Oct 20th, 11:55 AM - 12:20 PM

Information Privacy Concerns in the Age of Internet of Things

Madhav Sharma
Oklahoma State University - Main Campus, madhav.sharma@okstate.edu

David Biros
Oklahoma State University - Main Campus, david.biros@okstate.edu

Abstract
Internet of things (IoT) offer new opportunities for advancement in many domains including healthcare, home automation, manufacturing and transportation. In recent years, the number of IoT devices have exponentially risen and this meteoric rise is poised to continue according to the industry. Advances in the IoT integrated with ambient intelligence are intended to make our lives easier. Yet for all these advancements, IoT also has a dark side. Privacy and security were already priorities when personal computers, devices and work stations were the only point of vulnerability to personal information, however, with the ubiquitous nature of smart technologies has increased data collection points around us exponentially. Beyond that, the massive amount of data collected by IoT devices is relatively unknown and uncontrolled by users thereby exacerbating privacy issues and concerns. This study aims to create better understanding of privacy concerns stemming from most popular smart technologies, categorizing the data collected by them. We investigate how the data collection raises information privacy concerns among users of IoT.

Location
KC 460

Disciplines
Applied Behavior Analysis | Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Rapid advancements in electronics and connectivity have enabled users to connect everyday 'things' such as home appliances, vehicles and, wearables to each other. As chips get smaller and gain more processing power (Moore's Law), embedding physical objects with actuators, sensors and, small computers has become easier. Connectivity among these 'things' help users better monitor themselves (wearable technologies) and their environments (thermostats and motion sensors), increase convenience in everyday tasks (smart speakers, baby monitors) and, do plethora of other tasks that were not automated before (storefronts, smart locks, smart beds, vacuum cleaner). Internet of Things (IoT) is defined as '*connectivity of physical objects equipped with sensors and actuators to Internet via data communication technologies'(Oberländer, Röglinger, Rosemann, & Kees, 2018)*. Advances in IoT integrated with ambient intelligence can assist the elderly in daily living tasks making them more independent (Dohr, Modre-Opsrian, Drobics, Hayn, & Schreier, 2010), help people monitor their health (Yang et al., 2014), automate many tasks around the house (Gubbi, Buyya, Marusic, & Palaniswami, 2013) and, help to make driving safer (Chang et al., 2009). For all the good smart technology is poised to accomplish there can be many unintended consequences. Recent news reports of home security cameras being used in hacking attacks (KYODO, 2018) and physical fitness device data inadvertently showing the location of secret military bases underscore the security consequences (Taylor, 2018).

These anecdotes barely scratch the surface of how quickly concerns regarding privacy and security of IoT devices have gained the attention of media and research community. IoT has featured prominently in marketing research dealing with its acceptance and its system's integrity (De Cremer, Nguyen, & Simkin, 2017), research in computer science regarding its development (Atzori, Iera, & Morabito, 2010), security and, privacy (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015). However, due to limited penetration in day to day firm-level functions, information systems (IS) research has displayed limited interest in security and privacy scene of IoT. Combined market value of IoT is predicted to be over $7.1 trillion by 2020 (Hsu & Lin, 2016) with estimated number of devices projected to be over 50 billion (Nordrum, 2016). These developments indicate a growing interest in IoT's market and hence warrants more attention from IS research.(Lowry, Dinev, & Willison, 2017) claimed that the rise of IoT is rewriting rules of organizational privacy and security. IoT has gained prominence due to rapid adoption of smart speakers (Alexa, Homepod, and Google Home) by general

consumers (NPR, 2017).These speakers are usually cloud based and act as a de facto platform for all other IoT devices at home such as lights, thermostats, locks, and cameras (Wyman, 2015). The ubiquitous nature of IoT has increased data collection points in user's environments exponentially (Sun, Song, Jara, & Bie, 2016). All these devices work collectively to provide convenience such as ability to track health, monitor and change temperature and lighting, and, secure their home from burglaries. These devices are capable of continuously collecting personal data about their user's behavior. The massive amount of personal data collected by IoT devices is relatively unknown and uncontrolled by users thereby exacerbating privacy issues and concerns.

The objectives of this study are twofold. First, we seek to identify popular IoT devices and categorize the type of data collected by IoT. Second, we aim to determine the extent to which, users are concerned about the privacy implications of IoT.

LITERATURE REVIEW

Even though IoT is recognized as one of the most disruptive technologies in this decade, it is not consistently defined in academic literature (Atzori et al., 2010),. (Oberländer et al., 2018) compiled an extensive literature review over previous influential articles in IS and other research over IoT to triangulate the characteristics that makes classification of IoT clearer. They identified two dimensions and nine characteristics to compare different definitions (Table 1).

The first dimension, *Communication* refers to the capability of the device to connect to a network of devices (such as hubs, computers, phones, and, other IoT devices). These capabilities can be wired technologies such as fiber optics, telephone networks, Ethernet etc. or wireless technologies such as WiFi, Bluetooth, ZigBee, etc. Though 'Internet' has been an enabler of IoT devices, the characteristics in this dimension are not limited to devices that have the capability to connect to the TCP/IP network (Oberländer et al., 2018). These devices can display connectivity characteristics that do not necessarily lead to connection to the internet. For example: Zigbee hubs enable lighting and thermostats to be controlled by the user without internet.

The second dimension, *Thing* has more ambiguity surrounding its characteristics. There has been debates about inclusion of mobile devices and computers under IoT (Atzori et al., 2010; Mattern & Floerkemeier, 2010). (Oberländer et al., 2018)'s literature review compared and contrasted different

approaches and concluded in making two sub dimensions of *thing*: Identity and Capability. Identity refers to what an object is and capability refers to what an object has. Characteristics in the identity sub dimension are sensors, actuators, mobile devices and computers, physical objects, virtual objects. Similarly, characteristics in the capability dimension are ability of sensing (sensing and passing signals) and interacting (participation in reciprocal request and providing feedback)(Vermesan & Fries, 2014).

Dimension	**Characteristics**
Communication Dimension	Wired
	Wireless technologies
	Internet-only
Thing Dimension – Identity	Sensors and Actuators
	Mobile device and computers
	Physical Object (with embeded technology)
	Virtual Objects
Thing Dimension – Capability	Sensing
	Interacting

Table 1: Dimensions and characteristics of IoT(Oberländer et al., 2018)

According to the theory of diffusion of innovation (Rogers, 2010), adoption of new innovations follows a roughly fixed pattern (Shown in Figure 1). As market share increases different groups of consumers (Social participants) adopt it subsequently. According to a report compiled by Edison Research and NPR, 16% of Americans over the age of 18 used smart speakers at home. According to the market shares, we consider IoT to be in 'early majority' stage. As the market grows, these devices are poised to be deeply integrated in user's lives. The market for IoT enabled smart speakers is new and anticipated to grow by 48% annually (Koetsier, 2018).

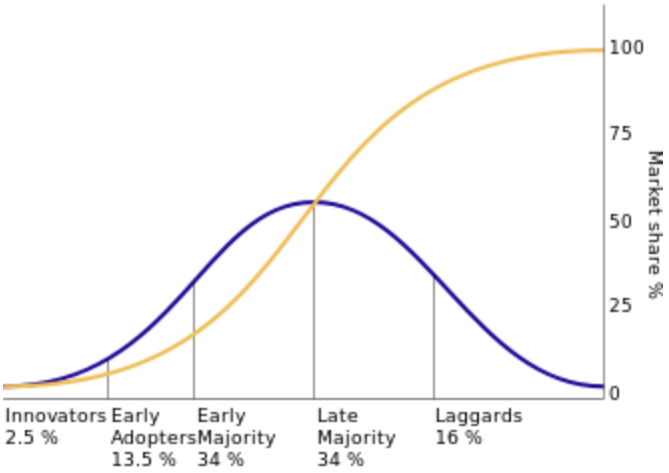

Figure 1: Diffusion of Innovation (Rogers, 2010)

There is precedence that an increase in data collection capabilities of devices raises information privacy concerns among users (Bélanger & Crossler, 2011; Smith, Milberg, & Burke, 1996; Stewart & Segars, 2002). With enhanced data collection capabilities (Sun et al., 2016) and increasing market share, IoT is becoming a potential source of privacy concern.

Research Question: To what extent are users concerned that they are surrendering their personal data by using IoT devices?

Qualitatively understanding these data collection capabilities of IoT devices is imperative since these capabilities initiate information privacy concerns among users (Smith et al., 1996). Information privacy concerns have been studied extensively in literature. (Westin & Ruebhausen, 1967) defined information privacy 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'. Information privacy concerns are subjective views of fairness of an individual in context of information privacy(Campbell, 1997). Users tend to value their personal information and its release is regarded as risky transaction as their information becomes vulnerable to opportunistic behavior of external entities. (Malhotra, Kim, & Agarwal, 2004) examined internet users' information privacy concerns and its dimensionality under the theoretical lens of social contract theory and concluded that concerns or perceptions of data collection, perceived control over personal data, and awareness of privacy practices influences information privacy concerns. They categorized these factors as dimensions of information privacy concerns.

The first dimension, '*Collection'* of data in this context, is measured as the degree to which a user is concerned about the amount of personal data possessed by others relative to its perceived benefits. Users submit their personal data in exchange for value after evaluating the predicted output (Laufer & Wolfe, 1977). This value may come in the form of personalized marketing suggestions or better health outcome as a result of monitoring. According to the theory of distributive justice, in this context, users choose to surrender their data after evaluating the possibilities of positive and negative outcomes (Cohen & affairs, 1997). In e-commerce and social media, presence of user interface (a website or an app) ensures that transactions of data are way more direct and controlled by the users since the user has a choice to initiate or not initiate the data transaction (Cranor, Reagle, & Ackerman, 2000). Social media is deeply integrated in user's daily lives and is a platform for variety of data transactions in form of personal features, sharing pictures, thoughts, and opinions. Transactions initiated by the users provide them with a sense of control over their information. Unlike e-commerce or social media, the transactions of data are not completely controlled by the users during the use of IoT (Ziegeldorf, Morchon, Wehrle, & Networks, 2014). Once a user possesses, configures and installs an IoT device (a wearable or home automation platform comprising sensors and actuators), the device has the capability to collect previously 'not anticipated data' and 'passive data' continuously, which may or may not be stored for organization's use (Abrams, 2014).

The second dimension, '*control'* is referred to as user's concern regarding individual has control over personal information by existence of voice or exit(Caudill & Murphy, 2000). User's 'perceived *control'* has been a significant variable in their concern over privacy invasion (Laufer & Wolfe, 1977). The greater the users value privacy, the less control they perceive to have over their personal data (Stone, Gueutal, Gardner, & McClure, 1983). However, when a user's intention to use is personalization (when the user wants convenience and custom offerings), it has been found that the value of personalization outweighs privacy concerns (Chellappa & Sin, 2005). In the past two decades, several technologies such as social media and online shopping, have offered users increased convenience (with personalized offerings) in exchange for personal data. Users who tend to value their privacy are seldom inclined to be transparent about their personal data while they are also enticed to get convenient personalized offerings giving rise to Personalization Privacy Paradox (Awad & Krishnan, 2006). IoT poses the same paradox to the users who tend to value their privacy but are also tempted to use personalized features. These users are theoretically poised to value personalization more than their privacy concerns. However, since IoT is in a relatively early stages

of diffusion, users do not completely know what information they are surrendering. It is interesting to note that with this ambiguity, do users still value personalization or are they unaware of the information they are surrendering?

The third dimension, '*awareness'* is measured as degree to which a user is concerned about the organization's privacy practices (Laufer & Wolfe, 1977). An organization in this context can be a manufacturer of IoT device (Amazon, google, Phillips) or a platform that these devices run on (Amazon voice services, Siri, Geeni). An organization's data practices plays an important role in user's evaluation of tradeoff between potential benefits and potential negative outcomes in data transaction. Drawing parallels to online shopping and social media, terms and conditions and privacy policies are highly publicized mechanics of data transactions in these technologies(Ackerman, Cranor, & Reagle, 1999),(Acquisti & Gross, 2006). Regardless of willingness to read the privacy policies, users refuse to reveal personal information when they are not sure how the data will be used (Hoffman, Novak, & Peralta, 1999). The user awareness of privacy practices of the organization is based on trust in the organization (Liu, Marchewka, Lu, & Yu, 2005). Due to lack of tangible user interface, IoT's data collection is largely passive and not anticipated (Abrams, 2014). Users have less opportunities to get familiar with privacy policies of IoT. Thus, trust in organization inclines them to share their personal data while using IoT. (Belanger, Hiller, & Smith, 2002) defined trustworthiness in context of e-commerce as *'perception of confidence in electronic marketer's reliability and integrity'*. This same definition can be applied in context of trustworthiness of IoT manufacturers. Instead of using the construct of awareness, it can be argued that trustworthiness in an organization's privacy policies better explains IoT information privacy concerns.

We adopt a modified part of the IUIPC model from (Malhotra et al., 2004) to test the effect of perception of data collection, perceived control over sharing personal data and, trust in organization of collection of personal data on IoT users' information privacy concerns using the following propositions.

Proposition 1: User's perception of collection of personal data gives rise to IoT information privacy concerns.

Proposition 2: User's concerns over control of personal data gives rise to IoT information privacy concerns.

Proposition 3: User's trust in the organization gives rise to IoT information privacy concerns.

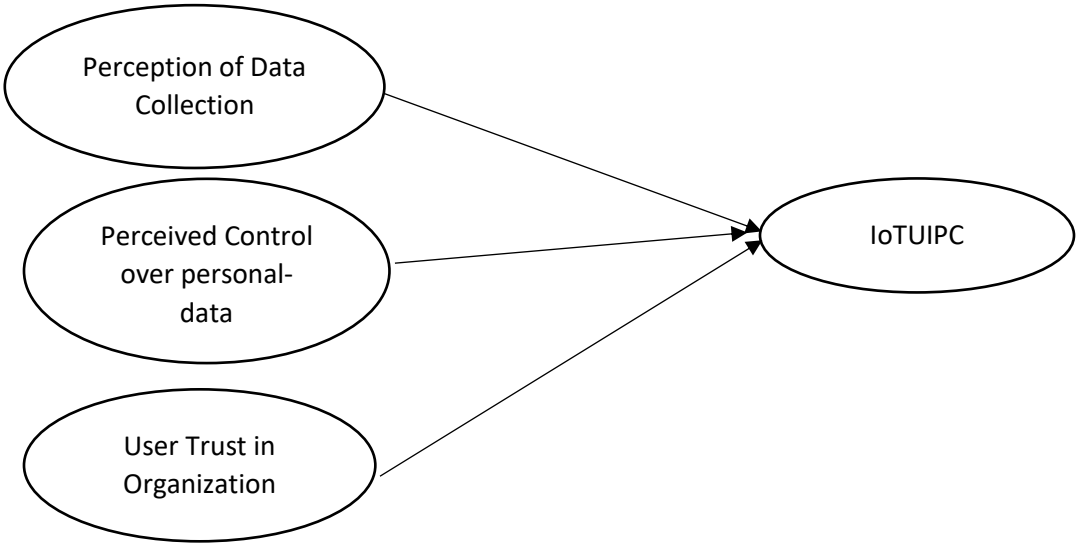

Figure 2: (Malhotra et al 2004)'s model for IUIPC adopted for IoTIPC

METHODOLOGY

Our goal is to analyze data collection capabilities of IoT devices and test effect of perception of data collection and, perceived control over personal data and user trust in organization's privacy practices on IoT privacy concerns. The analysis will be conducted using following two steps. First, we will do a qualitative capability analysis of data collection abilities of popular devices. Second, we will conduct a survey using existing scales from Malhotra et al 2004, (Smith et al., 1996), and (Belanger et al., 2002) to measure the constructs proposed in our model (Figure 2)

Objective 1: Capability Analysis

Data Collection

For our qualitative analysis, first, we will identify IoT devices available to consumers with market penetration of least 13.5%. We will study all devices with market penetration of 13.5% and more. Data about market penetration will be acquired individually for each device type. Due to loose standardization in IoT, we used National Institute of Standards and Technology's security and privacy considerations to lend us a framework to further identify IoT capabilities (NIST,

2018). (NIST, 2018)lists six capabilities that a device must possess to be considered as an IoT. We will collect data about these devices from multiple manufacturers. For each device, our variables and attributes will include the device's technical specifications like data storage (in GB), cloud back up ability, uplink to a smartphone app, RAM, manufacturer's information (headquarter country, OEM manufacturer's country), cost, and, market penetration. We will qualitatively study the access to data of the device (what sensors are used and what personal data of the users are these sensors and actuators exposed to).

Analysis

The personal data is categorized as per the taxonomy of personal data by origin (Abrams, 2014) (See Appendix 1). Using this classification, we are able to understand the scope of provided, observed, derived and inferred information collected by the most used IoT systems. This knowledge of scope will be used to study the degree of control, users are ready to release in order to get the convenience of personalization.

Objective 2: User Awareness

Data Collection

Based on results of objective 1, a survey will be designed and conducted of users of these IoT devices to understand their awareness of the data collected and its implications. We will build our survey using existing privacy and security scale based on information privacy concerns of internet users (Malhotra et al., 2004) and trust in organization's privacy practices (Belanger et al., 2002).We will incorporate data collection by the most used IoT devices to get a measure of user's personal dispositions and intent to give up privacy for personalization. The construction of survey is in process and will be submitted for an IRB review shortly.

Analysis

For this study, we are going to run a model according to Figure 2 to study estimated effect of concerns over data collection, control, and user awareness. This confirmatory analysis will help us test our 3 hypothesis mentioned above.

DISCUSSION

Our qualitative investigation proposed a device level analysis of data collection abilities of most used IoT devices. This part of study is chosen to be qualitative because there is limited research done on this group of devices. In future, we would consider adding laboratory experiments on these devices to further establish content validity. For our second objective, we are modifying Malhotra et al 2004's IUIPC scales according to the results of objective 1 in hopes of adding to the body of knowledge about user awareness. At this point of time, the study is a work in progress but we hope it will make significant contribution in IS literature in fields of privacy and user awareness.

REFERENCES

Abrams, M. (2014). The Origins of Personal Data and its Implications for Governance.

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). *Privacy in e-commerce: examining user scenarios and privacy preferences.* Paper presented at the Proceedings of the 1st ACM conference on Electronic commerce.

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the International workshop on privacy enhancing technologies.

Atzori, L., Iera, A., & Morabito, G. J. C. n. (2010). The internet of things: A survey. *54*(15), 2787-2805.

Awad, N. F., & Krishnan, M. S. J. M. q. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. 13-28.

Bélanger, F., & Crossler, R. E. J. M. q. (2011). Privacy in the digital age: a review of information privacy research in information systems. *35*(4), 1017-1042.

Belanger, F., Hiller, J. S., & Smith, W. J. J. T. j. o. s. I. S. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *11*(3-4), 245-270.

Campbell, A. J. J. J. o. D. M. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *11*(3), 44-57.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Chang, S.-H., Lin, C.-Y., Hsu, C.-C., Fung, C.-P., Hwang, J.-R. J. T. r. p. F. t. p., & behaviour. (2009). The effect of a collision warning system on the driving performance of young drivers at intersections. *12*(5), 371-380.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Journal of Information technology management* *6*(2-3), 181-202.

Cohen, G. A. J. P., & affairs, p. (1997). Where the action is: On the site of distributive justice. *26*(1), 3-30.

Cranor, L. F., Reagle, J., & Ackerman, M. S. J. T. I. u. r. q., seeking answers in communications policy. (2000). Beyond concern: Understanding net users' attitudes about online privacy. 47-70.

De Cremer, D., Nguyen, B., & Simkin, L. J. J. o. M. M. (2017). The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. *33*(1-2), 145-158.

Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., & Schreier, G. (2010). *The internet of things for ambient assisted living.* Paper presented at the Information technology: new generations (ITNG), 2010 seventh international conference on.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. J. F. g. c. s. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *29*(7), 1645-1660.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. J. T. I. S. (1999). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web. *15*(2), 129-139.

Hsu, C.-L., & Lin, J. C.-C. J. C. i. H. B. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *62*, 516-527.

Koetsier, J. (2018). Smart Speaker Users Growing 48% Annually, To Hit 90M In USA This Year. Retrieved from https://www.forbes.com/sites/johnkoetsier/2018/05/29/smart-speaker-users-growing-48-annually-will-outnumber-wearable-tech-users-this-year/#4e65a9b85dde

KYODO. (2018, May 7). Hackers disable scores of Canon-made security cameras across Japan. *The Japan Times.* Retrieved from https://www.japantimes.co.jp/news/2018/05/07/national/hackers-disable-scores-canon-made-security-cameras-across-japan/#.W22zWyhKiUk

Laufer, R. S., & Wolfe, M. J. J. o. s. I. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *33*(3), 22-42.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Journal of Information Management* *42*(2), 289-304.

Lowry, P. B., Dinev, T., & Willison, R. J. E. J. o. I. S. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *26*(6), 546-563.

Malhotra, N. K., Kim, S. S., & Agarwal, J. J. I. s. r. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *15*(4), 336-355.

Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things. In *From active data management to event-based systems and more* (pp. 242-259): Springer.

NIST. (2018). WHAT IS THE INTERNET OF THINGS (IOT) AND HOW CAN WE SECURE IT? Retrieved from https://www.nist.gov/topics/internet-things-iot

Nordrum, A. J. I. s. (2016). Popular internet of things forecast of 50 billion devices by 2020 is outdated. *18*.

NPR, E. R. a. (2017). *Smart Audio Report*. Retrieved from https://www.nationalpublicmedia.com/smart-audio-report/latest-report/

Oberländer, A. M., Röglinger, M., Rosemann, M., & Kees, A. J. E. J. o. I. S. (2018). Conceptualizing business-to-thing interactions–A sociomaterial perspective on the Internet of Things. *27*(4), 486-502.

Rogers, E. M. (2010). *Diffusion of innovations*: Simon and Schuster.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. J. C. n. (2015). Security, privacy and trust in Internet of Things: The road ahead. *76*, 146-164.

Smith, H. J., Milberg, S. J., & Burke, S. J. J. M. q. (1996). Information privacy: measuring individuals' concerns about organizational practices. 167-196.

Stewart, K. A., & Segars, A. H. J. I. S. R. (2002). An empirical examination of the concern for information privacy instrument. *13*(1), 36-49.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. J. J. o. a. p. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *68*(3), 459.

Sun, Y., Song, H., Jara, A. J., & Bie, R. J. I. a. (2016). Internet of things and big data analytics for smart and connected communities. *4*, 766-773.

Taylor, G. L. a. R. (2018, January 30). Pentagon Reviewing Troops' Use of Fitness Trackers in Light of Security Concerns. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/pentagon-reviewing-troops-use-of-fitness-trackers-in-light-of-security-concerns-1517290307

Vermesan, O., & Fries, P. (2014). Internet of Things–from research and development to market deployment. In: Aalborg: River Publishers.

Westin, A. F., & Ruebhausen, O. M. (1967). *Privacy and freedom* (Vol. 1): Atheneum New York.

Wyman, O. (2015). THE INTERNET OF THINGS - DISRUPTING TRADITIONAL BUSINESS MODELS.

Yang, G., Xie, L., Mäntysalo, M., Zhou, X., Pang, Z., Da Xu, L., . . . Zheng, L.-R. J. I. t. o. i. i. (2014). A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *10*(4), 2180-2191.

Ziegeldorf, J. H., Morchon, O. G., Wehrle, K. J. S., & Networks, C. (2014). Privacy in the Internet of Things: threats and challenges. *7*(12), 2728-2742.

APPENDICES

Category	Sub-Category	Example
Provided	Initiated	Applications, Registrations, Public records, Purchases
	Transactional	Bills Paid, Inquiries responses, Surveys
	Posted	Social networking posts, public speeches, photo and video services
Observed	Engaged	Website Cookies, loyalty program, location enabled on devices
	Not Anticipated	data from sensors when not in use
	Passive	facial images from cameras, obscured web technologies
Derived	Computational	Credit Ratios, average purchase per visit
	Notational	Classification based on common attributes (Tapestry Segments)
Inferred	Statistical	Credit Score, Response, score, fraud scores
	Advanced Analytical	risk of developing diseases based on multi factor analysis, college success score based on multi-variable big DATA analysis

Taxonomy of personal data (Abrams 2011)