Journal of Management, Marketing and Logistics
Year: 2017 Volume: 4 Issue: 3

CONSUMER PRIVACY IN INTERNET OF THINGS

DOI: 10.17261/Pressacademia.2017.487
JMML-V.4-ISS.3-2017(7)-p.251-258

Mehmet Marangoz[1], Ali Emre Aydin[2]
[1]Muğla Sıtkı Koçman University, Mugla, Turkey. mehmetmarangoz@mu.edu.tr
[2]Muğla Sıtkı Koçman University, Mugla, Turkey. aliemreaydin@mu.edu.tr

To cite this document
Marangoz, M. and A.E. Aydin (2017). Consumer privacy in internet of thıngs. Journal of Management, Marketing and Logistics (JMML), V.4, Iss.3, p.251-258.
Permemant link to this document: http://doi.org/10.17261/Pressacademia.2017.487

ABSTRACT

Purpose- This study aims to examine privacy from a consumer point of view and in relation to the Internet of Things.
Methodology- The concepts of Internet of Things and consumer privacy are covered in this study. These two phenomena are conceptually evaluated, and the relation between them are analyzed through applications and examples.
Findings- The monitoring of people's daily activities and recording of data about these activities cause concerns about the privacy of personal data. Consumers are concerned about how and for what purpose the data collected about them is being used.
Conclusion- Privacy concern can be an obstacle to consumers' adaptation to IoT technologies. Moreover, it also affects consumers' attitudes towards a particular product, brand or business. For this reason, all actors responsible for the development of the IoT must be aware of the importance of consumer privacy. These actors should show sensitivity to the protection of personal data and consumer privacy as well.

Keywords: Consumer, privacy, internet of things, personal data, concern.
JEL Codes: M20, M30, M31

1. INTRODUCTION

Internet of Things (IoT) is changing the decision-making and business processes of enterprises, governments and consumers. How they interact with the world is differentiated by these objects. Over the next five years, companies are expected to spend about 5 trillion dolars for IoT. The proliferation of IoT linked devices and the accompanying increase in the amount of data are indicators of an analytical revolution (Newman, 2017).

The process of producing, obtaining, communicating, and interpreting data is central to the design and implementation of IoT. This data relates specifically to consumers. Data such as date of birth, income, clicks on websites, social media comments, and similar information are already being obtained and used by businesses. IoT related objects have information about the behavior and the environment they are connected to. This corresponds to a totally different set of data. Blood composition, purchased and consumed food and beverages and eating habits are example of such personal data (Weinberg et al., 2015: 620).

Communication happening anywhere and at any time between people and objects will soon reach to unprecedented levels. For this reason, management of emerging data becomes crucial. The dynamic environment of IoT offers unique chances for

communication which transform the perception of computing and networking. However, such a revolution should also take into account secrecy and security issues. Thus, the protection of personal data and the privacy of users are now a fundamental problem in IoT (Kumar ve Patel, 2014: 25).

In this context, the development of IoT services requires privacy and security considerations. There is still a lack of vision to address the security and confidentiality requirements of IoT-related environments, including different tehcnologies and communication standarts. This is why, all relevant stakeholders should take responsibility for designing appropriate solutions (Sicari et al., 2015: 160).

This study aims to examine consumer privacy in relation to the IoT. The structure of the study is as follows. In the first part, IoT is discussed as a phenomenon and its importance is emphasized. Examples of related technologies are given and problems that may arise due to widespread use of IoT technologies are pointed out. The second part focuses on consumer privacy as one of the important problems that may arise with the proliferation of IoT technologies. This part deals with possible behavioral consequences of consumers who are concerned about the use of their personal data. The extent of consumer privacy is also discussed within this section. Thereinafter, consumer privacy is discussed in the contex of IoT. The relationship between the two phenomenon is examined. Suggestions for protecting the consumer's privacy are evaluated. In the final section, conclusions and suggestions are presented.

2. INTERNET OF THINGS

IoT is a phenomenon which deals with everyday devices that can be connected to the internet through small sensors and computers (Accenture, 2014). IoT is concerned with the ability to send and recieve data from daily objects connected to the internet. Systems that allow you to send photos instantly, applications that run your home heating system when you leave your office or smart wristbands which follow and share your cycling performance data are examples of these objects (FTC, 2015). Roman et al. (2013: 2266), summarize this approach in a single sentence: "*A worldwide network of interconnected entitites*". These things (human beings and computers, food and appliances, cars and books etc.) have a locatable, addressable and readable counterpart on the internet. They can create a communication channel with another entity by providing and taking services at any time, anywhere and in any form. Tools and technologies such as wireless sensor networks (WSNs), RFID, cloud services, machine-to-machine interfaces (M2M) are key elements of this new paradigm. This paradigm has many applications in the field. Automotive, healthcare, logistics and environmental monitoring are some of the sectors where this new paradigm becomes more and more prevalant.

From a conceptual point of view, IoT can be associated with three skills of smart objects. These are the ability to identify itself, the ability to communicate and the ability to interact. These processes can be accomplished either among the devices themselves or between them and the interconnected objects, end users or other entities on the network. Achieving full access to these talents and this vision can be seen as a major challange (Miorandi et al., 2012: 1498). Still, the process is moving fast. Today, many objects around us are somehow connected to a network. Radio frequency identification (RFID) and sensor network technologies will further enhance the presence of these objects in which information and communication systems are embedded. This will produce very large amounts of data to be recorded, stored, processed and interpreted easily (Gubbi et al., 2013: 1645).

This phenomenon is now becoming even mowidespread with numerous research and studies on IOT. On the other hand, information on the objects and technologies being examined and evaluated under the IOT is still limited. For this reason the following table gives an idea of both past and future use of IoT objects.

Table 1: Classifying IoT Devices by Application

Wearables - Entertainment - Fitness - Smart watch - Location and tracking	**Health Care** - Remote monitoring - Ambulance telemetry - Drug tracking - Hospital asset tracking - Access control - Predictive maintenance
Building and Home Automation - Access control - Light and temperature control - Energy optimization - Predictive maintenance - Connected appliances	**Smart Manufacutring** - Flow optimization - Real-time inventory - Asset tracking - Employee safety - Predictive maintenance - Firmware updates

Smart Cities	**Automotive**
- Residential e-meters - Smart street lights - Pipeline leak detection - Traffic control - Surveillance cameras - Centralized and integrated system control	- Infotainment - Wire replacement - Telemetry - Predictive maintenance - Car to car, and car to infrastructure

Source: Weingber re g et al., 2015: 617.

As IoT related technologies and objects become more widespread in daily life, they inevitably create important consequences in the economy and society. Especially automation, integration and servitization are three main areas that need to be emphasized in this regard. These effects can be explained as follows (Lucero, 2016: 5):

- *Automation*: Making machines and sensors connected to computer systems rapidly accelerate the automation of process. In addition, it allows automation facilities to work with very large sets of data. Data flow monitoring, the use of these data to generate solutions in case of problems, and the possibility of minimizing maintenance services arise.
- *Integration*: The IoT expresses more than just interconnected machines or automation of processes. Integrating data from one device, object or machine, from other sources, such as data from ERP (Enterprise Resource Planning) systems, open government databases and social media feeds, greatly enhances the acquisition and value.
- *Servitization*: Automation and integration helps businesses move from product-oriented business models to service-oriented business models. In this way, it is possible to develop a service-oriented relationship with the customer and to capture the revenue opportunities that arise.

Apart from the above mentioned effects, the most important characteristic of the IoT idea is the strong role that it plays in everyday life, and its high impact on users' behavior. From the point of view of a private user, IoT effect will be experienced both at work and at home. Home automation, assisted living, electronic health and advanced learning are the likely future applications of this new paradigm (Atzori et al., 2010: 2787).

Although it is an emerging technology, it is estimated that it will grow at a great pace in the coming years. In the sectors such as automotive, energy, consumer electronics and white appliances, there are objects already working with computers and sensors. It will be easier and cheaper to integrate this technology with physical objects along with developing tools. In this regard, this technolgy will become widespread and adopted (Accenture, 2014). Columbus (2016), compiles some fundamental estimates for the IoT sector. As indicated in his article, by 2020 the annual revenues could surpass $470B for the IoT vendors selling the hardware, software and comprehensive solutions. Moreover, the total IoT market size in 2015 was up to $900M, and forecasted that it will grow to $3.7B in 2020 attaining a 32.6 CAGR (Compound Annual Growth Rate). Notwithstanding these, according to the estimates, IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025.

In spite of this rapid development, transformational processes will also pose several challenges to be overcome. In the context of IoT, these challenges include both technical and social issues.

Table 2: Technical and Social Issues in IoT Transformations

Techincal Issues	**Social Issues**
Technical Solution	User Acceptance
Communication	Privacy and Ethics
Energy	Education & Training
Interoperability	Governance
Security	Management Support
Device Management	Business Dynamics
Data Analytics	Stakeholder Management
E-Waste & Recycling Mangement	Partner Collaboration
	Teaming

Source: Cicibaş and Demir, 2016: 110.

Issues such as the solution of technical problems, the functioning of communication processes, the energy consumption of objects and mutual working are important technical issues to be considered for IoT. On the other side, issues such as the

internalization of these technologies by consumers, the training of users and the management of these technologies are social issues to be dealt within the framework of the IoT.

One of the most important topics which needs to be examined in this regard is privacy. When the benefits and losses are left aside, the data obtained through IOT is quite valuable. Thanks to the possibilities offered by IoT technologies, it is possible to obtain personalized data in a wide variety of quantities. The intended use of this data and the sharing of it with others may cause consumer concern. This, of course, results in more serious consequences. Consumer privacy is therefore an important issue to be addressed.

3. CONSUMER PRIVACY

Consumer privacy is an issue that arise in any interaction process between profit-oriented or non-profit businesses and the consumer. This interaction can be accomplished through credit card or cash sales, online consumer behavior and marketing research, but not limited to these. Behaviors that may be examined here may inclued all processes from purchase preferences to use and finally to dispose of products within the context of buying decision models (Goodwin, 1991: 150). Dolgun (2015: 265-266) emphasizes that businesses try to understand consumer and consumption patterns in the best way possible to create a consumer society that is loyal to the brand and product in a competitive environment. According to the author, creating this consumer society is about focusing on personalized services. However, personalization efforts, when evaluated in the context of surveillance, cause question marks to appear on topics such as the confidentiality of consumer information in the internet, whether the consumer's consent is recieved during the process of obtaining the information and whether the information can be considered in the privacy field or not.

Groopman and Etlinger's report about consumer privacy indicates some key findings (2015: 2):

- Consumers don't know who is seeing their data. Therefore most of consumers are higly concerned about whom and for what purpose their information is shared.
- At least half of the consumers state that they are overly disturbed about the use and sale of their personal data.
- Consumers want to have more information and involvement in privacy.
- Consumers demand a value in exchange for their data. This value is mainly monetary. Yet, it can also be in the form of time, energy and convenience.
- Technology is a very important indicator for notifications, service, communication and confidence-related expectations. Awareness on technology is shaping consumer expectations.

The model developed by Phelps et al. (2000: 31) regarding the scope of consumer privacy clearly demonstrates the dimensions of the issue. Type of personal information requested from the consumers, the possibility of control over the consumers' personal information, the possible consequences in terms of the businesses and the characteristics of the consumers, constitute the input factors for consumer privacy. Consumers' perceptions of the use practices of personal data and the general level of concern regarding the ways in which such information is used are, represented as the results. Taking these factors into consideration, the expected behaviroal tendencies of consumers are considered as future outcomes.

This model also reveals the importance of consumer privacy as well as its scope. Businesses' decisions and strategies on this subject have important consequences in both short and long term. In particular, the widespread use of information and communication technologies has made the issue even more prominent. As computers, the Internet and mobile devices are used more and more, the amount of personal data shared through these systems has also increased. Just like these technologies and devices, IoT will also increase the amount and variety of personal data which is shared and used.

According to FTC report, the amount of data that a few devices can produce is quite striking. Report says that less than 10,000 households using the IoT home automation product generate 150 million discrete data points per day, or about one data point in every six seconds per household (FTC, 2015). Since the data is extremely important, concerns about the privacy of individuals and their ability to control their own personal information also become prominent. Monitoring daily activities and generating informational outputs will increase the level of profiling and targeting. This leads further concerns regarding the privacy of personal data (Andersen and Rainie, 2014).

Peppet (2014: 98) examines the IoT technologies currently avaliable to consumer. Health and fitness sensors, black boxes in automobiles, home monitors and smart grid sensors, devices designed for employee monitoring, and software applications that use sensors in smartphones give the general outlook of the IoT technologies. Sicari et al. (2015: 151) indicates that, in addition to these, IoT offers a wide range of applications in areas such as remote monitoring of patients, control of energy consumpiton, traffic control, smart parking systems, inventory management, production chain, personalization of the

shopping and civil protection. In such an environment it becomes extremely important to protect personal information related to users' behavior, habits, and their interaction with other people.

4. THE RELATION BETWEEN IoT AND CONSUMER PRIVACY

Consumer privacy, especially with the widespread use of information and communication technologies, has also been the subject of academic work. The first studies on the subject contributed to the evlouation of privacy from the consumers' point of view (Goodwin, 1991; Jones, 1991). These have been followed by studies investigating the behavioral consequences of privacy concerns (Sheehan and Hoy, 1999; Phelps et al., 2001; Cho et al., 2009; Blakesley and Yallop, 2015), online consumer privacy (Miyazaki and Fernandez, 2001; Sheehan, 2002; Brown and Muchira, 2004; Moscardelli and Divine, 2007; Kansal, 2014;) and strategies to protect personal information (Lwin et al., 2007; Wirtz et al., 2007).

Recently, with the spread of IoT technologies, the number of studies emphasizing the importance of consumer privacy in the context of IoT has increased. Initial work on the issue by Weber (2010), examined the privacy and security problems that may arise with IoT from a legal perspective. Subsequent studies focus more on security and privacy issues that may arise with the widespread use of IoT technologies and objects have been conducted (Roman et al., 2013; Kumar and Patel, 2014; Lee and Lee, 2015; Sicari et al., 2015; Weinberg et al., 2015). In addition to these Peppet emphasizes the importance of consumer consent in the context of consumer privacy in IoT-related regulations. Weinberg et al. (2015) discussed the threats that the IoT presents to consumer privacy along with the benefits it provides. The subject also attracts attention from private sector and practitioners. Reports on the relationship between consumer privacy and IoT confirm this (Accenture, 2014; Groopman and Etlinger, 2015; FTC, 2015; Lucero, 2016).

As these studies and the focus of academic interest indicates the issue of privacy becomes substantial, especially in the consumer adaptation process of IOT. The functionality of the IoT technology for consumers is related to the interaction between the consumer and the devices. One of the most important part of this interaction is the personal information that the consumer share. Personal information is meaningful for the customization and improvement of the services offered. On the other hand, consumer's perceptions of the use of personal information also influences the acceptance of IOT technologies. These reveal the challanges to deal with.

One major obstacle standing in front of the proliferation of IoT objects in the real world is the security of the internet. There are billions of objects associated with the IoT. IoT developers are supposed to deal with the interaction of these objects with each other and also with other entities such as humans or virtual entities. It is crucial that all these interactions take place in a safe manner, and that actor's information is protected and the service provision is maintained. It is necessary to limit the number of incidents that IoT can affect on this account (Roman et al., 2013: 2270). Security risks trigger privacy risks mediated by IoT technologies for users. These risks include direct compilation of sensitive personal information such as geographical location, financial records or health information already existing due to traditional internet and mobile commerce. Nonetheless, information such as habits, places and physical conditions that are not collected directly but are generated over time through other sensitive information pose a risk. With regard to IoT, risks that are perceived by consumers and likely to cause harm are: Unauthorized access and misuse of personal information, attacks on other systems and risks to personal safety (FTC, 2015).

But the risks about consumer privacy is not limited to these. Internet, mobile devices and information technologies have created a very complicated environment. When this complex environment is combined with IoT systems, the interaction of people, machines and robots via internet can raise the level of security-related threats even higher. Moreover, the structure of existing security systems and applications does not conform to IoT technology. Also, as the number of connected devices increases, it will be also difficult to deal with these problems. The full acceptance of IoT applications by the user depends on the creation of security and privacy models (Sicari et al., 2015: 146).

According to a blog article, a company that sells smart teddy bears leaked 800,000 user accounts. After hackers stole this information, they demanded a ransom. These smart bears are internet-connected objects that allow children and far-away parents to send messages to each other. Through these objects, more than 800,000 customers' credentials as well as e-mail addresses and passwords and two million messages were recorded. A parent who heard about this incident expressed that his biggest concern was the possibility of someone using this information to send inappropriate messages to his 6 year old girl (www.motherboard.com). This incident which takes place through a very innocent object, is a good example of how these objects are threatening the privacy of personal information. IoT technology might also lead to unintented consequences. In order to avoid these consequences, both the designers of this technology and the users have to get responsibility.

Kumar and Patel (2014: 24-25) discuss some dimensions the issue of privacy might arise. At the dimension which named "privacy in device", they explain getting sensitive information through software or hardware without permission. A device can be used to manipulate personal data in this way. In addition, personal data may change hands as the communication

takes place. It is possible to get involved in communication processes through various technologies in order to steal information. Authors examine this problem under the hading of "privacy during communication". Saving data for storage may also cause privacy problems. For this reason, the amount of personal data they will be stored should be as limited as possible and this data should be shared only when necessary. These are about "privacy in storage". Lastly, they discuss the problem of what tehy call "privacy at processing".Here, the problem is mainly of two folds. First of all, personal data must be treated with the intented purpose. Secondly, without explicit consent and knowledge of user, personal data should not be disclosed or retained to third parties. Roman et al. (2013: 2271), indicate that the information created by billions of entities poses a great risk to privacy. It is important that the users are equipped with tools that will help them to maintain their privacy in such a world. With these tools and policies, the perception that IoT controls our lives silently should be avoided. This is only possible by ensuring trasparency, taking the users' consent and implementing policies that protect the user.

When considering consumer privacy in IoT from the businesses point of view, strategies that can be implemented and the precautions that can be taken are listed below (FTC, 2015):

- Companies should meet the security requirements for devices at the beginnig of the process, not later. It is important to conduct an assesment of privacy or security risks, to minimize the collection of data and to test the security measures of the products.
- Privacy and security should be issues that concern all employees of the company of appropriate level of responsibilty.
- Companies should work with service providers who can provide reasonable security system.
- When a significant risk is identified in company systems, a defense approach should be implemented that can enforce security measures at various levels.
- Companies should consider control measures to limit the ability of an unauthorized person to access the device, personal data or network of the consumer.

Finally, companies must continue to monitor products throughout the life cycle and correct security vulnerabilities.

5. CONCLUSION

Scholars are in search of answers to important questions regarding consumer privacy in IoT: What kinds of information are gathered by the devices and using what kind of tools? Where are the collected data stored? Is it in the memory of the device or in the cloud services that the manufacturer uses? Is that information encrypted and how? Does the manufacturer have the ability to redefine the information? Does the user have the authority to see, change or delete the information contained in the vendor's server? According to the manufacturer, who is the true owner of the data? With whom the producers will share users' data? Does the user have the authority to say something about sharing the data? These are basic questions that IoT consumers seek answers for. (Peppet, 2014: 161). IoT related stakeholders should be aware that these questions need to be addressed in order to make them widespread and adapt the consumers to these technologies. Lee and Lee (2015: 439), similarly addressed that while the IoT continues to gain momentum through smart home systems and wearable devices, confidence in and acceptance of the IoT will depend on the protection of users' privacy.

Trust is also a very important factor for this adaptation process. The IoT system encompasses a variety of devices. These should operate in accordance with users' needs and rights (Sicari et al, 2015: 147). Otherwise, consumers will have difficulty in adopting IoT technologies and applications. Moreover, it might also lead to of moving away from brands and products besides the system. It can also affect the image of existing products and services. Hereat, behavioral consequences can arise such as abandoning a brand, giving false personal data, refusing downloading applications, giving up visiting a website, complaning about brand and resorting to legal means against a company. It is extremely important for businesses to be aware of these behavioral consequences and to address the of privacy adequately.

Businesses that have to manage processes properly or consumers who need to be careful when using these technologies are not the sole responsible for IoT related issues. There are many stakeholders on the subject. These stakeholders should analyze the risks as well as the benefits of the IoT. Agencies, legislators and relevant institutions that mediate the transfer or personal data are some of these stakeholders. For this reason, the correct operation of the ecosystem which coexist with IoT, depends on the awareness of the responsibilities of such institutions and organizations and their willingness to overcome potential problems.

Along with these, some practices may be useful to deal with privacy related problems over IoT. Firstly, trainings can be organized on the management of personal data in order to increase the acceptance of technolgy by consumers. Further, studies can be conducted to improve the knowledge and awareness of consumers about privacy. These studies, which can

be evaluated in the context of consumer empowerment, can be realized by both academicians and practitioners. Additionally, messages and campaigns about the importance of personal data and ways of protecting it can be delivered bu using the internet and mass media.

As a conclusion, Justin Reich, one of the experts on Internet and Society, said, “IoT will have widespread beneficial effects, along with widespread negative effects. There will be conveniences and privacy violations. There will be new ways for people to connect, as well as new pathways towards isolation, misanthropy, and depression. I’m not sure that moving computers from people’s pockets (smartphones) to people’s hands or face will have the same level of impact that the smartphone has had, but things will trend in the similar direction. Everything that you love and hate about smartphones will be more so.” (Andersen and Rainie, 2014).

Future studies on the subject can focus on the adaptation of users to IoT technologies. Moreover, in this context, quantitative and qualitative methods can be used to investigate consumers' privacy concerns and possible behavioral consequences. Demographic and cultural differences can help achieve meaningful conclusions about both privacy concern and adaptation to IoT technologies.

REFERENCES

Accenture, 2014, "The Internet of Things: The Future of Consumer Adoption", https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf (2017, February 05).

Andersen, J., Rainie, L. 2014, "The Internet of Things Will Thrive by 2025", http://www.pewinternet.org/2014/05/14/internet-of-things/ (2017, February 05).

Atzori, L., Iera, A., Morabito, G. 2010, "The Internet of Things: A Survey", Computer Networks, vol. 54, pp. 2787-2805.

Blakesley, R. I., Yallop, C. A. 2015, "Consumer Perceptions About Digital Privacy and Online Data Sharing in the UK Insurance Sector, International Conference-Marketing From Information to Decision, 8th Edition.

Brown, M., Muchira, R. 2004, "Investigating the Relationship Between Internet Privacy Concerns and Online Purchase Behavior", Journal of Electronic Conmmerce Research, vol. 5, no. 1, pp. 62-70.

Cho, H., Rivera-Sanchez, M., Lim, S. S. 2009, "A Multinational Study on Online Privacy: Global Concerns and Local Responses", New Media & Society, vol. 11, no. 3, pp. 395-416.

Cicibaş, H., Demir, A. K., 2016, "Integrating the Internet of Things (IoT) into Enterprises: Socio-Technical Issues and Guidelines", Yönetim Bilişim Sistemleri Dergisi, vol. 1, no. 3, pp. 106-117.

Columbus, L., (2016, February 30). "Roundup of Internet of Things Forecasts and Market Estimates", Retrieved from https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#3177f8ba292d

Dolgun, U., 2015, "Şeffaf Hapishane Yahut Gözetim Toplumu", 3. Edition, Ötüken, Ankara.

Federal Trade Commission, "Internet of Things: Privacy & Security in a Connected World", https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (2017, February 06).

Goodwin, C. 1991, "Privacy: Recognition of a Consumer Right", Journal of Public Policy & Marketing, vol. 10, no. 1, pp. 149-166.

Groopman, J., Etlinger, S. 2015, "Consumer Perceptions of Privacy in the Internet of Things", Altimeter.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. 2013, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660.

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings. Retrieved March 03, 2017, from https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

Jones, G. M. 1991, "Privacy: A Significant Marketing Issue for the 1990s", Journal of Public Policiy & Marketing, vol. 10, no. 1, pp. 133-148.

Kansal, P. 2014, "Online Privacy Concerns and Consumer Reactions: Insights for Future Strategies", Journal of Indian Business Research, vol. 6, no. 3, pp. 190-212.

Kumar, J. S., Patel, D. R. 2014, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications, vol. 90, no. 11, pp. 20-26.

Lee, I., Lee, K. 2015, "The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises", Business Horizons, vol. 58, pp. 431-440.

Lucero, S. 2016, "IoT Platforms: Enabling the Internet of Things", IHS Technology Report.

Lwin, M., Wirtz, J., Williams, D. J. 2007, "Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective", Journal of the Academy of Marketing Science, no. 35, pp. 572-585.

Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I. 2012, "Internet of Things: Vision, Applications and Research Challenges", Ad Hoc Networks, vol. 10, pp. 1497-1516.

Miyazaki, D. A., Fernandez, A. 2001, "Consumer Perceptions of Privacy and Security Risks for Online Shopping", The Journal of Consumer Affairs, vol. 35, no. 1, pp. 27-44.

Moscardelli, M. D., Divine, R. 2007, "Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors", Family and Consumer Sciences Research Journal, vol. 35, no. 3, pp. 232-252.

Newman, P. (2017, Feburary 20), "The Internet of Things 2017 Report: How the IoT is improving lives to transform the world", Retrieved from http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1

Peppet, R. S. 2014, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", Texas Law Review, vol. 93, no. 85, pp. 85-176.

Phepls, J. D'Souza, G., Novak, G. 2001, "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation", Journal of Interactive Marketing, vol. 15, no. 4, pp. 2-17.

Roman, R., Zhou, J., Lopez, J. 2013, "On The Features and Challenges of Security and Privacy in Distributed Internet of Things", Computer Networks, vol. 57, pp. 2266-2279.

Sheehan, B. K. 2002, "Toward a Typology of Internet Users and Online Privacy Concerns", The Information Society, vol. 18, no. 1, pp. 21-32.

Sheehan, B. K., Hoy, G. M. 1999, "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy", Journal of Advertising, vol. 28, no. 3, pp. 37-51.

Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. 2015, "Security, Privacy and Trust in Internet of Things: The Road Ahead", Computer Networks, vol. 76, pp. 146-164.

Weber, H. R., 2010, "Internet of Things-New Security and Privacy Challenges", Computer Law & Security Review, vol. 26, pp. 23-30.

Weinberg, B. D., Milne, G. R., Andonova, Y. G., Hajjat, F. M. 2015, "Internet of Things: Convenience vs. Privacy and Secrecy", Business Horizons, vol. 58, pp. 615-624.

Wirtz, J., Lwin, O. M., Williams, D. J. 2007, "Causes and Consequences of Consumer Online Privacy Concern", International Journal of Service Industry Management, vol. 18, no. 4, pp. 326-348