Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions

Noura Aleisa and Karen Renaud
School of Computing Science, University of Glasgow, Glasgow, U.K.

Keywords: Internet of Things, Privacy.

Abstract: The Internet of Things (IoT) ability to monitor our every move raises many privacy concerns. This paper reports on a study to assess current awareness of privacy implications of IoT devices amongst Saudi Arabians. We found that even when users are aware of the potential for privacy invasion, their need for the convenience these devices afford leads them to discount this potential and to ignore any concerns they might initially have had. We then conclude by making some predictions about the direction the IoT field will take in the next 5-7 years, in terms of privacy invasion, protection and awareness.

1 INTRODUCTION

The term "Internet of Things" (IoT) refers to ubiquitous networking; where all things or objects are connected to each other via wired or wireless communication networks. The idea is that these "things" remove the need for humans to undertake deliberate repetitive actions. IoT devices, everyday objects such as kettles, lights and fridges are all connected and add a whole new dimension in terms of ease of access and control to device owners. The number of IoT devices has mushroomed and their presence in people's lives is now almost guaranteed, especially when one realises that the Smartphone is also an IoT device.

When the term "Internet of Things" was first coined by Kevin Ashton at Procter & Gamble in 1999 (Ashton, 2009) there were claims that it would revolutionise peoples' lives. IoT devices accumulate every personal data about our day to day lives. What they do with this data could easily constitute a violation of personal privacy (Fink et al., 2015; Ministry of Communication and Information Technology, 2010). The question is whether the 21st century citizen understands that this is happening.

The Saudi government is engaged in a programme of reform specifically to address network-connected devices and renewable energy (Nikkei Asian Review, 2016). This paves the way for many more IoT devices to enter the Saudi economy. A recent study by Accenture has shown that Saudi Arabia is ranked fifth among Arab states in terms of using technology, and on the 7th rank at the world level in term of mobile phone penetration in 2010. This is an opportunity to study a population who is newly entering the IoT market, to determine whether they understand the risks, and to explore their sensitivities.

We carried out a study with 236 Saudi Arabian participants and detected a relatively low level of privacy-awareness and concern,, although some were indeed concerned about privacy invasions. We conclude by making some predictions about the direction the IoT field might take in the next few years, in terms of privacy invasion, awareness and protection.

2 RELATED WORK

Warren and Brandeis defined privacy as the 'right to be let alone' (Warren and Brandeis, 1890). Currently, privacy is a sweeping concept, including freedom of thought, home isolation, control over personal information, freedom from surveillance, reputation protection, and protection from searches and investigation (Solove, 2008). Even with the increased collection of personal information by a number of public and commercial institutions, there is still an expectation of privacy. People believe that they can "control" their personal information by controlling who can access the information and deciding how the information will be used (Solove, 2008). In the new world of pervasive IoT this is not the case.

Aleisa, N. and Renaud, K.
Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions.
DOI: 10.5220/0006233701980205
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 198-205
ISBN: 978-989-758-245-5

The advent of the IoT requires us to reassess traditional definitions of privacy. Whereas traditional privacy entails people granting access, IoT devices often collect data without awareness, let alone permission. Such information can be very personal and sensitive, and such data can potentially reveal a great deal about us, without device owners even being aware thereof (Rouse, 2014).

IoT Privacy.

The IoT era has added new dimension of functionality and convenience to our lives. People can now unlock their doors, check the contents of their fridge, find a parking spot, make coffee, or turn up their house's heating before they even leave work[1].

Users permit companies, suppliers, and partners to access their data so that these devices can understand and satisfy their needs, often without any privacy guarantees (Guinard, 2015).

This means that outsiders could listen to what you're saying in your living room, gather information about what TV programmes you watch, and collect details about your personal daily routine. Before IoT, only your closest friends and family, those you trust, were privy to this information. Having IoT devices is the equivalent of replacing all your walls with glass, and sacrificing all your privacy.

As IoT emereged researchers argued for a global legal framework binding all IoT manufacturers to be established, given the potential durability of this new technical environment (Weber, 2010; Medaglia and Serbanati, 2010). Six years later this has not yet happened.

A study conducted by Slettemeås (Slettemeås, 2009) predicted a "Big Brother" public concern scenario surrounding RFID. With a network of millions of RFID readers and tags placed everywhere that constantly read, process and evaluate people's behaviours will create surveillance societies. Without encryption, RFID tags attached to items or people would respond to relevant readers without the holder's knowledge. People have no practical way to disable such tracking (Kelly and Erickson, 2005; Lee and Kim, 2006; Spiekermann and Berthold, 2005).

In addition, de Saint-Exupery (de Saint-Exupery, 2009) predicted that the more autonomous and intelligent IoT objects become, the more problems will arise related to the identity, privacy and responsibility of "things". He also raised concerns about the context of the information held across billions of "things" being updated in real time. Millions of transactions or data being interchanged across thousands of "things" with differing update policies opens up the potential for a range of privacy invasions.

Preuveneers and Berbers (Preuveneers and Berbers, 2008) presented a list of concerns related to information being stored locally or remotely in the future. They also raised concerns about information being retrieved from RFID tags and used by multiple parties on the network and being made available on a remote server for further analysis. Static and profiled information could be exploited, especially if historic values could be woven into the analysis in order to derive new information.

IoT Privacy Predictions.

We can summarize the privacy-related IoT predictions raised by the researchers as follows:

1. The personal data collected by smart devices (things) will be far in excess of what can be conceived and managed by the device owners.

2. Greater realisation of the potential for misuse of personal data will lead to demands for greater control of personal data collected by IoT things.

3. New regulation will force all IoT manufacturers to provide their consumers with the means to manage their recorded data that is transmitted by their smart device.

4. New regulation will also be required to force IoT manufacturers to **provide their consumers with detailed information** on how their personal data is being used, and who has access to it.

5. IoT-related cyber crime will continue to increase with the expansion of IoT as criminals branch out to exploit the potential of this new technological development.

6. The trade-off between convenience and privacy will swing towards sacrificing privacy for convenience, especially if effort is required to preserve privacy.

We will return to this list later to consider how many of these predictions have indeed materialised.

3 PRIVACY IN SAUDI ARABIA

We carried out this study with Saudi Arabians because they are newly entering the IoT market. As such, they are not yet used to the widespread invasion of privacy that seems to be accepted by so many countries where IoT devices have already become part of people's lives to the extent that they no longer think about the data they might be collecting. Studies of adoption of other online services have shown privacy to be one of the most important factors to Saudi Arabians (Al-Ghaith et al., 2010; Eid, 2011; Sait et al., 2004).

[1]It is difficult to separate privacy from security in the IoT domain, since a security failure often enables a privacy invasion; this means IoT security, and IoT cyber crime, is included in our privacy-related discussions

In the first place, do they know that IoT devices quietly and continuously accumulate their personal data? If they do know, are they also aware of the potential for privacy invasion?

If we inform people of these facts, what kinds of information would they be most concerned about, in terms of such data being collected and then shared with other parties? Moreover, how do they think this data ought to be protected, and what level of control would they, as device owners, like to have over their personal data?

Saudi Study.

We used a questionnaire, in both English and Arabic, to assess IoT-related privacy awareness of Saudi Arabians[2]. Completion took 10 - 15 minutes. The questionnaire was advertised to any smart device over 18 from the 20th of June to the 20th of July, 2016. 261 responses, and 250 refusals were collected. Sampling was snowball-based, advertised using social media tools such as Facebook, Twitter, WhatsApp, and email invitation.

For the validation process, first, we had an expert on questionnaire construction to check the questionnaire for common errors like double-barreled, confusing, ambiguous and leading questions. Secondly, we had two experts read through the questionnaire and three people with no technological expertise filled out the questionnaire while talking aloud. Finally, after collecting the data, we entered the responses into a spreadsheet and cleaned the data to present the final results (Collingridge, 2014).

RESULTS.

A total of 236 individuals responded to the questionnaire. The majority were aged 21 to 40 years (72.8%) and were either employees (68.19%) or students (20.3%). The percentage of female respondents was (67.43%), (31.8%) for male, and only (0.76%) did not provide gender. In terms of technological expertise, the majority rated themselves between 3 and 4 (74.31%), with 5 being the highest level.

Familiarity with IoT

The respondents were asked about their familiarity with the term 'Internet of Things' (IoT). The answers varied between being fully aware of this new technology to complete ignorance with 41 answers out of 100 not related to the definition of IoT. Participants used the following words to describe the IoT, "*connect objects to the Internet*", "*devices more smart*", "*make life easier*", "*Smart TV*", "*Simplicity*", "*Access to everything*", "*fast communication* ", "*convenience*", "*share data between all devices*", "*security and safety* ", "*remotely control devices*", ' '*minimal effort and less time*", "*gadgets, and smart devices*".

[2]http://ow.ly/WGRa306hg8Q

Respondents were asked if they owned a smart device (68%) or whether they were planning to acquire one (26% did not want to own one). Only one respondent mentioned a lack of privacy as a reason not to purchase a smart device.

When respondents were asked which criteria were important in informing their decision to buy a particular smart device. *Functionality* is paramount with a weighted average of 4.56. This was followed by *privacy and security* with a weighted average 4.3. The rest cited privacy as a critical aspect to be considered before making the decision to buy a smart device.

Privacy Concerns.

Respondents had different opinions about the kind of collected information that would most concern them. Figure 1 presents all weighted averages.

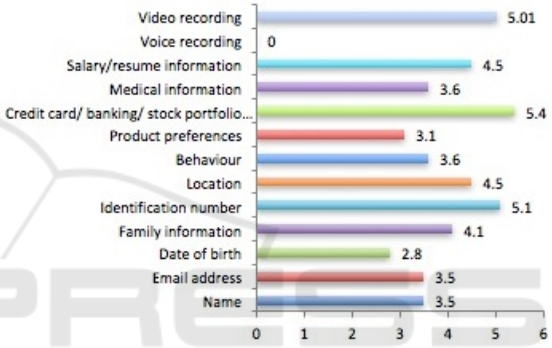

Figure 1: The most concerning types of information.

We provided respondents with three different scenarios to measure their willingness to share information in particular contexts. (Figure 2)

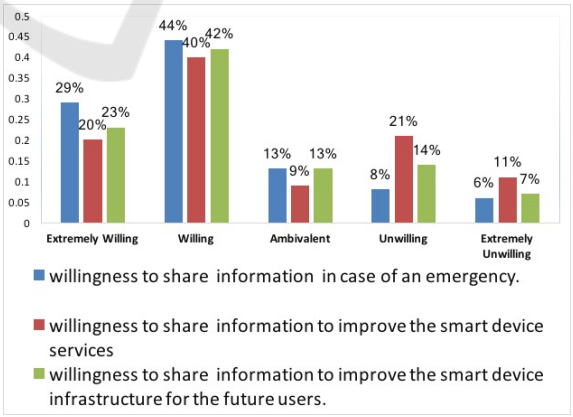

Figure 2: Willingness to share information.

Privacy Protection.

Questions explored how the respondents would like to protect their privacy. 86% were in interested what data is being collected before buying a smart device. Figure 3 presents the responses.

Humans have a fundamental need for control and certainty and a lack thereof constitutes suffering (Boff, 2012; Siegel, 2008) so giving the user the possibility of understanding when and why their data is being collected will make them less anxious.

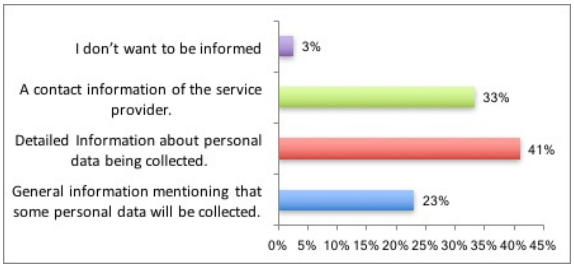

Figure 3: Data collected notifications.

Figure 4 shows how people want to be informed about data collection activities. The main problem with notifications is that users tend to drop their current task to check the notification instead (Iqbal and Horvitz, 2010). Too-frequent notifications can interrupt and frustrate. Yet people still think this is what they want (Shirazi et al., 2014).

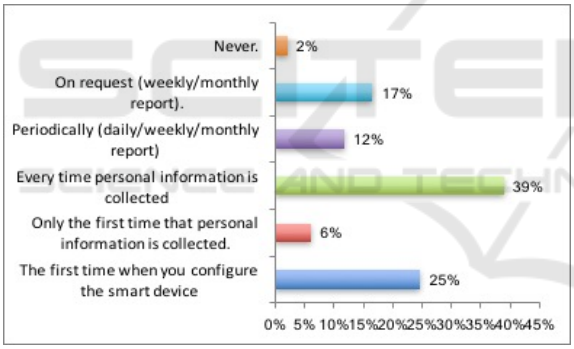

Figure 4: How often the users like to be informed that a smart device is collecting their information.

Analysis of the questionnaire answers demonstrated that the preferred notification method is to be alerted the first time a smart device starts collecting your personal information. The preferred mechanism is the short message service (SMS), second email or alarm on the device, finally the light display on the device.

The primary challenge of notification is preventing unwanted distraction to the primary task, while still delivering information in an accurate and timely manner. In some cases, a little distraction can be tolerated. In other cases, a user is willing to accept some distraction to receive valuable information presented in a timely fashion. To avoid annoying people, we believe a prior estimation of the user's prioritization should be achieved by tracking user attention priorities before setting up a notification schedule (McCrickard and Chewar, 2003).

The final question asked respondents to choose how they would want their personal information to be protected. Figure 5 depicts the responses.

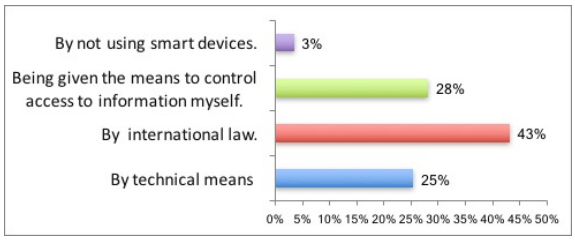

Figure 5: Data protections.

4 DID PREDICTIONS MATERIALISE?

We now reconsider each of the IoT privacy predictions in the light of our study and also recent IoT-related news and events. In particular, in order to assess the general public's perceptions, we looked for comments on one particular high profile story, the one about Samsung Smart TV recording audio in people's living rooms and transmitting it to unknown third parties for processing (Landau, 2015). We found two websites that had allowed people to comment[3]. On https://www.techdirt.com people responded to Samsung's eavesdropping with 91 comments. We also inspected comments on the British Guardian newspaper's website to the same story. There were 34 comments. These comments provide a snapshot, not an exhaustive survey of public opinion. Even so, they do provide insights into how people feel about devices that invade their privacy.

1. Lack of Awareness: The prediction was that the amount of data collected would be inconceivable. Only one of our respondents cited privacy as a reason for not purchasing an IoT device. When prompted with a list of criteria they would consider when buying a device, privacy and security were rated very highly. This suggests that privacy is important in general but that it is not at the forefront of their minds when they think about IoT devices.

A research project carried out by Norway's Consumer Council (NCC) in 2016 filed a formal complaint about a wristband that helped people to monitor their fitness. It collected data on asymmetrical and obscure terms, gathered too much data, did not say who

[3]Search undertaken on the 15th November 2016

had access to it and failed to say how long it would be retained (BBC, 2016). Some very intimate information collected by these devices was even revealed by a Google search (Rao, 2011). Public awareness of this seems low: people focus primarily on the functionality the device affords and do not seem to consider how it is being provided (Weinstein, 2015).

✓ Hence this prediction holds.

2. Greater Realisation of Potential for Misuse: Nothing our respondents told us suggested a realisation of the potential for misuse. In fact, it was only when we primed them with a list of criteria that included privacy did they even consider this aspect. The fact that voice recording did not bother them suggested that they were not aware of the Samsung Smart TV furore, nor could they conceive of this being misused.

Some comments on the Samsung story on https://www.techdirt.com suggested that the IoT potential for invasion of privacy was news to the commenters:

"Thinking about it, it seems anything that is smart needs to be avoided if you want a little bit of privacy these days..."

A few expressed outrage. One quote (with the heading related to George Orwell's book, 1984): *"The idea of the spyscreens was wild enough at the time. The ability to monitor all of them all the time would have been viewed as completely ludicrous. Turns out reality is even worse than fiction in this case"*

→ ✓ This prediction appears to be emerging but we are not observing any strong public outrage yet, suggesting only dawning realisation.

As we were finalising this paper a news story appeared which reported that a Chinese company had been harvesting text messages from Android phones and sending them to a server in China[4]. As more of these stories emerge we can expect the realisation amongst the general public to grow.

3. New Regulation to Force Full Disclosure before Purchase: 86% of our respondents wanted to know what data the smart device was going to collect about them *before* buying the device. Yet there is little evidence that this information is routinely provided. An international privacy study by Canada's federal Office of the Privacy Commissioner studied smart health equipment and found that about three-quarters of the users were not informed about how their collected information is stored and protected, while about half of the devices did not explain how the collected information could be deleted (Solomon, 2016).

Unlike the European Union, there are no specific laws for data protection and privacy in the Middle East. Saudi Arabia currently does not have a comprehensive data breach protection law in effect. However, there are several sources of law relevant to privacy. One of these laws rules that Internet Service Providers and telecommunications companies are prohibited from breaching any data carried by their public systems unless it is allowed by law. There are no relevant laws to force full disclosure before purchase(BakerHostetler, 2013).

✗ Since such regulation has not yet been implemented this prediction has not yet materialised.

4. Demands for Information about how Data is Handled: 28% of our respondents wanted to be able to exercise control over their own data. On https://www.techdirt.com someone explicitly calls for more information: *"They need to explicitly explain what's happening to all the data they're collecting."*

There is a caveat, though. It seems that when users are presented with the means to control their personal data, they, at some point, seem to become used to the devices and push that worry to the back of their minds. Over the years, Facebook has gone to great lengths to give users more control over their personal data. The irony is that few people actually exercise the control they have, perhaps because it is boring or complex (Hutchinson, 2015; Singer, 2015).

→ ✓ The prediction is weakly supported.

5. IoT-related Cyber Crime Increase: Earlier this year, anonymous hackers have targeted Saudi Arabia's Ministry of Defence website with a sustained distributed denial-of-service (DDoS) attack. Other targets were the Ministry of Finance, the Saudi Customs Service, the General Passports Service and the Saudi Ombudsman's Office. Such attacks work by flooding the target server with web traffic, usually stemming from a botnet, in order to overload it and force it offline for more than 24 hours. The attack was in revenge for execution of Nimr al-Nimr, a Shia leader (Cuthbertson, 2016).

A number of other attacks were reported in the month before this paper deadline. We mention only a few here (Pultarova, 2016; rt.com, 2016; Pauli, 2016). One high profile DDoS attack targeted the DNS service provider Dyn. It was a wake-up call for everyone, and an inconvenience for the people who are looking to access their favorite sites such as Amazon, Netflix, and Twitter. The attack was facilitated by compromised the Internet-connected DVRs, video cameras,

[4]http://www.kryptowire.com/adups_security_analysis.html

and other Internet of Things (IoT) devices, generating the largest DDoS attack the world has ever seen. (Roberts, 2016; Gleicher, 2016).

✓ This Prediction has Materialised.

6. Device Owners Sacrifice Privacy for Convenience: Our respondents considered functionality the most important factor when purchasing an IoT device. They said they considered privacy and security the second most important factor but the fact that 70% owned a device in the Saudi environment, which has so little legislation to protect them, suggests that in reality they are sacrificing their privacy in return for the convenience the device affords.

Given realistic scenarios, Saudi respondents traded privacy for the benefits gained from using the smart device, even if these benefits are relatively trivial (Figure 2).

Other reports confirm how cavalier people are with their privacy, even for small benefits (MacGregor, 2016; Connelly et al., 2007; Edwards, 2003; Turow et al., 2015; Hutchinson, 2015).

✓The prediction has materialised.

5 IOT PRIVACY PREDICTIONS FOR 2027

Predictions are based on an integration of knowledge and experience of IoT-related publications (Anthony, 2016; Compert, 2016; Kam, 2016; Markman, 2016; Khera, 2016; Nordrum, 2016), participants' opinions and the authors' reflections on their findings. A list of predictions and trends related to IoT privacy for 2027 are suggested here:

Tighter Regulation: Because of the visibility of recent IoT hacks, and the wide spread disruption they have caused, we predict that new regulations will be enacted to impose stricter rules pertaining to securing of IoT devices. As a reaction some prominent voices in the security arena are starting to call for regulation (Nextgov, 2016; Khera, 2016; Price, 2016; Schneier, 2016; Bracy, 2015). In the UK, where they are rolling out Smart Meters to all homes, and manufacturers had made all of these devices use the same encryption key. GCHQ, Britain's electronic intelligence agency, intervened to prevent this and to ensure that these devices were more adequately secured. This is a positive sign that government is starting to recognise the need to force manufacturers to behave more responsibly (Clark and Jones, 2016).

Full Disclosure: When people are given the opportunity to abandon their privacy in exchange for some benefit, the response is somewhat resigned, even accepting. This is especially so if they perceived a direct benefit of exchanging their data. However, when people are told that their personal data is being collected without their knowledge, the whole debate shifts. We are happy to give up our data, but only if we retain a sense of control. We do not like it being taken from us without our knowledge (Hutchinson, 2015; Singer, 2015).

We predict that international law will require all IoT manufacturers to provide detailed information to potential consumers about what data is recorded and transmitted by their smart device. There are already calls for Privacy-by-Design (Yu, 2016; Hospitality Technology, 2016).

More Privacy-Related IoT News: The news will report more privacy and security violations of IoT, thereby raising public awareness of the problem. This has already started to happen (Pultarova, 2016; rt.com, 2016; Pauli, 2016; Matyszczyk, 2015)

Rising Demand for IoT Security: IoT "things" will be secured more effectively. The more news stories about hacks appear, the greater the opportunity for security companies to offer services to consumers to secure their devices for them. Microsoft is already moving into this arena (Weinberger, 2016). Since security and privacy are so interwoven when it comes to IoT, the side effect of this move towards better security ought also to reduce the potential for privacy invasion.

Kinds of Solutions: Privacy- and security-preserving solutions will focus primarily on cryptographic methods but the consumers will not be asked to take deliberate action because they prioritise convenience over privacy protection.

6 CONCLUSION

As IoT spreads and permeates our daily lives, more privacy challenges will emerge. Manufacturers are currently sacrificing IoT owner privacy with impunity and they will never police themselves. It is time for consumers to start demanding better, and voting with their wallets and purses. Future research should focus on how to communicate these risks to John and Jane Citizen. Moreover, we need to find ways to encourage consumer participation in terms of demanding more information about the collecting and transmitting of their data and the data protection process the manufacturer of the device has put into place.

ACKNOWLEDGEMENT

We thank Lewis Mackenzie for his feedback on an earlier draft of this paper.

REFERENCES

Ministry of Communication and Information Technology (2010). Saudi Arabia ranks fifth globally in mobile phone growth rate. http://www.mcit.gov.sa/En/Communication/Pages/LocalNews/telnews_31_en.aspx.

Al-Ghaith, W., Sanzogni, L., and Sandhu, K. (2010). Factors influencing the adoption and usage of online services in Saudi Arabia. *EJISDC: The Electronic Journal on Information Systems in Developing Countries*, (40):1.

Anthony, R. (2016). Internet of Things: Is the Future Susceptible to Hacking? 13 November http://www.inquisitr.com/3712810/internet-of-things-is-the-future-susceptible-to-hacking/.

Ashton, K. (2009). That 'internet of things' thing. *RFiD Journal*, 22(7):97–114.

BakerHostetler (2013). Bakerhostetler's international compendium of data privacy laws. http://www.edrm.net/resources/data-privacy-protection/bakerhostetler-data-privacy-laws/saudi-arabia#7_Breach_Notification.

BBC (2016). Privacy complaint for fitness wristband makers. http://www.bbc.co.uk/news/technology-37859676.

Boff, L. (2012). Satisfying fundamental human needs). https://leonardoboff.wordpress.com/2012/12/23/satisfying-fundamental-human-needs/.

Bracy, J. (2015). Senate committee explores internet-of-things regulation. https://iapp.org/news/a/senate-committee-explores-internet-of-things-regulation/.

Clark, P. and Jones, S. (2016). GCHQ intervenes to secure smart meters against hackers. 18 March https://www.ft.com/content/ca2d7684-ed15-11e5-bb79-2303682345c8.

Collingridge, D. (2014). *Validating a Questionnaire*. SAGE Publishing. http://www.methodspace.com/validating-a-questionnair.

Compert, C. (2016). Football and a crystal ball: Data privacy predictions for 2016.

Connelly, K., Khalil, A., and Liu, Y. (2007). Do i do what i say?: Observed versus stated privacy preferences. In *IFIP Conference on Human-Computer Interaction*, pages 620–623. Springer.

Cuthbertson, A. (2016). Saudi Arabia: Government websites knocked offline by Anonymous hackers in revenge for executions. http://www.ibtimes.co.uk/saudi-arabia-kingdoms-websites-knocked-offline-by-anonymous-hackers-revenge-sheikh-nimr-1535961.

de Saint-Exupery, A. (2009). Internet of things, strategic research roadmap. http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf.

Edwards, L. (2003). Consumer privacy, on-line business and the internet: Looking for privacy in all the wrong places. *International Journal of Law and Information Technology*, 11(3):226–250.

Eid, M. I. (2011). Determinants of e-commerce customer satisfaction, trust, and loyalty in Saudi Arabia. *Journal of electronic commerce research*, 12(1):78.

Fink, G. A., Zarzhitsky, D. V., Carroll, T. E., and Farquhar, E. D. (2015). Security and privacy grand challenges for the internet of things. In *Collaboration Technologies and Systems (CTS), 2015 International Conference on*, pages 27–34.

Gleicher, N. (2016). The Big Lesson We Must Learn From The Dyn DDoS Attack. http://www.darkreading.com/endpoint/the-big-lesson-we-must-learn-from-the-dyn-ddos-attack/a/d-id/1327432.

Guinard, D. (2015). Internet of things: businesses must overcome data and privacy hurdles. https://www.theguardian.com/media-network/2015/jun/01/internet-of-things-businesses-data-privacy.

Hospitality Technology (2016). Security Must Be Built into the Design of IoT Devices . 28 October http://hospitalitytechnology.edgl.com/news/Security-Must-Be-Built-into-the-Design-of-IoT-Devices-107556.

Hutchinson, A. (2015). Convenience vs privacy: The latest study in the data tracking debate. http://www.socialmediatoday.com/technology-data/adhutchinson/2015-06-05/convenience-vs-privacy-latest-study-data-tracking-debate.

Iqbal, S. T. and Horvitz, E. (2010). Notifications and awareness: A field study of alert usage and preferences. In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, CSCW '10, pages 27–30. ACM.

Kam, R. (2016). Top predictions for 2016: Privacy and security. http://www.healthcareitnews.com/blog/top-predictions-2016-privacy-and-security.

Kelly, E. P. and Erickson, G. S. (2005). RFID tags: commercial applications v. privacy rights. *Industrial Management & Data Systems*, 105(6):703 – 713.

Khera, M. (2016). Are regulations the answer to better Internet of Things security? 10 November https://www.cyberscoop.com/iot-security-op-ed-dyn-ddos-mandeep-khara/.

Landau, S. (2015). What Was Samsung Thinking? *IEEE Security & Privacy*, (3):3–4.

Lee, H. and Kim, J. (2006). Privacy threats and issues in mobile rfid. In *First International Conference on Availability, Reliability and Security (ARES'06)*, pages 5–pp. IEEE.

MacGregor, A. (2016). Telco CEO: Consumers have double standards over data privacy. 9 November https://thestack.com/big-data/2016/11/09/thorsten-dirks-telefonica-deutschland-double-standards-data-privacy/.

Markman, J. (2016). Massive IoT Hacks Should Lead To Positive Change. 10 November http://www.forbes.com/sites/jonmarkman/2016/11/10/massive-iot-hacks-should-lead-to-positive-change/.

Matyszczyk, C. (2015). Samsung's warning: Our Smart TVs record your living room chatter. http://www.cnet.com/uk/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/.

McCrickard, D. S. and Chewar, C. M. (2003). Attuning notification design to user goals and attention costs. *Commun. ACM*, 46(3):67–72.

Medaglia, C. M. and Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer.

Nextgov (2016). Who'S in change of regulating the Internet of Things? 1 Sept http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/.

Nikkei Asian Review (2016). Japan, Saudi Arabia to cooperate on Internet of Things, renewables. http://asia.nikkei.com/Politics-Economy/International-Relations/Japan-Saudi-Arabia-to-cooperate-on-Internet -of-Things-renewables.

Nordrum, A. (2016). Wanted: Smart Public Policy for Internet of Things Security. 10 November http://spectrum.ieee.org/tech-talk/telecom/security/wanted-smart-public-policy-for-internet-of-things-security).

Pauli, D. (2016). IoT worm can hack Philips Hue lightbulbs, spread across cities. 10 November http://www.theregister.co.uk/2016/11/10/iot_worm_can_hack_philips_hue_lightbulbs_spread_across_cities/.

Preuveneers, D. and Berbers, Y. (2008). Internet of things: A context-awareness perspective. *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*, pages 287–307.

Price, R. (2016). The government needs to step in and save the internet from hacked toasters. 25 October http://www.businessinsider.com/dyn-hack-calls-grow-regulation-internet-of-things-security-mikko-hypponen-f-secure-interview-2016-10.

Pultarova, T. (2016). Webcam hack shows vulnerability of connected devices. 11 November https://eandt.theiet.org/content/articles/2016/11/webcam-hack-shows-vulnerability-of-connected-devices/.

Rao, L. (2011). Sexual Activity Tracked By Fitbit Shows Up In Google Search Results. 3 July https://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/.

Roberts, J. J. (2016). Who to blame for the attack on the internet. http://fortune.com/2016/10/23/internet-attack-perpetrator/.

Rouse, M. (2014). Internet of Things privacy (IoT privacy). http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-privacy-IoT-privacy.

rt.com (2016). Smart fridge browses porn in us store, shows hot action while keeping its cool. 3 October https://www.rt.com/viral/361440-iot-fridge-shows-porn/.

Sait, S., Al-Tawil, K., and Hussain, S. (2004). E-commerce in Saudi Arabia: Adoption and perspectives. *Australasian Journal of Information Systems*, 12(1).

Schneier, B. (2016). Regulation of the Internet of Things. November https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html.

Shirazi, A., Henze, N., Dingler, T., Pielot, M., Weber, D., and Schmidt, A. (2014). Large-scale assessment of mobile notifications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 3055–3064. ACM.

Siegel, D. (2008). The need for a sense of control).

Singer, N. (2015). Sharing data, but not happily. http://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html.

Slettemeås, D. (2009). RFID—the "Next Step" in Consumer–Product Relations or Orwellian Nightmare? Challenges for Research and Policy. *Journal of Consumer Policy*, 32(3):219–244.

Solomon, H. (2016). Most makers of IoT devices still dont explain how personal info is used: Report. http://www.itworldcanada.com/article/most-makers-of-iot-devices-still-dont-explain-how-personal-info-is-used-report/386650.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Spiekermann, S. and Berthold, O. (2005). Maintaining privacy in RFID enabled environments. In *Privacy, Security and Trust within the Context of Pervasive Computing*, pages 137–146. Springer.

Turow, J., Hennessy, M., and Draper, N. A. (2015). The tradeoff fallacy: How marketers are misrepresenting american consumers and opening them up to exploitation. *Available at SSRN*.

Warren, S. D. and Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, pages 193–220.

Weber, R. H. (2010). Internet of things–new security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30.

Weinberger, M. (2016). This is how Microsoft is preventing hackers from hijacking IoT devices. 26 October http://www.businessinsider.com/microsoft-azure-iot-security-program-2016-10.

Weinstein, M. (2015). What your FitBit doesn't want you to know.

Yu, E. (2016). Asia must adopt 'data protection by design' in IoT era. 10 November http://www.businessinsider.com/microsoft-azure-iot-security-program-2016-10.