12-15-2019

Cybersecurity and smart home devices: A resource governance model

Aurelia Mandani

Ronald Ramirez

CYBERSECURITY AND SMART HOME DEVICES: A RESOURCE GOVERNANCE MODEL

Aurelia Mandani[1]
Business School, University of Colorado Denver
Denver, CO, United States

Ronald Ramirez
Business School, University of Colorado Denver
Denver, CO, United States

ABSTRACT

A yet to be explored area of cybersecurity, as experienced through the security embedded within a focal firm's products, is cloud-based smart home devices being rapidly adopted in homes. Adoption of these cloud-based products is growing some 22%, indicating the potential of the home market for future revenue and profit growth (Statista 2019). With the uncovering of generous data collection functionality currently built-into these products and the seeming routineness of data breaches in general, security and data privacy of smart home devices has been identified as a critical concern of consumers (Gonzales 2019; Osborne 2019; Brandom 2019; Mangalindan 2019). As a first step in addressing this concern, we propose a theoretical model of cybersecurity in smart home devices based on a foundation of information governance and resource dependence theories. The Resource Governance Model provides a framework for smart home device firms to help ensure products incorporate their chosen cybersecurity design. Future direction for application of the Resource Governance Model is then discussed.

Keywords: Smart Home Devices; Cybersecurity; Smart Home Security; Resource Governance

[1] Aurelia Mandani. aurelia.mandani@ucdenver.edu

INTRODUCTION

The International Data Corporation (IDC) predicts spending on cybersecurity will grow from $91.4 to $120.7 billion between 2018 and 2021, highlighting the scale and diffusion of cybersecurity issues (IDC 2018). Approximately 9% of this growth is due, in part, to the $3.5 million average cost of a cyber breach (Ponemon 2017). Contributing to the challenges of cybersecurity is continued innovation in new technologies being rapidly adopted by firms and their subsequent security implications. One such technology, a service at the foundation of today's digital environment, is cloud technology.[2]

IS researchers have begun to examine adoption, risk identification, and standards associated with cloud computing (Borgman et al. 2016; Borgman et al. 2013; Morin et al. 2012; Prasad et al. 2013; Zainuddin 2012). However, the examination of governance and cloud computing remains an area of shortfall. This is especially the case with consumer-based technologies that operate on the public cloud. Major unanswered governance questions exist in the areas of 1) data-ownership*: who owns the data collected and hosted in the cloud* (the firm that developed the technology, or the consumer who purchased the technology), and 2) data-protection: *when a breach of information happens to cloud-based devices, what protections or policies help protect the data of consumers who implement these technologies?* The importance of these questions are reflected in current adoption statistics; in 2018 there were more than 45 million smart home devices, with a projected annual growth rate of 22% for the near future (Statista 2019).

[2] In a recent IDG survey, 73% of respondents indicated they had "at least one cloud application or a portion of their computing structure already in the cloud" with the remaining planning, "..to do so within the next 12 months" (IDG 2018).

Data privacy and security issues related to consumer smart devices hosted on the internet fall under the umbrella of cybersecurity. Many cybersecurity issues have arisen with smart home devices, including malware attacks on IoT devices, lack of privacy and security protections of consumer data via unsecure authentication methods, and unapproved access of surveillance of smart home data, such as audio or video recording (van Ooschot and Smith 2019; Alrawi et al. 2019; O'Connor et al. 2019; Celik et al. 2018). As these technologies continue to evolve and become more integrated within consumer's homes, there is an urgent need for understanding how product and service firms can protect and secure the information of their customers (O'Connor et al. 2019; Alrawi et al. 2019). If product firms want to take advantage of this burgeoning market, their customers must have trust in the devices they are purchasing and implementing in their homes, especially if home products have spillover effects to other company products carrying the same brand name (Simonin and Ruth 1998).

Our research project addresses this need by developing a new theory-based model of cybersecurity for smart home devices. We define smart home devices as home-based electronic devices that connect to the internet and connect to peripheral devices that utilize home assistants as a central gateway (hub) into the assistant host ecosystem. As smart home devices continue to become more widely integrated and sold to consumers, data privacy and data security have become major concerns for consumers (van Ooschot and Smith 2019; Alrawi et al. 2019; O'Connor et al. 2019). Our proposed model can serve as a tool for understanding the role of governance and resources, such as development teams and data protection policies, play in cloud cybersecurity. Future research can apply and adapt this model when researching cloud cybersecurity requirements and developing management recommendations for IoT smart home devices.

Presently, extant research on smart home devices has evaluated the vulnerabilities within these devices, and found a disconnect between security and usability of these devices; smart home devices are developed in such a way where consumers' abilities to use the product is prioritized over security (Zhou et al. 2019; Notra et al. 2014). Much of the research on vulnerabilities have pointed to issues with the security development of these devices, leaving consumer-data open for misuse (O'Connor et al. 2019; Ling et al. 2017; Ding and Hu 2018; Zeng et al. 2017). Moreover, news reports have indicated that there is a growing movement in data advocacy for consumers that use and implement these smart home devices, which opens the discussion of data governance from a consumer standpoint surrounding the question of "who owns the data, the firm that created the device or the consumer" (Gonzales 2019; Nieva and Rubin 2019). Our cybersecurity model combines the areas of information governance and resource dependence theory in the context of cloud technology. These foundations are fitting: information governance research seeks to understand how polices and internal structures within a firm govern how data is treated (Kooper et al. 2011; Tallon et al. 2013), and resource governance theory looks at understanding how organizations and the existing resources play a role in how an organization acts based on its environment (Pfeffer and Salancik 1978). Specifically, we examine the question: *how can information governance and resource dependence theory inform cybersecurity research on smart home devices?*

This article will address: 1) information governance, 2) resource dependence theory, and 3) will analyze how information governance and resource dependence theory can be combined to understand and examine smart home devices in future research.

PRIOR RESEARCH

Information Governance

Information technology (IT) governance is defined as the decision-making processes and outcomes associated with IT in a firm (Weill and Ross 2004). IT governance research has had an influential and important history within information systems, as it has helped firms and organizations address issues governance of technology hardware to recent focus on information assets (Tallon et al. 2013). As a subset of information technology governance, information governance goes beyond the technology artefact, and begins to conceptualize the processes that are involved in the information dissemination process (Kooper et al. 2011; Tallon et al. 2013; Khatri and Brown 2010; Weber et al. 2009). Moreover, as a subset of IT governance, information governance research was born out of a growing need for a scientific framework to support the security and confidentiality within the National Health Society (Donaldson and Walker 2008; Koper et al. 2011). Information governance can be described as a set of roles, processes, and standards that can be used to assist in specifying how information is handled (via archival methods), stored, analyzed, or created (Kooper et al. 2011; Tallon et al. 2013). For the purpose of this article, we will follow Kooper et al.'s (2011) definition of information governance, as:

> "[a] set of activities aimed at establishing a normative foundation to facilitate and stimulate sense making interactions."

Information governance research focused on policies of information handling has investigated the relationship of information governance and data (Tallon et al. 2013; Kooper et al. 2011). Research in this area has found that information handling is context specific, based on the type of data that is collected, and should be looked at from a risk standpoint where the firm addresses the key risks involved with the data that a firm collects (Khatri and Brown 2010). In addition to information governance and data policies, information governance and data lifecycle literature has found that it is important for firms to understand the processes of how data is

collected and the upkeep process of the data (Watson et al. 2004; Tallon et al. 2013; Khatri and Brown 2010). From a data lifecycle viewpoint, firms can utilize information governance to assist with modifying and identifying areas of growth to manage and set policies to reach necessary goals (Watson et al. 2004; Khatri and Brown 2010). Combined, these two areas of information governance can aid firms in understanding how to address governance concerns especially, when they are collecting, analyzing, and disseminating data.

Resource Dependence Theory

Resource dependence theory (RDT) has had a long history in organizational research starting with seminal a paper by Pfeffer and Salancik (1978). RDT assumes that organizations are controlled by environmental factors and argues that organizations enter into relationships to obtain resources lacking within the focal firm (Pfeffer and Salancik 1978; Ulrich and Barney 1984). Pfeffer and Salancik's (1978) initial version of RDT is similar to the resource-based view in that resources are seen as commodities, with the main differences of RDT being that key resources are a factor of the environment of the organization. Using a sociological and ecological perspective of organizations, RDT has become paramount in the field of organizational research exploring the environment's influence and impact on organizations. Three main conceptual elements include:

1. Organizational effectiveness
2. Organizational environment
3. Constraints (Pfeffer and Salancik 1978; Ulrich and Barney 1984).

Through these three concepts, Pfeffer and Salancik explore the assorted aspects of organizational culture that interplay into an organization's resource dependence. The organizational effectiveness is the notion that organizations have partnerships from social

interactions to regulate behavior of inside of an organization (Pfeffer and Salancik 1978; Tillquist et al. 2002). It is through the interactions across organizations that describe as a means of cross-organizational effectiveness, which in turn, allows for organizations to control organizational behavior (Pfeffer and Salancik 1978; Grant 1991). Thus, the effectiveness of an organization is based on the following internal and external aspects: social partnerships and behavior regulations of an organization. An organization that exhibits organizational effectiveness is one that is able to effectively organize the social aspects internally and with partner organizations. Contradictorily, Casciaro and Piskroski (2005) find that organizational effectiveness is better measured when split into two separate measurements of power imbalance and mutual dependence, which have opposing effects on one another. Casciaro and Piskroski (2005) find that power imbalance plays a key role in an organization's effectiveness, and when re-modeled, has the potential to address the interorganizational aspects at play. Thus, organizational effectiveness can address the inner aspects of an organization and how it operates.

The organizational environment is described by Pfeffer and Salancik (1978) as an organization shifting to its environment based on environmental survival of a focal organization. This shifting of the environment is described is the firm environment that is based on the resources that exist internally within firms. Organizational survival is an important aspect of resource dependence theory and addresses how organizations will have to shift for survival when an organization's environment is dependent on the resources available (Pfeffer and Salancik 1978). In addition, this intra-view of organizational resources is important as it explains how the internal and external powers interact with one another and how environments can shape the focus and needs of a firm (Pfeffer and Salancik 1978; Tillquist et al. 2002; Medcof 2001; Ulrich and Barney 1984).

Resources are the basis of power in RDT and the amount power that an organizational control versus what other organizations control in the environment can impose constraints on the focal firm (Pfeffer and Slancik 1978). Within these constraints, organizations are subject to understanding internal dependencies that exist in order to achieve the goals of the organization (Tillquist et al. 2002). By understanding its internal dependencies, firms can come to the actualizations necessary, through governance control, to achieve necessary goals (Tillquist et al. 2002). These constraints are important to understand because the resources of one organization can be offered and used to meet the constraint of another organization (Pfeffer and Slancik 1978). The search and need to solve such resources constraints offers potential merging points for two or more organizations.

Cloud Technologies and Smart Home Integration

Cybersecurity within cloud technologies has become a big topic of research within the information and privacy field (Borgman et al. 2016; Ahluwalia et al. 2018; Alrawi et al. 2019). Research on privacy and security within cloud technologies has spanned across topics such as cloud adoption, risk identification, and standards; however, there exists a gap in research examining the role of information governance in cloud cybersecurity (Borgman et al. 2016; Borgman et al. 2013; Morin et al. 2012; Prasad et al. 2013; Zainuddin 2012). Cloud cybersecurity research has focused on threat analysis on events such as DDoS attacks, risk assessment, implementation of cloud services, value chain, and policy management (Prasad et al., 2013). Threat analysis research has investigated the effects of threats on firms, and the economics of threats on cloud services to firms (Ahluwalia et al. 2018; Becker and Bailey 2014; Keller and König 2014; Medcof 2001). Additionally, threat analysis research (existing research in the IS field on risk assessment) has focused on the risks that cloud services can bring to a firm

(Singh and Dutta 2018). Finally, risk assessment research has largely focused on the internal aspects of the firm and securing the internal infrastructures of the firm (Su 2011). Overall, within the existing body of research, cloud security has mostly focused on the internal structures related directly to the firms themselves. Smart home technologies hosted in the cloud have opened a new territory of privacy and security integrations of these devices.

What once were simple network integrations have now become more highly integrated "enterprise like" networks and device connectivity within consumers' homes (Alrawi et al. 2019). Integrated cloud infrastructures within consumers' homes are now beckoning to a new age of security and privacy, comprised of multi-networked devices from smart assistants, smart phones, smart security cameras, to smart appliances (Alawi et al. 2019). Furthermore, these smart home infrastructures are opening a new relationship between security and privacy issues related to the information governance of data between firms and consumers (Van Oorschot and Smith 2019; Zhou et al. 2019). These security and privacy issues are only expected to grow as more devices and newer smart home technologies are developed and implemented (Alawi et al. 2019; Ding and Hu 2018; Celik et al. 2018).

Smart Home Devices: Extant Research on Privacy and Security

Extant privacy and security research on smart home devices has explored various topics such as: privacy risks, IoT (internet of things) detection, and vulnerabilities; interoperability issues between home-based IoT devices and mobile devices; lack of user knowledge about IT security practices; and information sharing and disclosure behaviors of smart home devices. Privacy risks are abundant within smart home devices, much of the extant literature has addressed the questions of "what does a security or privacy risk of an IoT smart device look like" or "how can these IoT smart home devices be compromised, and what data is exposed"

(Notra et al. 2014; Ding and Hu 2018; Hernandez et al. 2014; Van Ooschot et al. 2019). The findings of privacy and security research on IoT smart home devices has found that much of the reason why IoT smart home devices have privacy risks is due to a disconnect between the development of these electronics and the user-implementation of them (Van Ooschot and Smith 2019; Zeng et al. 2017). Security and privacy researchers have found that the security architecture of many of these devices have been built without a security-mindset to protect the data that these devices collect, with most of these technologies aimed at being usable for the customers not necessarily as more secure (Zhou et al. 2019). Findings from this research has indicated that there are easy ways to intercept the data being shared between smart home devices, leaving consumers vulnerable to having their data of their devices (including location, name, address, and other personal information) exposed to hackers (Zhou et al. 2019, O'Connor et al. 2019). Because many of the smart home devices are designed to be usable for consumers, it has also been found that most consumers do not know or are not aware of steps that they need to take to protect their data (Van Ooschot and Smith 2019; Zhou et al. 2019). User-based implementation research has found that most consumers expect for these devices to protect and secure their data (Van Ooschot and Smith 2019). Research has found that the consumer's lack of security knowledge on how to secure their personal smart home devices has also become an issue of vulnerability for unauthorized access of consumers' devices and data (which are usually hosted in the cloud) (Zeng and Rosener 2017). Related to a user's lack of knowledge, research on information disclosure behaviors has found that consumers are more willing to disclose security information about their IoT smart home to take care of their home (i.e. smart door lock info, smart camera info, etc.) to friends, neighbors, and family (Jha et al. 2019). This openness to disclosure can cause issues of data protection because most consumers do not have practices for

access control and password changing policies once they share this information with other consumers who are not from the same household (Jha et al. 2019). Overall, extant research points to a growing need for 1) firms to develop more secure IoT devices that can protect data and secure these devices from vulnerabilities, and 2) for consumers to be more aware of how to implement more secure changes to control the data that they share.

CYBERSECURITY RESOURCE GOVERNANCE OF IOT SMART HOME DEVICES: A PROPOSED THEORETICAL MODEL

As smart home devices continue to gain popularity among consumers, more integrated frameworks that address the impacts of cybersecurity governance of these devices should be derived to help consumers with their data protection and privacy. Figure 1 presents the proposed theoretical model for addressing how resource governance theory, data policies and management, and information governance have the potential to address the security issues that relate to smart home devices. The main focus of this research is on the interaction between resources available, present policies, and information governance of smart home devices. Resources available to the firm impact how they integrate and implement customer data policies, and management of said policies for consumers. In turn, policies from the smart home device developers consequently impact how information governance is implemented.

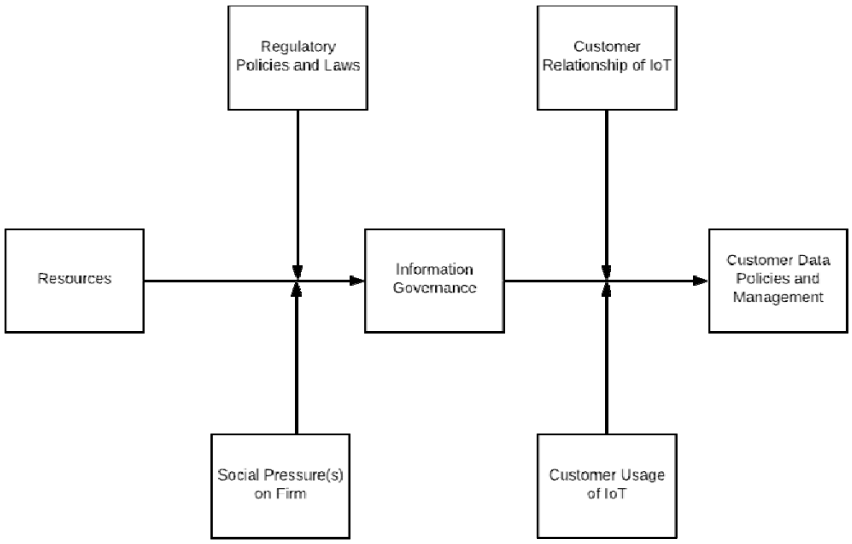

Figure 1. Theoretical Model: Resource Governance Cybersecurity Model of Smart Home Devices

PROPOSITIONS

RDT's main conceptual elements of organization effectiveness, environment, and constraints define how an organization acts to a specific environment (Pfeffer and Salancik 1978; Ulrich and Barney 1984). Research has shown that for smart home devices, resources available to the firm (such as development and cybersecurity teams) have defined how these technologies were developed (Zhou et al. 2019; O'Connor et al. 2019; Van Oorschot and Smith 2019). Research has uncovered security issues in these devices, because of development teams not integrating security that protects the consumers (Zhou et al. 2019; Van Oorschot and Smith 2019). As RDT proposes resources being the foundation, we suggest the following proposition:

Proposition 1: The type of resources that a firm has affects the information governance of smart home devices.

As smart homes are a fairly new and rapidly growing area of technology, information governance surrounding the data regulations on these devices will continue to transform

(Wachter 2018). Furthermore, current news reports and research shown that governmental regulatory policies will have an effect on the information governance of these devices (Sysman 2019; Richter et al. 2019). The U.S. does not presently have any federally regulatory laws to address these technologies. States such as California has enacted an IoT law, which will be enacted on January 1, 2020 for smart devices to ensure that consumers information is reasonably protected and that security safeguards are met such to protect these consumers (SB-327 Information Privacy: Connected Devices 2019). In addition, the U.K. has implemented GDPR (General Data Protection Regulation), which includes best practices for IoT devices and data safeguards for consumers; in turn, GDPR has impacted how smart home technologies consent to data usage, collection, analysis, and deletion processes (Wachter 2018; GDPR 2016). We expect in the coming of years that changes like these will be made in the U.S., further influencing the landscape of the information governance of smart home devices. Therefore, we propose the following mediating relationship:

> ***Proposition 1-1:*** Regulatory policies and laws have a moderating effect on the resources and information governance of smart home devices.

Along with the regulatory policies moderating the relationship between resources and information governance of smart home devices, we propose that social pressure(s) on a firm also mediate these constructs. Throughout the development and implementation lifecycles of smart home devices, device breaches or privacy vulnerabilities have put pressures on the firms to become more transparent about the customer privacy policies and data policies (Nieva and Rubin 2019; Brandom 2019; Mangalindan 2019; Osborne 2019; Segarra 2019; Gonzalez 2019). One example of this can be seen in the shift of both Amazon and Google allowing for consumers to access smart home device recordings in the cloud after privacy researchers and consumers alike

brought up these concerns (Nieva and Rubin 2019; Osborne 2019; Segarra 2019; Amazon 2019; Google 2019). As more vulnerabilities are uncovered and consumers become aware of these issues, we suspect that social pressures on firms will continue to grow. Therefore, we propose:

> ***Proposition 1-2:*** Social pressure(s) on a firm have a moderating effect on the information governance of smart home devices.

Related to the resources, information governance plays a role in how customer data policies and management is implemented on the cloud based IoT devices and the security of those devices. Because customer data and privacy policies define how the smart home devices are used, it's important to understand the relationship that these policies play in the development and implementation of the information governance and security aspects of these devices. Best practice governance standards such as COBIT 2019 and the ISO/IEC 27000 provide great examples of for firms to implement within their development teams (ISACA 2019; ISO 2019). However, COBIT 2019 and ISO/IEC 27000 are just best practice models that apply to the internal development and management processes inside firms (ISACA 2019; ISO 2019). The FTC (Federal Trade Commission) released an IoT report on the cybersecurity and privacy issues with smart devices, conversely, there have not been any federally regulated laws enacted in the U.S. (FTC 2015). Regulatory laws such as GDPR and California's SB-327 define the types of data safeguards smart home developers must implement in regard to data collection, data archiving, and data processing to protect consumers and to increase device security (Richter et al. 2019; GDPR 2016; SB-327 Information Privacy: Connected Devices 2019). GDPR has started to shape how firms notify and enact customer data policies, and this is expected to change as more states in the U.S. begin to implement similar policies such as the one enacted by California (Wachter 2018; GDPR 2016; Perez et al. 2018). Therefore, we propose:

Proposition 2. Information governance affects the customer data policies of the smart home and the IoT security of the device.

In addition to the overall security of the smart home devices, we believe that there are two possible moderating constructs: the customer relationship of the device, and the customer usage of these smart home devices. Previous research on IoT devices and smart home electronics has found that when a consumer is less knowledgeable about the privacy and security of a device, they are less likely to fully implement said technology, and might be more cautious about the ways that they use and interact with the technology (O' Connor et al. 2019; Zeng et al. 2017; Zhou et al. 2019). Therefore, we propose the following two mediators:

Proposition 2-1: Customer relationship of IoT has a moderating effect on the customer data policies and management and the IT governance and IoT security of smart home device.

Proposition 2-2: Customer usage of IoT has a moderating effect on the customer data policies and management and the IT governance and IoT security of smart home device.

DISCUSSION

This article explored the application of information governance and resource dependence theory in the context of cloud-based smart home IoT devices. With the emergence of these technologies, firms need to become more aware and develop a deeper understanding of the types of cybersecurity issues that affect consumers and systems alike; especially when considering security perceptions, the experience of customers, and how these issues affect the market opportunity of the digital home market. Because of the complexity of the systems and information at stake, we propose a Resource Governance Model to address internal cybersecurity issues that are embedded within cloud based smart products.

IMPLICATIONS AND FUTURE CYBERSECURITY RESEARCH

The contribution of this research is two-fold: (1) organizational theories that are employed to address a new dimension of cybersecurity such as product firm cybersecurity factors that affect cloud-based smart home products, and (2) the proposal of a new theoretical cybersecurity research model; the Resource Governance Model (RGM). This model highlights how internal cybersecurity governance impacts consumer cloud-based technology products and sets a direction.

Future studies on cloud cybersecurity using the RGM model can address cybersecurity challenges that arise through the shift in consumer IT infrastructure to smart home devices. Future IS research should address this evolution, with the resource governance model providing a foundation for this examination and for understanding differences in cybersecurity governance and related resources across firms. This paper also addresses the area of smart home device data collection and security. This is a vital subject given the diffusion of smart home devices and the private and personal data being collected within homes. Especially when the use of that data can be outside of what consumers may expect. For example, some firms have been awarded governmental contracts for sharing smart home camera footage on public social platforms without data release agreements from the customers or individuals present in the videos (Harwell 2019). Additionally, smart home devices and smart toys have been created and marketed for children and pets and collect information such as the GPS coordinates of your children or animals, feeding times of pets, and learning behaviors of children (Harwell 2019; Mozilla n.d.). While such data can inform product and service decisions, even improving the fit of future offerings, firms must address the cybersecurity and protection of such data. We see the Resource Cybersecurity Governance Model as a starting point for undertaking such research.

REFERENCES

Ahluwalia, P., and Merhi, M. 2018. "Moral and Subjective Norms: How Do They Effect Information Security Compliance?" in *Proceedings of the 24th Twenty-fourth Americas Conference on Information Systems (AMCIS),* New Orleans, Louisiana, *USA.*

Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). "SoK: Security evaluation of home-based IoT deployments," *IEEE S&P* (pp. 208-226).

Amazon. 2019. "Alexa Terms of Use." from https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740

Becker, J., and Bailey, E. 2014. "A Comparison of IT Governance & Control Frameworks in Cloud Computing," in *Proceedings of the 20th Americas Conference on Information Systems (AMCIS),* Savannah, Georgia, USA

Borgman, H., Heier, H., Bahli, B., and Boekamp, T. 2016. "Dotting the I and Crossing (out) the T in IT Governance: New Challenges for Information Governance," in *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS): IEEE*, pp. 4901-4909.

Borgman, H. P., Bahli, B., Heier, H., and Schewski, F. 2013. "Cloudrise: Exploring Cloud Computing Adoption and Governance with the Toe Framework," in *Proceedings of* the *46th Hawaii International Conference on System Sciences: IEEE*, pp. 4425-4435.

Brandom, R. 2019. Amazon pushes Alexa privacy with new delete options. From https://www.theverge.com/2019/9/25/20883745/amazon-alexa-privacy-hub-security-voice-recordings-echo-devices

Casciaro, T., and Piskorski, M. J. 2005. "Power Imbalance, Mutual Dependence, and Constraint Absorption: A Closer Look at Resource Dependence Theory," *Administrative Science Quarterly* (50:2), pp. 167-199.

Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., and McDaniel, P. 2018. "Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities," *arXiv preprint arXiv:1809.06962*).

Ding, W., and Hu, H. 2018. "On the Safety of IoT Device Physical Interaction Control," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security: ACM*, pp. 832-846.

Donaldson, A., & Walker, P. 2004. "Information Governance—A View From the NHS," *International Journal of Medical Informatics*, *73*(3), pp. 281-284.

Federal Trade Commission. 2015. "Internet of Things: Privacy & Security in a Connected World," *Washington, DC: Federal Trade Commission*.

GDPR. 2016. "Regulation (Eu) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/Ec (General Data Protection Regulation) (Oj L 119, 4.5.2016, P. 1–88)," in: 2016/679. Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.

Gonzales, O. 2019. Google assistant updates seek to calm privacy concerns over human review. From https://www.cnet.com/news/google-assistant-updates-seek-to-calm-privacy-concerns-over-human-review/

Google. 2019. "Data Security & Privacy on Google Home." From https:// support.google.com/googlehome/answer/7072285?hl=en

Grant, R. M. 1991. "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation," *California management review* (33:3), pp. 114-135.

Harwell, D. 2019. "Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns." From https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/

Hernandez, G., Arias, O., Buentello, D., and Jin, Y. 2014. "Smart Nest Thermostat: A Smart Spy in Your Home," in *Proceedings of Black Hat USA*, pp. 1-8.

IDC. 2018. "Worldwide Spending on Security Solutions Forecast to Reach $91 Billion in 2018, According to a New IDC Spending Guide." From https://www.idc.com/getdoc.jsp?containerId=prUS43691018

IDG. 2018. "2018 Cloud Computing Survey." From https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/

ISACA. 2019. COBIT 2019 Framework: Introduction and methodology. From http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Introduction-and-Methodology.aspx

ISO. 2019. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. From https://www.iso.org/standard/73906.html

Jha, A., Kropczynski, J., Lipford, H. R., and Wisniewski, P. J. 2019. "An Exploration on Sharing Smart Home Devices Beyond the Home," in *Proceedings of Intelligent User Interfaces Workshops* 20 March 2019, Los Angeles, California, United States.

Keller, R., and König, C. 2014. "A Reference Model to Support Risk Identification in Cloud Networks."

Khatri, V., & Brown, C. V. 2010. "Designing Data Governance," *Communications of the ACM*, *53*(1), pp. 148-152.

Kooper, M. N., Maes, R., & Lindgreen, E. R. 2011. "On the Governance of Information: Introducing a New Concept of Governance to Support the Management of Information," *International Journal of Information Management*, *31*(3), pp. 195-200.

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., and Fu, X. 2017. "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System," *IEEE Internet of Things Journal* (4:6), pp. 1899-1909.

Mangalindan, J.P. 2019. 3 things to expect from amazon's Alexa hardware event on Wednesday. From https://fortune.com/2019/09/24/amazon-alexa-earbuds-new-speaker-privacy

Medcof, J. W. 2001. "Resource-Based Strategy and Managerial Power in Networks of Internationally Dispersed Technology Units," *Strategic Management Journal* (22:11), pp. 999-1012.

Morin, J.-H., Aubert, J., and Gateau, B. 2012. "Towards Cloud Computing Sla Risk Management: Issues and Challenges," in *Proceedings of the 45th Hawaii International Conference on System Sciences: IEEE*, pp. 5509-5514.

Mozilla. N.d. "*Privacy Not Included Guide." From https://foundation.mozilla.org/en/privacynotincluded

Nieva, R. and Rubin, B. F. 2019. "Amazon Alexa adds new commands to tamp down privacy concerns." From https://www.cnet.com/news/amazon-alexa-adds-new-commands-to-tamp-down-privacy-concerns/

Notra, S., Siddiqi, M., Habibi Gharakheili, H., Sivaraman, V., and Boreli, R. 2014. "An Experimental Study of Security and Privacy Risks with Emerging Household Appliances," in *Proceedings of 2014 Conference on Communications and Network Security:* IEEE, pp. 79-84.

O'Connor, T., Mohamed, R., Miettinen, M., Enck, W., Reaves, B., and Sadeghi, A.-R. 2019. "Homesnitch: Behavior Transparency and Control for Smart Home IoT Devices," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*: ACM, pp. 128-138.

Osborne, C. 2019. Google revamps privacy policy to give users more control over assistant voice recordings. From https://www.zdnet.com/article/google-revamps-privacy-policy-to-give-users-more-control-over-assistant-voice-recordings/

Perez, A. J., Zeadally, S., and Cochran, J. 2018. "A Review and an Empirical Analysis of Privacy Policy and Notices for Consumer Internet of Things," *Security and Privacy* (1:3), p. e15.

Pfeffer, J., and Salancik, G. R. 2003. The External Control of Organizations: A Resource Dependence Perspective. Stanford University Press.

Ponemon. "2017 Cost of Data Breach Study." From https://www.ibm.com/account/reg/us-en/signup?formid=urx-15763

Prasad, A., Green, P., Heales, J., and Finau, G. 2013. "On Structural Considerations for Governing the Cloud," in *Proceedings 19th Americas Conference on Information Systems (AMCIS)*, 15-17 August 2013, Chicago, Illinois, USA.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).2016/679.

Richter, J., Milne, K., and Hiner, V. 2019. "State Lawmakers Go after IoT Security Risks ", from https://www.govtech.com/policy/State-Lawmakers-Go-After-IoT-Security-Risks-Contributed.html

SB-327 Information privacy: connected devices.1798.91.04.

Segarra, L.M. 2019. Google says it's cutting back on audio data collection on google home speakers. From https://fortune.com/2019/09/23/google-home-privacy-changes/

Simonin, B. L., and Ruth, J. A. 1998. "Is a Company Known by the Company It Keeps? Assessing the Spillover Effects of Brand Alliances on Consumer Brand Attitudes," *Journal of marketing research* (35:1), pp. 30-42.

Singh, V., and Dutta, K. 2018. "Predicting Security Events in Cloud Computing," in *Proceedings of 24th Twenty-fourth Americas Conference on Information Systems (AMCIS),* 16-18 August 2018, New Orleans, Louisiana, *USA.*

Statista. 2019. Smart Home Market. From https://www.statista.com/out look/279/109/smart-home/united-states

Su, N. 2011. "Emergence of Cloud Computing: An Institutional Innovation Perspective," in *Proceedings of the 31st International Conference on Information Systems* , St Louis, MO, Paper 11.

Sysman, D. 2019. "California's IoT Security Law: Why It Matters and the Meaning of 'Reasonable Cybersecurity'." from https://www.forbes.com/sites/forbestechcouncil/2019/11/20/californias-iot-security-law-why-it-matters-and-the-meaning-of-reasonable-cybersecurity/#4bb841551e2d

Tallon, P. P., Ramirez, R. V., and Short, J. E. 2013. "The Information Artifact in IT Governance: Toward a Theory of Information Governance," *Journal of Management Information Systems* (30:3), pp. 141-178.

Tillquist, J., King, J. L., and Woo, C. 2002. "A Representational Scheme for Analyzing Information Technology and Organizational Dependency," *MIS Quarterly*, pp. 91-118.

Ulrich, D., and Barney, J. B. 1984. "Perspectives in Organizations: Resource Dependence, Efficiency, and Population," *Academy of Management Review* (9:3), pp. 471-481.

Van Oorschot, P. C., and Smith, S. W. 2019. "The Internet of Things: Security Challenges," *IEEE Security & Privacy* (17:5), pp. 7-9.

Wachter, S. 2018. "Normative challenges of identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR". *Computer law & security review*, *34*(3), pp. 436-449.

Watson, H. J., Fuller, C., & Ariyachandra, T. 2004. "Data Warehouse Governance: Best Practices at Blue Cross and Blue Shield of North Carolina," Decision *Support Systems*, *38*(3), pp. 435-450.

Weill, P., and Ross, J. W. 2004. "IT Governance: How Top Performers Manage It Decision Rights for Superior Results," Harvard Business Press.

Willson, P., and Pollard, C. 2009. "Exploring IT Governance in Theory and Practice in a Large Multi-National Organisation in Australia," *Information Systems Management* (26:2), pp. 98-109.

Zainuddin, E. 2012. "Secretly SaaS-Ing: Stealth Adoption of Software-as-a-Service from the Embeddedness Perspective," in *Proceedings of 33rd International Conference on Information Systems (ICIS)*, 16-19 December 2012, Orlando, Florida, USA.

Zeng, E., Mare, S., and Roesner, F. 2017. "End User Security and Privacy Concerns with Smart Homes," in *Proceedings of the Thirteenth Symposium on Usable Privacy and Security* ({SOUPS} 2017), pp. 65-80.

Zhou, W., Jia, Y., Yao, Y., Zhu, L., Guan, L., Mao, Y., Liu, P., and Zhang, Y. 2019. "Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms," in *Proceedings of 28th {USENIX} Security* Symposium ({USENIX} Security 19), pp. 1133-1150.