Network Process and COBIT 5 For Information Security A Case Study of Unit XYZ". In: *2015 International Conference on Information Technology Systems and Innovation* 1 (2015), pp. 16–19.

[129] Nile Lars. *Connected Medical Devices, Apps: Are They Leading the IoT Revolution - or Vice Versa?* 2014. URL: https://www.wired.com/insights/2014/06/connected-medical-devices-apps-leading-iot-revolution-vice-versa/ (visited on 02/15/2017).

[130] Pedro Giovanni Leon et al. "Token Attempt: The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens". In: *ACM Workshop on Privacy in the Electronic Society (WPES 2010)* (2010), pp. 93–104.

[131] Pedro Giovanni Leon et al. "What matters to users?: factors that affect users' willingness to share information with online advertisers". In: *Proceedings of the Ninth Symposium on Usable Privacy and Security* (2013).

[132] Pedro G. Leon et al. "Why people are (Un)willing to Share Information with Online Advertisers". In: *Technical Report CMU-ISR-15-106, Carnegie Mellon University* (2015).

[133] Ilaria Liccardi, Alfie Abdul-Rahman, and Min Chen. "I Know Where You Live: Inferring Details of People's Lives by Visualizing Publicly Shared Location Data". In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 2016, pp. 1–12.

[134] Huichen Lin and Neil Bergmann. "IoT Privacy and Security Challenges for Smart Home Environments". In: *MDPI Information* 44.7 (2016).

[135] Fei Liu et al. "A Step Towards Usable Privacy Policy: Unsupervised Alignment of Privacy Statements". In: *Proceedings of The 25th International Conference on Computational Linguistics (COLING 2014)* (2014), pp. 884–894.

[136] Carl D. Livitt. *Preliminary Expert Report of Carl D. Livitt, October 23, 2016*. 2016. URL: https://medsec.com/stj_expert_witness_report.pdf (visited on 03/20/2017).

[137] Martin G. Löhe and Knut Blind. "Regulation and Standardization of Data Protection in Cloud Computing". In: *ITU Kaleidoscope: Trust in the Information Society*. Vol. 3. 2016.

[138] Natasha Lomas. *Cue Is A Connected Lab-In-A-Box For On-Demand Health Testing At Home*. 2014. URL: https://techcrunch.com/2014/05/17/cue/ (visited on 02/15/2017).

[139] Ignac Lovrek, Antun Caric, and Drazen Lucic. "Future Network and Future Internet: A Survey of Regulatory Perspective". In: *2014 22nd International Conference on Software, Telecommunications and Computer Networks* (2014), pp. 186–191.

[140] Lorrie Luellig and Jake Frazier. *A COBIT Approach to Regulatory Compliance and Defensible Disposal.* 2013. URL: `http://www.isaca.org/Journal/archives/2013/Volume-5/Pages/A-COBIT-Approach-to-Regulatory-Compliance-and-Defensible-Disposal.aspx` (visited on 02/15/2017).

[141] James Macaulay, Lauren Buckalew, and Gina Chung. "Internet of Things in Logistics". In: *DHL Trend Research* 1.1 (2015).

[142] Mauricio Marrone et al. "IT Service Management: A Cross-national Study of ITIL Adoption". In: *Communications of the Association for Information Systems* 34.49 (2014).

[143] Aleecia M McDonald and Lorrie F. Cranor. "The Cost of Reading Privacy Policies". In: *ISJLP* 4 (2008), p. 540.

[144] Aleecia M. Mcdonald et al. "A Comparative Study of Online Privacy Policies and Formats". In: *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies* (2009), pp. 37–55.

[145] Margaret Harding McGill. *AT&T Exec Says Internet Of Things Needs Light Regulation.* 2015. URL: `https://www.law360.com/articles/716922/at-t-exec-says-internet-of-things-needs-light-regulation` (visited on 02/24/2017).

[146] Aref Meddeb. "Internet of Things Standards: Who Stands Out from the Crowd?" In: *IEEE Communications Magazine* July (2016), pp. 40–47.

[147] Medtronic. *Notice of Privacy Practices.* 2016. URL: `https://www.medtronicdiabetes.com/notices` (visited on 03/16/2017).

[148] Florian Michahelles and Stephan Karpischek. "What Can the Internet of Things Do for the Citizen (CIoT)?" In: *Pervasive Computing* (2010), pp. 102–104.

[149] Simon Mingay and Steve Bittinger. *Combine CobiT and ITIL for Powerful IT Governance.* 2002. URL: `https://www.gartner.com/doc/359806/combine-cobit-itil-powerful-it` (visited on 02/15/2017).

[150] Kathryn C Montgomery, Jeff Chester, and Katharina Kopp. *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection.* Tech. rep. Center for Digital Democracy, 2016.

[151] Andrew P. Moore et al. “The Economics of Information Security”. In: *Science* (2006), pp. 610–613.

[152] Madison Moore. *Senator asks FTC to look into IoT toy privacy concerns*. 2017. URL: https://iapp.org/news/a/senator-asks-ftc-to-look-into-iot-toy-privacy-concerns/ (visited on 05/10/2017).

[153] Katsuhiro Naito. “A Survey on the Internet-of-Things: Standards, Challenges and Future Prospects”. In: *Journal of Information Processing* 25 (2017), pp. 23–31.

[154] Arvind Narayanan and Vitaly Shmatikov. “Myths and Fallacies of “Personally Identifiable Information””. In: *Communications of the ACM* 53.6 (2010), p. 24.

[155] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books. Stanford University Press, 2009.

[156] NIST. “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems”. In: (2016).

[157] NSTC. *National Privacy Research Strategy*. Tech. rep. National Science and Technology Council, 2016.

[158] OECD. *The OECD Privacy Framework*. Tech. rep. OECD, 2013.

[159] Office of Senator Ed Markey. *Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & “Cyber Dashboard” Rating System*. 2015. URL: https://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system (visited on 05/10/2017).

[160] Great Britain Home Office and K. Younger. *Report of the Committee on Privacy: Chairman Kenneth Younger. Presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by Command of Her Majesty, July 1972*. H.M. Stationery Office, 1972.

[161] Maureen K. Ohlhausen. *Reactions to the FCC’s Proposed Privacy Regulations*. Tech. rep. Federal Trade Commission, 2016.

[162] Paul Ohm. “Branding Privacy”. In: *Minnesota Law Review* 97 (2012), pp. 907–989.

[163] Marwan Omar, Derek Mohammed, and Van Nguyen. “Enhancing Cyber Security for Financial Industry Through Compliance and Regulatory Standards”.

In: *Security Solutions for Hyperconnectivity and the Internet of Things*. Ed. by Maurice Dawson, Mohamed Eltayeb, and Omar Marwan. June. IG Global, 2016. Chap. 5, pp. 113–129.

[164] oneM2M. *TS-0001 Functional Architecture*. Tech. rep. 2016.

[165] oneM2M. *one Certification for oneM2M Standard: Product Types*. 2017. URL: `http://www.onem2mcert.com/sub/sub02_03.php` (visited on 04/28/2017).

[166] oneM2M. *Published Specifications*. 2017. URL: `http://www.onem2m.org/technical/published-documents` (visited on 02/24/2017).

[167] Ajit Pai. *Dissenting Statement Of Commissioner Ajit Pai: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*. Tech. rep. Federal Communication Commission, 2017.

[168] Maria Rita Palattella et al. "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models". In: *IEEE Journal on Selected Areas in Communications* 34.3 (2016), pp. 510–527.

[169] Hyuncheol Park, Hoichang Kim, and Hotaek Joo. "Recent Advancements in the Internet-of-Things Related Standards: A oneM2M Perspective". In: *ICT Express* 2.3 (2016), pp. 126–129.

[170] Michael Quinn Patton. *Qualitative Evaluation and Research Methods*. SAGE Publications, Inc., 1990.

[171] Scott R. Peppet. "Regulating the Internet of Things: First Steps". In: *Texas Law Review* 93.85 (2015).

[172] Angela Guimarães Pereira and Mariachiara Tallacchini. *Governance of ICT Security: A Perspective from the JRC*. Tech. rep. EU Joint Research Centre, 2014.

[173] Rúben Pereira and Miguel Mira Da Silva. "A Maturity Model for Implementing ITIL V3 in Practice". In: *Proceedings of the IEEE International Enterprise Distributed Object Computing Workshop* (2011), pp. 259–268.

[174] N. Pidgeon, R.E. Kasperson, and P. Slovic. *The Social Amplification of Risk*. Cambridge University Press, 2003.

[175] Axelos Global Best Practice. *What is ITIL® Best Practice?* URL: `https://www.axelos.com/best-practice-solutions/itil/what-is-itil` (visited on 02/15/2017).

[176] The 3rd Generation Partnership Project. *About 3GPP*. 2017. URL: `http://www.3gpp.org/about-3gpp/about-3gpp` (visited on 02/24/2017).

[177] The 3rd Generation Partnership Project. *SA3 - Security*. 2017. URL: http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security (visited on 02/24/2017).

[178] The 3rd Generation Partnership Project. *Service and System Aspects*. 2017. URL: http://www.3gpp.org/specifications-groups/sa-plenary (visited on 02/24/2017).

[179] Lee Rainie and Maeve Duggan. *Americans' Opinions on Privacy and Information Sharing*. Tech. rep. 2016.

[180] Carlo Ratti, Yaniv J. Turgeman, and Eric Alm. *Smart toilets and sewer sensors are coming*. 2014. URL: http://www.wired.co.uk/article/yaniv-j-turgeman (visited on 02/15/2017).

[181] Joel R Reidenberg. "Disagreeable Privacy Policies: Mismatches Between Meaning and User's Understanding". In: *Erasmus* November (2005).

[182] Joel R Reidenberg et al. "Privacy Harms and the Effectiveness of the Notice and Choice Framework". In: *Journal of Law and Policy for the Information Society* 11.2 (2014).

[183] FTC Press Release. *FTC, NHTSA to Conduct Workshop on June 28 on Privacy, Security Issues Related to Connected, Automated Vehicles*. 2017. URL: https://www.ftc.gov/news-events/press-releases/2017/03/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues (visited on 05/09/2017).

[184] FTC Press Release. *FTC Releases New Guidance For Developers of Mobile Health Apps*. 2017. URL: https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps (visited on 05/09/2017).

[185] *Report on Privacy Research within NITRD*. Tech. rep. Federal Networking, Information Technology Research, and Development Program, 2014.

[186] M. Rotenberg. *Privacy Law and Society*. American Casebook Series. West Academic, 2015.

[187] Shamsul Sahibudin, Mohammad Sharifi, and Masarat Ayat. "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations". In: *Proceedings - 2nd Asia International Conference on Modelling and Simulation* (2008), pp. 749–753.

[188] Mathias Sallé. *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing*. Tech. rep. 2004.

[189] Florian Schaub et al. “A Design Space for Effective Privacy Notices”. In: *Eleventh Symposium On Usable Privacy and Security* (2015).

[190] Paul M. Schwartz. “Privacy, Ethics, and Analytics”. In: *IEEE Security and Privacy* 9.3 (May 2011), pp. 66–69.

[191] Paul M. Schwartz and Daniel J Solove. “The PII Problem: Privacy and a New Concept of Personally Identifiable Information”. In: *NYU Law Review* 86 (2011), p. 1814.

[192] Securview. *Vulnerability Assessment.* 2017. URL: `http://www.securview.com/services/advisory/vulnerability-assessment/` (visited on 05/08/2017).

[193] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. “Privacy Tipping Points in Smartphones Privacy Preferences”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2015, pp. 807–816.

[194] Irina Shklovski et al. “Leakiness and Creepiness in App Space : Perceptions of Privacy and Mobile App Use”. In: *Proceedings of the 32nd ACM Conference on Human Factors in Computing Systems* (2014).

[195] Bahareh Shojaie, Hannes Federrath, and Iman Saberi. “Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A”. In: *Proceedings of the 9th International Conference on Availability, Reliability and Security*. 2014, pp. 259–264.

[196] S. Sicari et al. “Security, Privacy and Trust in Internet of Things: The Road Ahead”. In: *Computer Networks* 76 (2015), pp. 146–164.

[197] The IT Skeptic. *The Real Cost of ITIL V3 Expert Certification.* 2009. URL: `http://www.itskeptic.org/real-cost-itil-v3-expert-certification` (visited on 02/15/2017).

[198] Daniel J Solove. “Privacy Self-Management and the Consent Dilemma”. In: *Harvard Law Review* 126 (2013), p. 1880.

[199] Daniel J Solove and Woodrow Hartzog. “The FTC and the New Common Law of Privacy”. In: *Columbia Law Review* 114 (2014), p. 583.

[200] Sarah Spiekermann and Lorrie F. Cranor. “Engineering Privacy”. In: *IEEE Transactions on Software Engineering* 35.1 (2009), pp. 67–82.

[201] William Stallings. “The Internet of Things: Network and Security Architecture”. In: *The Internet Protocol Journal* (2015).

[202] National Institute of Standards and Technology. *Internal Report 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems.* Tech. rep. 2017. (Visited on 05/09/2017).

[203] National Institute of Standards and Technology. *Risk Management Framework.* 2017. URL: `http://csrc.nist.gov/groups/SMA/fisma/framework.html` (visited on 05/09/2017).

[204] Myles Suer and Les McMonagle. *Extending COBIT 5 Data Security and Governance Guidance.* 2017. URL: `http://www.isaca.org/COBIT/focus/Pages/extending-cobit-5-data-security-and-governance-guidance.aspx` (visited on 02/20/2017).

[205] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. "Information Security Management System Standards: A Comparative Study of the Big Five". In: *International Journal of Electrical & Computer Sciences* 11.5 (2011).

[206] Shaun Sutner. *Wellness Wearables on Display at Connected Health Symposium.* 2014. URL: `http://searchhealthit.techtarget.com/feature/Wellness-wearables-on-display-at-Connected-Health-Symposium` (visited on 02/25/2017).

[207] Symantec. *An Internet of Things Reference Architecture for IoT Security.* Tech. rep. 2015.

[208] Intel Information Technology. *Prioritizing Information Security Risks with Threat Agent Risk Assessment.* Tech. rep. 2009. URL: `http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf` (visited on 05/09/2017).

[209] Janice Y. Tsai. "The Impact of Salient Privacy Information on Decision-Making". PhD Dissertation. Carnegie Mellon University, 2009.

[210] Jy Tsai et al. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study". In: *Information Systems Research* 22.2 (2011), pp. 254–268.

[211] Zsuzsa Varvasovszky and Ruairí Brugha. "How to do (or not to do)... A Stakeholder Analysis". In: *Health Policy and Planning* 15.3 (2000), pp. 338–345.

[212] Zsuzsa Varvasovszky and Ruairí Brugha. "Review Article Stakeholder Analysis: A Review". In: *Health Policy and Planning* 15.3 (2000), pp. 239–246.

[213] Samuel D. Warren and Louis D. Brandeis. "The Right to Privacy". In: *Harvard Law Review* IV.5 (1890).

[214] Rick Wash. "Folk Models of Home Computer Security". In: *Proceedings of the 6th Symposium on Usable Privacy and Security*. Redmond, Washington, USA, 2010.

[215] Shaun Waterman. "FCC abandons plans for rules on IoT cybersecurity". In: *CyberScoop* (2016).

[216] Shaun Waterman. "FCC looks to tackle IoT cybersecurity through 5G regulation". In: *CyberScoop* (2017), pp. 2–5.

[217] Rolf H. Weber. "Internet of things: Privacy Issues Revisited". In: *Computer Law and Security Review* 31.5 (2015), pp. 618–627.

[218] Bruce D. Weinberg et al. "Internet of Things: Convenience vs. Privacy and Secrecy". In: *Business Horizons* 58.6 (2015), pp. 615–624.

[219] Alan F. Westin. *Privacy and Freedom*. Atheneum, 1967.

[220] Shomir Wilson et al. "Crowdsourcing Annotations of Websites' Privacy Policies: Can It Really Work?" In: *In Proceedings of the World Wide Web Conferernce* (2016), pp. 133–143.

[221] Maryanne Winniford, Sue Conger, and Lisa Erickson-harris. "Confusion in the Ranks: IT Service Management Practice and Terminology". In: *Information Systems Management* April (2009).

[222] Li Da Xu et al. "Internet of Things in Industries: A Survey". In: *IEEE Transactions on Industrial Informatics* 10.4 (2014), pp. 2233–2243.

[223] Danny Yadron. *America's Top Privacy Regulator Refuses to Wear a Fitbit*. 2016. URL: `https://www.theguardian.com/technology/2016/jan/06/fitbit-ces-privacy-concerns-health-step-counter-technology` (visited on 03/09/2017).

[224] Agnieszka Zajac and Piotr Soja. "ITSM Adoption in European SMEs: Transition versus Developed Economies". In: *Proceedings of the 18th Americas Conference on Information Systems*. 2012.