The Internet of Things: The Disclosure Paradox

Brent Coetzee and Reinhardt A. Botha
School of Information and Communication Technology,
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

Abstract: Advances are continuously being made in core enabler technologies of the internet of things. The perceived value of the internet of things and its ability to change the way we live are heralded widely. However, information privacy remains an issue. The privacy concerns of potential consumers can hamper the adoption of the internet of things. Therefore, it is necessary to understand the extent to which the privacy concerns potential consumers have are affected by the benefits the internet of things provides. This research study measured respondent's privacy concerns before introducing them to potential internet of things applications. Thereafter, privacy concerns are again measured. Results before and after the exposure to an internet of things use case are compared using Wilcoxon signed-rank test. Results shows a significant decrease in privacy concerns relating to home and location privacy but are inconclusive regarding body sensors.

Key words: Internet of things, information privacy, privacy calculus, significant, understand, consumers

INTRODUCTION

The term "Internet of Things" (IoT) was coined by Ashton (2009) during his presentation linking Radio Frequency Identification (RFID) with the internet. The internet of things is generally viewed as a self-configuring wireless network of sensors whose purpose is to interconnect all things (Khoo, 2011) or as a pervasive presence around us comprised of a variety of objects or "Things" (Atzori *et al.*, 2010).

RFID chips are small transceivers used to identify and track objects they are embedded within. Together with Wireless Sensor Networks (WSN), RFID is a key enabler of the internet of things.

The importance of information privacy is evident within literature. Technology has a noticeable influence, as the boundaries of an individual's information privacy are often challenged by the progression and arrival of new technology. The rise of the World Wide Web (also referred to as Web 1.0) and the subsequent progression to social networking sites (Web 2.0) (Coetzee and Eksteen, 2011) with the addition of e-Commerce shape information privacy. The internet of things (Web 3.0) will no doubt have a large effect on information privacy literature.

Adopting the internet of things provides a host of benefits such as improved home security and health care. It is necessary to understand the relationship between information privacy concerns users have and the benefits

the internet of things provides. Privacy calculus refers to the comparison individuals make regarding the benefits and costs of disclosing their personal information. This study aims to use the current literature on information privacy together with the internet of things in order to predict how the two will affect each other. More specifically the primary goal of this study is to measure the extent to which the privacy concerns of potential consumers are affected by the benefits the internet of things provides.

The internet of things: The internet of things is still in its infancy. However, it is gaining awareness and support as it evolves. Google search results show that interest in the internet of things has out grown that of ubiquitous computing and Wireless Sensor Networks (WSN). Furthermore while technology is moving to accommodate the internet of things, the primary enablers are already widely used within industry (Cho *et al.*, 2007; Khoo, 2011).

Radio Frequency Identification (RFID): RFID fills the role of one of the major enabling technologies of the internet of things (Yun and Yuxin, 2010). RFID's primary objective is to act as a means to identify the target it is embedded within. Much like an Internet Protocol (IP) address, each device participating within the internet of things needs to have a unique identity. RFID is capable of sending more information than just its host's identity. Manufacturer

information, product code and type and most relevant to this study, current location (Feng and Fu, 2010). Unlike similar technologies such as barcode technology, RFID tags do not need to be in the line of sight of reading devices (Cho *et al.*, 2007).

RFID technology works with the concept of tags and readers (Want, 2006). Tags respond to readers that are within range. The tags do not need a power source as they use the energy provided by the reader in the form of electromagnetic waves which are used to respond to the reader (Gubbia *et al.*, 2013). The range between the RFID tag and reader can be increased by integrating a power source with the tag, depending on the application.

RFID allows any object to be identified, located and examined by integrating a RFID tag within the object. While such information is already passed around with current technology even at consumer level, explicit permissions are required from the user beforehand. Due to the very nature of the internet of things, information of RFID containing devices will be transmitted automatically as objects travel throughout the network (Feng and Fu, 2010).

Wireless sensor networks: Wireless Sensor Networks (WSN) are another key technology powering the internet of things. WSN fulfills the role of measuring and documenting environmental factors, often referred to as “Feeling” the environment (Yun and Yuxin, 2010).

A large number of sensing nodes are placed strategically throughout the environment and communicate wirelessly in a multi-hop fashion to a specific node within the environment. This specific node is called a sink and acts as the gateway for multiple nodes as only the sinks communicate with third party technologies (Cho *et al.*, 2007; Zhu *et al.*, 2010).

Current WSN architecture does not integrate well with RFID and the current internet IP backbone. Furthermore, due to the multi-hop nature of WSN, nodes closer to the sink node use more power than nodes further from the sink node. It is not economically justifiable to replace batteries on individual sensors. As a result, nodes around the sink become dormant and the WSN dies. Cho *et al.* (2007) presents a fully specific architecture called SARIF (Sensor and RFID integration framework) to integrate RFID and WSN technologies. New technology such as SARIF are paving the way for the internet of things. Once the internet of things is accepted into society, consumer will be carrying around technology such as SARIF everywhere they go. Together, RFID and WSN form the backbone of what powers the internet of

things. RFID identifies objects and provides key information about them while WSN describes the environment the objects are in.

Information privacy: Information privacy is the desire of individuals to have control over information about themselves (Belanger and Crossler, 2011). Privacy is an age old concern of which information privacy has seen an increase in academic works since the rise of the internet. Information privacy can be examined at four levels namely individual, group, organizational and societal (Smith, 2011). The internet of things will no doubt have an effect on all four levels, however, this study will focus on the individual’s information privacy concerns.

According to privacy calculus, individuals are willing to disclose personal information in exchange for benefits whether it be social or economic. These individuals weigh the benefits of disclosing personal information against the potential negative impact that disclosure could have on their information privacy. When asked to provide personal information to corporations, consumers would perform a risk-benefit analysis to assess the outcome they would face in return (Dinev and Hart, 2006). Culnan and Armstrong (1999) state that individuals performing a privacy calculus would be willing to disclose information if they are informed about a vendor’s information practices and perceive business as fair. Furthermore, Culnan and Bies (2003) suggest that individuals are more likely to disclose should they perceive the overall benefits to be at least balanced with if not greater than the assessed risk of disclosure.

While there is no arguing against the fact that individuals perform a sort of risk-benefit analysis before disclosing personal information, practice shows that privacy calculus is not the only factor that must be considered. What is known as the privacy paradox suggests that individual’s initial intentions towards disclosing personal information is not always a true representation of their disclosure behavior. Norberg *et al.* (2007) provide evidence of the privacy paradox by conducting two separate two-phase questionnaires. By asking respondents to state their intentions towards disclosing specific pieces of information and then several weeks later asking them to disclose that information, the authors show that actual disclosure significantly exceeded the intentions to disclose.

People’s stated intentions are not always reflective of their behavior because of factors that influence intention and behavior independently (Krasnova and Veltri, 2010). Perceived risk and trust are two such factors that have significant influence. Perceived risk has the most influence on behavioral intention whereas trust has most

influence on the decision of actual disclosure (Norberg *et al.*, 2007). Trust in the party the individual is disclosing information to grants them a feeling that they will receive the benefits associated with disclosing their personal information without any of the perceived costs that influenced their initial intentions to disclose (Krasnova and Veltri, 2010).

The certainty effect states that people attach less weight to outcomes that are merely a possibility in comparison to outcomes that are obtained with certainty (Kahneman and Tversky, 1979). When individuals are offered benefits in exchange for disclosing information they inadvertently place more priority on the positive outcome (the immediate gratification of the benefits) of disclosure than the negative (the possibility of the costs happening). This forms part of the prospect theory which is currently the most popular theory of decision under risk (Abdellaoui *et al.*, 2007). O'Donoghue and Rabin, (2000) aptly stated "we tend to pursue immediate gratification in a way we ourselves do not appreciate in the long run".

What about individuals who are aware of these shortcomings? Indeed, this behavior is not limited only to the naive. The illusion of validity suggests that one often predicts future outcomes based off of a single event (for example, the presentation of the benefits of disclosing information). The illusion persists even when said individual is aware of the factors that limit the accuracy of his or her predictions (Tversky and Kahneman, 1975).

Research objective: This study set out to determine whether the privacy concerns of potential consumers of internet of things are affected when confronted with the practical benefits the internet of things provides. Specifically, three types of potentially sensitive data were considered: home monitoring, location monitoring and wearing personal sensors. Three hypothesis were considered, each of the type (info = home, location and sensor):

- H_{info} : when faced with a specific use case where info is necessary consumers will be less concerned regarding privacy

To further test the effect of control, home surveillance was considered from a self-monitoring perspective ($H_{home-self}$) as well as from an external monitoring perspective ($H_{home-ext}$).

In other words, this study predicted that a consumer's concerns regarding privacy of home, location

and personal sensor data decreases when exposed to the benefits it provides consumers are thus more willing to share their personal information through the use of the internet of things technologies.

MATERIALS AND METHODS

The questionnaire consisted of questions related to the respondent's general privacy concerns by proposing the use of a specific technology prevalent in IoT implementations. Thereafter, the respondents are introduced to two use cases, based on a study entitled "Smart Community: an internet of things Application" by Li *et al.* (2011). The internet of things use cases were related to neighborhood watch and pervasive healthcare. They were selected based on the observation that both use cases could apply widely and thus represent a feasible application of the internet of things.

After each use case respondents were asked to rate the likelihood of them adopting the use case if available. These responses were then compared to the initial responses regarding the technologies.

The questionnaire was distributed as a Google Form to three different groups representing three different categories of internet users: internet gamers, internet forum users and social media users. Targeting distinct internet user categories was done to reduce bias. After all, the internet of things will affect most if not all, categories of internet users.

The choice of groups presents the risk that the respondents may interpret the questionnaire and use cases different and thus inadvertently affect the data. Since, the questionnaires were provided online to open forums "Internet trolls" also provided a threat to the integrity of the data. To combat this an identical but separate questionnaire was presented to each group, initially separating the results of one category from another.

However, for the final analysis of the results, all the data was combined to represent one population. The questionnaire was open to respondents for two months. During that time a total of 75 valid responses were documented.

RESULTS AND DISCUSSION

Data analysis and discussion: Since, the questionnaire collected ordinal data, non-parametric analyses were carried out. Given that the hypotheses were directional, one-tailed Wilcoxon signed rank tests for pairwise comparisons tested for significant differences between before-use-case and after-use-case ratings. All statistical

tests were performed with a significance value of 0.05. Analyses were carried out using SPSS V. 23. Consider each of the three categories of information in turn.

Home monitoring: Two hypotheses were tested. The first $H_{\text{home_self}}$ predicted that using internet of things technology to self-monitor your home would decrease concerns regarding home monitoring technologies. There was a significant increase from before-use-case (mean rank = 14.15) to after-use-case (mean rank = 29.44) in the predicted use of home monitoring technology ($Z = -5.078$; $p = 0.000 < 0.05$) and the increase was medium ($r = -0.41$). The second hypothesis, $H_{\text{home_ext}}$ predicted that using the internet of things technology to have your home monitored by an external party for the purpose of neighborhood safety would decrease concerns regarding home monitoring technologies.

There was a significant increase from before-use-case (mean rank = 21.50) to after-use-case (mean rank = 25.29) in the predicted use of home monitoring technology ($Z = -2.398$; $p = 0.016 < 0.05$) and the increase was small ($r = -0.195$).

In both cases a use case increased the use of specific technologies shown to possibly impact on the privacy of individuals. This indicated that the privacy concerns were deemed lower when faced with a specific use case. The two hypothesis were different in that they moved the locus of control from the individual to some external party using it for neighborhood surveillance. The effect size was significantly bigger when the locus of control was with the individual, indicating the role perceived control plays in the assessment of privacy risks.

Location information: The H_{location} hypothesis predicted consumers would be less concerned with providing location information when faced with an internet of things use case that requires location information.

There was a significant increase from before-use-case (mean rank = 19.50) to after-use-case (mean rank = 23.34) in the predicted use of home monitoring technology ($Z = -2.388$; $p = 0.017 < 0.05$) and the increase was small ($r = -0.195$).

As was the case with home monitoring it can be argued that when faced with a use case the perceived benefits may become more vivid in the mind's eye, thus leading to it outweighing the more distant risks more easily.

Body sensors: The H_{sensors} hypothesis predicted consumers would be less concerned with wearing sensors when faced with an internet of things use case that requires the wearing of sensors.

No significant difference could be observed ($Z = -1.554$; $p = 0.12$) causing us to not accept the hypothesis H_{sensors} .

Of the three scenarios wearing sensors can indeed be construed to be the "Most personal" of these scenarios as it touches the consumer's actual body. That those that find the general idea of such close monitoring invasive will keep finding it invasive regardless of the vividness of the advantages is not too surprising. The perceived benefits would also be influenced by one's current perception of their health. Someone who is in good health may not perceive the advantages to be as relevant as someone with a health condition.

CONCLUSION

The privacy paradox has shown that individuals disclose more information than their initial intentions would suggest. The results derived from this paper agree with the paradox as a significant decrease in privacy concerns was observed relating to home and location privacy. This can be explained by the fact that once the benefits of the said internet of things applications was emphasized, respondents naturally focused on the said advantages.

The results concerning the wearing of sensors is inconclusive. A possible explanation for this result is that those who found the idea of placing sensors on their person as too invasive may still feel that is the case. In other words, the perceived benefits in exchange for disclosure do not yet outweigh the perceived costs. It is also reasonable to conclude that the benefits of having sensors on one's person is hard to justify unless they are in particular need of medical supervision as depicted in the questionnaire.

Potential consumers may further indulge in the internet of things if businesses communicate how one's personal information will be gathered, used and stored effectively. Users of the IoT will be more willing to disclose information if they perceive a higher level of control over how and when their information is used in line with what (Culnan and Armstrong, 1999) stated.

This research highlights the ongoing struggle between the progression and innovation of technology and the ever sought after information privacy. Future research would do well to find the illusive balance between these two seemingly opposing forces.

REFERENCES

- Abdellaoui, M., H. Bleichrodt and C. Paraschiv, 2007. Loss aversion under prospect theory: A parameter-free measurement. *Manage. Sci.*, 53: 1659-1674.

- Ashton, K., 2009. That internet of things thing. *Rfid. J.*, 22: 97-114.
- Atzori, L., A. Iera and G. Morabito, 2010. The internet of things: A survey. *Comput. Netw.*, 54: 2787-2805.
- Belanger, F. and R.E. Crossler, 2011. Privacy in the digital age: A review of information privacy research in information systems. *Manage. Inform. Syst. Q.*, 35: 1017-1042.
- Cho, J., Y. Shim, T. Kwon, Y. Choi and S. Pack *et al.*, 2007. SARIF: A novel framework for integrating wireless sensor and RFID networks. *IEEE. Wireless Commun.*, 14: 50-56.
- Coetzee, L. and J. Eksteen, 2011. The Internet of Things-promise for the future? An introduction. *Proceedings of the Conference on IST-Africa*, May 11-13, 2011, IEEE, Africa, pp: 1-9.
- Culnan, M.J. and P.K. Armstrong, 1999. Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Org. Sci.*, 10: 104-115.
- Culnan, M.J. and R.J. Bies, 2003. Consumer privacy: Balancing economic and justice considerations. *J. Soc.*, 59: 323-342.
- Dinev, T. and P. Hart, 2006. An extended privacy calculus model for e-commerce transactions. *Inform. Syst. Res.*, 17: 61-80.
- Feng, H. and W. Fu, 2010. Study of recent development about privacy and security of the internet of things. *Proceedings of the 2010 International Conference on Web Information Systems and Mining (WISM)*, October 23-24, 2010, IEEE, New York, USA., pp: 91-95.
- Gubbia, J., R. Buyya, S. Marusic and M. Palaniswami, 2013. Internet of Things (IoT): A vision, architectural elements and future directions. *Future Generat. Comput. Syst.*, 29: 1645-1660.
- Kahneman, D. and A. Tversky, 1979. Prospect theory: An analysis of decision under risk. *Econometrica*, 47: 263-292.
- Khoo, B., 2011. RFID as an enabler of the internet of things: Issues of security and privacy. *Proceedings of the 2011 International Conference and 4th International Conference on Cyber, Physical and Social Computing Internet of Things (iThings/CPSCoM)*, October 19-22, 2011, IEEE, New York, USA., pp: 709-712.
- Krasnova, H. and N.F. Veltri, 2010. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences (HICSS)*, January 5-8, 2010, The Grand Hyatt Kauai Resort & Spa Honolulu, HI, USA, pp: 1-10.
- Li, X., R. Lu, X. Liang, X. Shen and J. Chen *et al.*, 2011. Smart community: An internet of things application. *IEEE. Commun. Mag.*, 49: 68-75.
- Norberg, P.A., D.R. Horne and D.A. Horne, 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *J. Consum. Affairs*, 41: 100-126.
- O'Donoghue, T. and M. Rabin, 2000. The economics of immediate gratification. *J. Behav. Decis. Making*, 13: 233-233.
- Smith, H.J., 2011. Information privacy research: An interdisciplinary review. *Manage. Inform. Syst. Q.*, 35: 989-1016.
- Tversky, A. and D. Kahneman, 1975. Judgment under Uncertainty: Heuristics and Biases. In: *Utility, Probability and Human Decision Making*, Wendt, D. and C. Vlek (Eds.). Springer, Netherlands, pp: 141-162.
- Want, R., 2006. An introduction to RFID technology. *IEEE Perv. Comput.*, 5: 25-33.
- Yun, M. and B. Yuxin, 2010. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. *Proceedings of the 2010 International Conference on Advances in Energy Engineering (ICAEE)*, June 19-20, 2010, IEEE, New York, USA., pp: 69-72.
- Zhu, Q., R. Wang, Q. Chen, Y. Liu and W. Qin, 2010. IoT gateway: Bridging wireless sensor networks into internet of things. *Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)*, December 11-13, 2010, IEEE, New York, USA., pp: 347-352.