https://doi.org/10.48009/3_iis_2020_142-152
Issues in Information Systems
Volume 21, Issue 3, pp. 142-152, 2020

EMERGING CHALLENGES WITH INTERNET OF THINGS

Trisha Bartlett, Robert Morris University, tkbst210@mail.rmu.edu*

ABSTRACT

The purpose of this study is to examine the current IoT users' privacy concerns and to highlight the emerging challenges of several IoT users' privacy and security practices. This paper discusses the emerging challenges of several IoT users' privacy and security practices and surface several IoT challenges that are expected to emerge as the digital world expands. The study utilized a qualitative approach to explore factors related to users' perceptions and social perspectives as defined and measured by the Protection Motivation Theory (PMT) and the Diffusion of Innovation (DOI) models. The study used a total of 17 participants with varying levels of education and years of professional experience ranging from 2 to over 30 years in different industries. The data revealed four recurring themes: (1) Security Concerns, (2) Consumer Awareness, (3) Privacy Concerns, (4) Data Ownership, (5) Policy and Laws, and (6) Financial Benefits.

Keywords: Diffusion of Innovation, Internet of Things, Protection Motivation Theory, Privacy, and Security

INTRODUCTION

It is widely observed that our society has become consumed with the emerging trend of new connected devices known as IoT. As a result, there has been a shift in product, technological, and environmental innovations. However, new trends also raise privacy and security concerns. In 2016, the Mirai botnet attacks sparked a rapid growth of IoT attacks in which devices are exploited maliciously by malware, ransomware, or distributed denial of service (DDoS) (Kolias et al., 2017). Consequently, in 2020 the dangers are unquestionably increasing for observation, information exfiltration, and direct control of consumer devices, while at the same automated home products are becoming inexpensive for consumers to purchased and set-up. Consumers may see IoT as harmless, but there are outstanding security issues to be researched and evaluated as the market expands into home thermostats, controlled door locks from smartphones and smart appliances, or other home automation products.
As the IoT ecosystem expands, the interest and research in this topic continue to increase. For example, Schurgot, Shinberg, & Greenwald (2015) explored IoT networks; specifically, "the risks to security and privacy of IoT networks, focusing first on home automation networks" (p.1). The authors' emphasis is on privacy preservation in home automation networks; on the other hand, their concepts can extend to other IoT devices.

This research reexamines privacy practices, explores concerns about the potential data collection and sharing by unsecured devices, and aims to foster new solutions to IoT security challenges on this complex issue. The goal of this study is to analyze current users' IoT technologies' privacy and security practices.

In addition to emphasizing the importance of information security to address privacy issues, which is the primary purview of this research, it is also essential to understand the privacy and security controls of IoT devices. Privacy is an important topic when referring to IoT devices, how data is collected, protected, and used are the foremost IoT user's privacy concerns. Whereas, security controls present new and unique challenges for IoT users. The number of those interconnected devices continues to grow daily, and the number of security threats and vulnerabilities grows with them. Security is one of the principles overriding technological research issues that currently exist for IoT (Jindal, Jamar, & Churi, 2018).

*The author's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

Security has several facets: security designed among the device, security of information transmission, and information storage among the systems and its applications. There is an extensive body of literature focused on this topic with innumerable issues along with proposed solutions. Also, this qualitative study will explore factors related to users' perceptions and social perspectives as defined and measured by the Protection Motivation Theory (PMT) and the Diffusion of Innovation (DOI) model, which provides the theoretical and conceptual framework listed. Most importantly, this study will also contribute to the existing body of knowledge in the information security and privacy rights sectors. Information systems engineers and scholars, among others, can benefit from this study that will be supported by a strong theoretical base and address prevalent IoT challenges.

LITERATURE REVIEW

Theory of Privacy

The literature review revealed that the fast growth of the internet and emerging technologies over the past decade had raised the problems of privacy and security of mobile device users' data. Posadas (2017) suggests Internet users are forced on influences associated with the protection of their personal data once discharged in online repositories. Privacy problems are explored and represented in various publications to shield and regulate the capturing, storing, and, therefore, the unauthorized accessing and dissemination of Internet users' personal data. According to Spinello (2014), "theories of privacy often confuse the *concept* of privacy with the normative justification for a *right* to privacy" (p. 154). The concept of privacy is vague and inaccurate, where the definition of privacy implies that the right to privacy is different from the moral perspective of non-intrusion of privacy.

Singh, Millard, Reed, Cobbe, and Crowcroft (2018) found that over 120 countries have data protection laws with wide-ranging "applications to businesses (the U.S. patchwork of privacy laws makes it a notable outlier)" (p. 59). Applying privacy data-protection laws or rules to IoT devices is necessarily a challenge. Partly, almost any type of data is considered personal data, and using stringent governing standards will be astonishingly broad. Undeniably, many privacy and security challenges exist and must be taken care of before the reality of securing the emerging IoT evolution. The critical explorations regarding IoT require privacy security and trust (Sfar, Natalizio, Challal, & Chtourou, 2018).

IoT Privacy and Security Challenges

The growth of the IoT domain ultimately constrains privacy and security challenges with IoT devices. Hogewoning (2018) found that IoT network ecosystems are facing a challenging situation due to widely deployed devices. Security risks are compounded across hundreds or thousands of devices such as those that created distributed Mirai botnet attacks in October 2016. It is unrealistic to expect IoT manufacturers to develop bug-free devices. "Because of the vulnerabilities that continue to plague devices within the IoT space, the prospect of zombie connected devices quietly wreaking havoc upon the Internet remains a real threat…" (Hogewoning, 2018, p. 2). All software has bugs and producing flaw-free software remains a challenge—as some IoT devices are shipped directly from the factory with pre-installed software that is either outdated or becomes outdated over time. Hogewoning states that as a best practice, device users or owners of IoT devices must make sure to update these devices before becoming exploitable when the device is connected to the internet.

From a regulatory standpoint, Edward Snowden, a whistleblower of the United States (U.S.) National Security Agency (NSA), spoke out on these longstanding security concerns. This revelation demonstrated that the U.S. government has been collecting and mining online data for years, not just for business purposes (Clement & Obar, 2016). In their study, Clement and Obar evaluate the importance of data privacy transparency. The authors "define data privacy transparency as the act of being open about commitments to data privacy protections, as well as publicly forthcoming about data collection, management, storage, retention, disclosure, and routing practices" (pp. 295-296). Data privacy transparency allows for stronger accountability and secure data access for how the data is collected.

Similarly, the U.S. Department of Homeland Security (2016) released a set of Strategic Principles for Securing the Internet of Things to help guide consumers and companies in their decision-making process regarding connected devices. This guideline sets forth suggested principles to be considered in developing and manufacturing IoT devices

for consumers, companies, service providers, and other stakeholders. IoT can increase productivity, ease of use, and integrated features that make the IoT application vulnerable to unauthorized users to have physical access to device users (Henze et al., 2016). IoT resources for managing privacy and security features of the devices for commercial connections do not always provide full access to and from the internet. Nevertheless, building on the recognized privacy and security practices, Voas (2016) proposed Network of 'Things' (NoT) in a distributed structure for including IoT technologies, a foundational concept on data and security concerns in the operations and lifecycle of IoT.

IoT applications represent emerging technologies in several interdisciplinary domains. Triantafyllou, Sarigiannidis, and Lagkas, (2018) focus on the essential domain areas and related applications from the smart grid, smart living, smart mobility, and smart tourism, to healthcare, logistics, agriculture, and industrial IoT technologies, to name a few, for real-time monitoring. Table 1 provides an adapted version of IoT application domains to represent the areas where businesses, services, and systems enable seamless connections among consumers, environmental functions, and networks.

Table 1. IoT Applications Domains. Adapted from Triantafyllou, Sarigiannidis, and Lagkas, (2018)

APPLICATION DOMAIN	APPLICATION
Agriculture	Animal tracking, certification, and trade control Irrigation, monitoring agricultural production and feed Farm registration management
Healthcare	Remote monitoring medical parameters, diagnostics Medical equipment tracking, secure indoor environment management Smart hospital services, entertainment services
Independent living	Elderly assistance, disabled assistance Personal home/mobile assistance, social inclusion Individual well-being, personal behavior impact on society
Industrial processing	Real-time vehicle diagnostic, assistance driving Monitoring industrial plants Luggage management, boarding operation, mobile tickets
Logistics	Identification of materials/product deterioration Waterhouse management, retail, inventory Shopping operation, fast payment
Public safety and environmental monitoring	Environmental and territorial monitoring Video/radar/satellite surveillance Emergency site/ personal rescue tracking, emergency plan
Smart Grid	Load management, storage service, entertainment services Sustainable mobility, booking charging slot Power generation/distribution/storage, energy management

Table 1. IoT Applications Domains. Adapted from Triantafyllou, Sarigiannidis, and Lagkas, (2018)

APPLICATION DOMAIN	APPLICATION
Smart Home	Plant maintenance, energy management Video surveillance, access management, children protection Entertainment, comfortable living
Smart Mobility	Traffic management, multi-modal transport Road condition monitoring, parking system, waste collection Payment systems, tour guide services

Miorandi, Sicari, De Pellegrini, and Chlamtac (2012) propose that IoT is a significant emerging technology trend and define IoT expansion in three areas: to identify the capacity of smart things to (1) be recognizable "anything identifies itself," (2) to convey "anything communicates" and (3) to connect "anything interacts"– either among themselves, systems of interconnected items, or with end-clients or different elements in the system (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012, p. 1498).

Theoretical Frameworks

The researcher also used seminal works found within the literature to identify additional materials for an in-depth analysis, which involves locating scholarly resources using the names of authors or references listed under publications relevant to specific topic information. Also, this chapter includes theoretical views associated with information security. In order to close the knowledge gap in the literature, this research focuses on the literature review to explore user practices to address privacy and security concerns, and it uses the Protection Motivation Theory (PMT) as the conceptual framework to explore how IoT users enable the adoption of IoT devices. PMT theory is often used as the theoretical basis for the study of personal protective behaviors. It was first proposed by Rogers (1975), who reasoned that an individual facing a security threat would undergo a threat appraisal process and a coping appraisal process for self-protection. PMT addresses "three crucial components of a fear appeal occurrence; and (c) the efficacy of a protective response" (Maddux & Rogers, 1983, p. 470). The theory also consists of five core variables, namely perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response costs. In Rogers' revised study, he advanced the idea that an individual's intention of performing communication behaviors would be determined by his or her appraisal of perceived severity and vulnerability, and his or her evaluation of the efficacy of coping with the threat of certain Internet behaviors. Therefore, the PMT is a social cognitive model that prioritizes relevant perceptions to predict the outcome of certain Internet behaviors.

A study by Verkijika (2018) looked at smartphone behaviors of users in South Africa. In this study, the author describes PMT as grounded in how individuals address and build choices in times of harmful or disagreeable events in life. Notably, PMT is one of the leading theoretical models used by researchers for understanding information security behaviors (Verkijika, 2018). Previous studies have examined the antecedent variables of using PMT and emphasize the perceived values of user behaviors toward the user's privacy and security protection. Several authors propose a detailed framework that is focused on the characteristics of the IoT to examine traditional and new PMT factors to predict users' behaviors (Hanus & Wu, 2016; Tsai et al., 2016; Verkijika, 2018). Hanus and Wu (2016) applied PMT to understanding the impact of information security on user computer awareness. Moreover, PMT proposes the protective behavior that is inspired by coping, and the threat will transpire, and other studies imply privacy risks negatively across different intentions associated with PMT (Verkijika, 2018).

This study also explores the concepts of analysis on mobile devices and privacy precautions that have formed beyond PMT research. "There is ongoing research on Internet security that integrates PMT variables to examine users' psychological responses to security-related events. The variables PMT measures include factors such as users' previous knowledge of online safety hazards and their understanding of online protections (Tsai et al., 2016). Furthermore, Hanus and Wu (2016) found that computer safety protection motivations on the part of users are a crucial

factor in security behaviors. This study utilizes the PMT framework and adds to the knowledge of IoT device users' practices on security awareness. As a result, this exploratory study adopts the tenets of PMT to explain how individuals develop protection motivation and shared cultural practices that factor into individual experiences

In addition to PMT, diffusion of Innovation (DOI) theory has been used to guide the data collection and analysis process. According to Rogers (1976), there are five steps for the adoption of innovations explicitly, knowledge, persuasion, decision, implementation, and confirmation. Based on these five steps, innovation adoption can be defined as: "the process through which an individual or other decision-making association passes from first knowledge of innovation to forming an attitude towards innovation, to a decision to adopt or reject, to implementation of the new idea and confirmation of this decision" (p. 11). The DOI theory is valuable to extract the advancement of technology adoption within the IoT field. For instance, previous research has discovered that IoT acceptance at the application stage and technology adoption is occurring at the level of social influence instead that of individual user level (Walldén & Mäkinen, 2014).

De Cremer, Nguyen, and Simkin (2017) note that "capturing and analyzing the data that come from the sensors at the endpoints of the connected objects, the IoT's value lies in its ability to track, measure and create 'smart' devices that bring considerable benefits to individuals, businesses, and society" (p. 145). The issue of information tracking increases concerns in the data collection process, and the potential lies more productively with enhanced effectiveness, targeting, and financial advantage for the IoT businesses. In another study, Miorandi, Sicari, De Pellegrini, and Chlamtac (2012) present "a survey of technologies, applications and research challenges for Internet-of-Things" (p. 1497). The authors introduce research challenges within the IoT technologies landscape. For example, the underlying computing capabilities have the potential to enable new security challenges for the development and securing and preserving privacy into transactional statistics, metrics and, observations of the user activities and behaviors. Based on this paradigm of IoT computing, companies can access mainstream information that gives them more know-how about customers' desires. In this sense, privacy data (approximate age, employment, weight, financial statements) are available via IoT devices, along with wearable exercising gadgets (Fitness trackers, smartphone apps, and so on) (De Cremer, Nguyen, & Simkin, 2017). Going forward, IoT manufacturers will need to give significantly more consideration to privacy and security issues.

Gilchrist (2017) discusses the importance of security risks in personal wearables, the data being collected in the cloud, and how manufacturers of these devices offer both private and public modes that consumers should be concerned about unlawful processing of their personal data. IoT structures can be used to preserve statistics of customers' spending and can even disclose via smart devices what consumers' likes and dislikes are. Nevertheless, Gilchrist (2017) states that consumers need to be more concerned about reading terms and conditions (TOC) and privacy policies even though the manufacturers claim that data collected will be anonymized, "regardless of the moral or ethical questions the consumer should be aware that their privacy might well be compromised when they are wearing an IoT wearable device" (p. 80). Since data security is a significant concern, securing personal data that these devices collect is essential, and these concerns may extend beyond the type of data that customers feel comfortable with sharing. On the other hand, Sombir and Solanki (2018) discuss the emerging security aspects of IoT and the technology innovation through various security parameters in which the IoT network system acts as a vulnerable component. Despite the reality of the many IoT device types, inherent limitations of IoT security flaws that have been identified are privacy and security, which are shown jointly as a single concept.

RESEARCH METHODOLOGY

As IoT innovation is advancing, the extent of privacy and security vulnerabilities is emerging as an essential factor in creating an Internet of trusted data that provides safe and secure access for everyone. IoT devices have present privacy and security challenges. Currently, the majority of published IoT literature on this topic of emerging technologies does not focus on the connection between privacy and data security from IoT user's perspectives. While attempting to understand IoT users' privacy and security concerns, a qualitative approach was decided to be the best option. This qualitative study using semi-structured interviews is used to collect data from approximately 17 IoT users to gather

their perceptions regarding the issues of privacy and security of IoT devices. Also, this still allowed the researcher to ask follow-up questions and asked for clarification on some responses.
The study provides a deeper understanding of privacy concerns that potentially are impacting users' IoT security practices and contributes to the existing body of knowledge in the information security and privacy rights sectors. Information systems engineers and scholars, among others, can benefit from this study that is supported by several theories and addresses IoT challenges that are prevalent.

The sample population for this research study consisted of IoT participants who work in various companies in the U.S. Before the interview began, the researcher asked a limited number of demographic questions to further clarify the specific aspects of the participants. These questions included what type of IoT device the participant owned, job title, educational background, and years of professional experience (see Appendix A). Table 2 illustrates the demographic information provided by each participant. Out of the 30 potential participants contacted, 17 individuals were successfully selected and interviewed (face-to-face and Skype) who met the screening criteria of owning an IoT device.

The distribution of the research population was 65% males and 35% females with varying levels of education and years of professional experience ranging from 2 to over 30 years in different industries (see Table 2). The professional affiliations of the research participants were: Action Officer, Computer Science Intern, Contracting Analysis Lead, Cyber Security Architect, Director of Data Science, Economics Analyst, Information Security Engineer, Information Technology Analyst, Principal Information Systems Engineer, Principal Software Engineer, Program Analyst, Quantitative Analyst, Senior Risk Manager, Senior Systems Engineer, Workforce Management Analyst.

Table 2. Participant Demographics

Participant ID	**Gender**	**Educational Background**	**Years of Experience**
1	Male	Graduate	30
2	Female	Graduate	8
3	Male	Graduate	6
4	Male	Graduate	7
5	Male	Graduate	23
6	Female	Graduate	21
7	Female	Graduate	31
8	Female	Graduate	12
9	Male	Undergraduate	20
10	Female	Graduate	8
11	Male	Graduate	5
12	Female	Graduate	27
13	Male	Graduate	30
14	Male	Some College	17
15	Male	Graduate	30
16	Male	Some College	2
17	Male	Undergraduate	16

Findings

The findings revealed several recurring themes: *Security Concerns, Consumer Awareness, Privacy Concerns, Data Ownership, Policy and Laws,* and *Financial Benefits.*

Theme One: Security Concerns
The first significant IoT security implication exists within data collection, analysis, and storage. Users have difficulty controlling their private information because IoT communications, data collection, and storage can activate automatically and, by default, unbeknownst to the user.

Theme Two: Consumer Awareness
Even though this relates to the extent to which users made their information disclosure dependent on its subjective sensitivity or the perceived identity of the data recipient, the user is unaware of the collection of the data, the data collection is pervasive, and the purpose of that collection is unclear.

Theme Three: Privacy Concerns
The privacy implication thus arises with the collection, analysis, and storage of private user data and the creation of profiles with private user data. Privacy management and questionable assumptions are directly affected and violated by *privacy concerns*.

Theme Four: Data Ownership
The role of the user in helping to secure their IoT components, e.g., changing default manufacturer passwords. Achieving secure compose-ability of individually secure devices and components. *Data Ownership* (accounting for interoperability, regulatory compliance, and governance) has, as of now, many risks unmistakably connected with IoT. The basic principles underpinning data protection related to data access and confidentiality.

Theme Five: Policy and Laws
While the results suggest that *Policy and Laws* could be effective means to enforce IoT privacy and security, it also shows that regulation and rules could serve to compel policymakers and manufacturers to follow strong security practices. The basic principles underpinning data protection laws (fairness, storage limitations, and individual rights to data access) might encourage regulators to promote privacy-aware IoT devices.

Theme Six: Financial Benefits
There is a general agreement from research participants that *Financial Benefits* IoT users accept constant tracking, monitoring, and profiling because they are persuaded that the benefits outweigh the cost of the IoT device.

Some research participants honed in on the importance of compliance with laws and government regulations. Whereas seven research participants expressed concern that network access and hacking made their personal data less secure, and that data collection poses more risks than benefits. They believe it is not possible to go through daily life without being tracked or their personal data being compromised.

The overarching themes help to understand IoT user's privacy and security concerns with the potential vulnerabilities of IoT devices. Constructs relevant to how individuals are motivated to react in a protective way towards a perceived potential vulnerability of IoT devices from PMT were considered. The four key elements: "threat appraisal," followed by "coping appraisal," which comprises "response efficacy" – the belief that specific processes will mitigate the threat - and "self-efficacy," an individual's idea of their ability to implement the required actions to mitigate the threat (Maddux & Rogers, 1983). Adopting privacy and security measures for IoT devices is not as common as ensuring privacy preferences matched with that of IoT device default settings. In some cases, research participants acknowledged the privacy and security issues did not balance with the benefits provided by these devices. For example, if the device requires personal data from the user for a feature to function, then the user would provide that data to leverage the benefit despite the potential consequence of doing so.

DISCUSSION

This research study explored the central question: How do IoT users view and manage the privacy and security of their IoT devices? This research study focused on the concerns and views IoT users share on their knowledge and experiences on IoT privacy and security practices that influence the adoption of innovation as espoused by Rogers (2003). DOI theory is a relative advantage, compatibility, complexity, observability, and trialability that are supplementary factors of security, standards, and laws and policy. However, a few factors have the potential to prevent IoT users from adopting privacy behavior during the use of their devices. These factors drive IoT user

behaviors in the context of understanding and reducing IoT vulnerabilities based on the theory of reasoned action within PMT. Three of the constructs of PMT are self-efficacy, response efficacy, and response cost, which assist in explaining consumer privacy behavior during the purchase decision process (Tsai et al., 2016). The emerging themes surfaced as participants discussed the lack of IoT privacy. Even though the IoT users assume control rights over their private information, they also want to be able to choose their device management settings according to the "how much of the disclosed information can be shared with others (permeability rules), and the level of independent judgments the owner allows the co-owner to determine third-party access (control rules)" (Petronio & Child, 2020, p. 77). Adopting privacy and security measures for IoT devices is not as common as ensuring privacy preferences matched with that of IoT device default settings. In some cases, research participants acknowledged the privacy and security issues did not balance with the benefits provided by these devices.

LIMITATIONS

This research had four limitations encountered during the study. First, the small size of the convenience sample used for this study could be a limitation of the research, as it can make it hard for the researcher to generalize the overall study's findings. Second, the limitation of this exploratory study is that the participants to be interviewed are centered in the professional systems engineering social networks, which may lead to participant bias based on their experiences in the technology industry. Third, the snowball sampling technique used to choose participants may be considered as a limitation as participants referred a colleague to participate in the study. Fourth, this study does not provide a view of cultural influences or control for volunteer bias.

CONCLUSION

As the IoT ecosystems continue to develop, accountability aspects must receive proper consideration to ensure the technologies built and deployed are acceptable, adopted, fit for purpose from a user perspective. Based on this study, IoT designs and regulations need to interact with the listed tools and resources to understand regulation in the context of privacy protection. To some extent, system designers are de-facto regulators; they exercise great power to utilize a rich set of tools and resources in carrying out their role, particularly regulatory designs. Therefore, by looking at the regulatory environment surrounding IoT designs, the results of this could help understand how to improve privacy regulations.

From a theoretical standpoint, this study supports the application of DOI theory as a multidisciplinary tool to provide several valuable insights and new information for IoT practitioners and the policymakers of IoT device products and services. Besides DOI, other theoretical frameworks, such as PMT, have been used by several researchers to understand and analyze Internet users' security behavior for a wide variety of applications and devices. Reasoning factors, such as threat appraisal and threat severity, have been studied in detail to understand its impact on perceived vulnerabilities and susceptibility to risks, as well as rewards associated with users' unsafe behaviors (Tsai et al., 2016). According to PMT, self-efficacy describes a consumer's belief in their ability to engage in specific protective behavior in response to a privacy concern while acquiring an IoT device.

When it comes to privacy and security issues concerning the IoT ecosystem that has been manufactured to date, it seems as if consumers are not overly concerned with the possibilities of security threats and vulnerabilities that come along with using these devices. There are special considerations for privacy and security. Perhaps this is because the device itself is not transparent in its use of the internet and is not accessed or used the same way most are used to access some form of networking. For example, consumers do not see a user interface for a lightbulb with embedded sensors in it. Since the industry is relatively new and ever-growing concerns about convenience and value have seemed to take priority over concerns about security or general user safety.

REFERENCES

Clement, A., & Obar, J. A. (2016). Keeping internet users in the know or in the dark. *Journal of Information Policy, 6*, 294–331. https://doi.org/10.5325/jinfopoli.6.2016.0294

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): On understanding its dark side. *Journal of Marketing Management*, *33*(1/2), 145–158.

Gilchrist, A. (2017). *IoT Security Issues* (Vol. First edition). Boston: De|G Press.

Hanus, B., & Wu, Y. "Andy." (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2–16.

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., & Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems*, *56*, 701–718.

Hogewoning, M. (2018). IoT and regulation – striking the right balance. *Network Security*, *2018*(10), 8–10. https://doi.org/10.1016/S1353-4858(18)30099-0

Jindal, F., Jamar, R., & Churi, P. (2018). Future and challenges of internet of things. *International Journal of Computer Science & Information Technology*, *10*(2), 13–25.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Privacy and Disclosure, Online and in Social Interactions*, *31*, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Posadas Jr., D. V. (2017). After the gold rush: The boom of the Internet of Things, and the busts of data-security and privacy. *Fordham Intellectual Property, Media & Entertainment Law Journal*, *28*(1), 69.

Rogers, E. M. (1976). New Product Adoption and Diffusion. *Journal of Consumer Research*, *2*(4), 290–301.

Rogers, E. M. (2003). *Diffusion of innovations*. New York: Free Press.

Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015). Experiments with security and privacy in IoT networks.

Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the internet of things. *Digital Communications and Networks*, *4*(2), 118–137. https://doi.org/10.1016/j.dcan.2017.04.003

Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the Internet of Things: Systems, law, and ways forward. *IEEE Computer, 51* (7), 54-65. https://doi.org/10.1109/MC.2018.3011052

Sombir, & Solanki, K. (2018). Literature review on security of IoT. *International Journal of Advanced Research in Computer Science*, *9*(2), 131–134.

Spinello, R. A. (2014). *Cyberethics: Morality and law in cyberspace, fifth edition*.

Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends. *Wireless Communications & Mobile Computing*, 1–24.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150.

U.S. Department of Homeland Security (DHS). (2016, November 15). Department of Homeland Security. Strategic Principles for Securing the Internet of Things (IoT). Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Voas, J. (2016, July). Networks of 'things', NIST Special Pub. 800-183, 2016. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-183

APPENDIX A: Semi-Structured IoT Privacy and Security Interview Questions

Demographics Questions:

1. Do you own any Internet of things (IoT) device(s) such as a smart personal assistants, smartwatch, smart appliance, or smart home monitoring system (i.e. ring doorbell)?
Probe: Which or what type of IoT device(s)?
2. What is your job title?
3. How do you define your career level (early, mid, or senior)?
4. How many years of experience do you have in this field?
5. Which industry do you work in? (Government, Military, Financial, Healthcare, Information Technology, or Vendor)
6. What is your highest education level?
7. Interviewee Gender:

Interview Questions:

Section 1: IoT Privacy and Security Concerns
1. What are your main privacy and security concerns with IoT devices? Please explain.
Probe: Do you have any concerns? If so, why or why not?
2. With the amount of data being collect from IoT devices, what concerns do you think consumers (users) need to be aware of regarding security and privacy issues?
Probe: Do you have experience or heard of any stories and/or experiences of privacy and security issues?
3. Describe your thoughts on apps privacy and security when connected to IoT devices?
Probe: When using your IoT devices, do you think of any potential dangers or harm?
4. What privacy, security, and reliability strategies have you used to adopt IoT devices?
5. How do you manage privacy and security settings on your IoT devices?
Probe: Do you make changes on your own, or do you seek help from others?
6. What would you like to see concerning privacy and security support in using IoT devices?
Probe: Is this an easy task, or do you need help? If so, what kind of help?

Section 2: IoT Privacy and Security Practices
1. What type of safety practices do you perform on your IoT device to protect against malicious activity?
2. What is the privacy or security default settings have you changed on your IoT device(s)?
Probe: What made you decide to or not to change your device default security or privacy settings?

Section 3: Consumer Awareness Section:
1. What are your views on the United States data ownership and privacy laws?
Probe: With this in mind, Is the data yours, and is it available to any business collecting personal data to use it?

2. In using your IoT device (s), data can be generated and used without your permission. What type of consent (i.e., direct, indirect, or partial) would you provide before the use of your data?
3. Would you prefer to own your data?

Probe: If not, why? If yes, would you support a policy or law to protect your data ownership and privacy?