Jonathan Lowe

jl4ge

9/13/2017

STS4600

Thesis Chunk One

DISCLAMER:

This is a terrible first draft

***Abstract – Later maybe if warranted***

***Introduction***

***Problem frame/background:*** The term “the internet of things”, commonly referred to as IoT, refers to embedded computers connected to the internet. IoT devices range from thermostats and fitness trackers to cars. This emerging technology, which was made possible by the expansion of the internet, has the potential to change our daily lives.

IoT devices will be widespread and produce a huge amount of information. If the current trend holds, there will be about 50 billion devices connected to the internet by the year 2020 (Federal Trade Commission, 2015). An average of 150 million points of data is made a day from all of the devices produced by a relatively small IoT company (Federal Trade Commission, 2015). They will collect huge amounts of possibly extremely personal consumer data, such as sensitive health information, driving habits, and whether or not you are at home (Federal Trade Commission, 2015).

The collection and retention of data collected by IoT systems presents privacy risks that did not previously exist. Privacy in this case means the right of individuals to a certain amount of control over the flow of personal information about themselves. Examples of information that falls under this definition of personal privacy include information about one’s health, voting history, academic records, and other such information. IoT privacy risks firstly include corporate misuse. Corporate misuse of consumer data consists of unlawful or inappropriate use of consumer data such as releasing data without their customer’s consent or using it in unlawful ways. An example of corporate misuse is that Uber executives at one point could view all of the positions of their drivers and riders on a map using a “God View” mode (Frizell, 2014). Users of the Uber app don’t expect or necessarily want that Uber executives would be able to see their location on a whim.

Another privacy risk is hackers gaining access to insecure devices. Security standards are either fragmented or not present at some IoT manufacturing companies and some IoT devices have no security measures built into them (Chen, 2017). Thus, many IoT devices present little to no obstacles to hacking. In the recent past, there has been several incidents of hackers breaking into IoT devices in the news.

Also, the potential for governments having access to all the data you ever have produced is another privacy risk. Surveillance programs in the US have been present since the 1930 (Elkin-Korerd & Haber, 2016). All the new information generated by IoT devices will only increase the amount of information that governments can collect about citizens. Around the turn of the century, the FBI developed a system for collecting emails, instant messages, and other internet activities (Donahue, 2006). The government has the ability to build tools that monitor IoT systems. All this begs the question: How should the data produced by IoT systems affect personal privacy?

***Claim about the problem:*** The widespread use of IoT devices will make corporations effectively own a large amount of their users’ personal information, which the corporations could easily misuse or put their users’ personal privacy at risk without significant legal ramifications. ***How I will support the claim:*** Once corporations collect information from IoT devices about their users, they will pretty much have exclusive legal control it. The data collected by IoT devices though maybe not apparently sensitive can be used to infer private information and thus give corporations significant control over their users’ privacy. Technology companies that store data collected from their users have historically misused the data collected about their users and IoT device makers will likely behave similarly.

To explore this question, I will use contextual integrity to analyze the situation. Contextual Integrity is a theory which states that different social contexts have different norms about how information should be shared. Whenever one of these norms is violated or information is revealed in the wrong context, a person’s privacy has been violated. ***TODO – Maybe add more details about it and maybe integrate/relate it to previous paragraph***

***Supporting Argument 1***

***Section claim:*** Once corporations collect information from IoT devices about their users, they will pretty much exclusively control it.

***TODO – Flesh out***

***Supporting Argument 2***

***Section claim:*** The data collected by IoT devices though maybe not apparently sensitive can be used to infer private information and thus give corporations significant control over their users’ privacy. Data mining is the process of taking large amounts of data and analyzing it to find patterns or relationships that exists between members of a certain data points (Keating, 2008). Companies are already using data mining to find out the interests of their consumers given different circumstances. When a hurricane is approaching, Walmart found that sales of beer increase (Keating, 2008).

Data mining has been used to infer private information. The retailer Target has a sophisticated model for predicting how much money a person will likely spend on different items (Corrigan, Craciun, & Powell, 2014). It has proven to be pretty accurate for at least a few types of applications. One way that they used data mining is predicting when a woman is pregnant. Target researchers found that pre-natal mothers usually bought certain items regularly and came up with a scoring system to predict the likelihood of a woman being pregnant (Corrigan, Craciun, & Powell, 2014). This is at least slightly disturbing. Many people don’t think about what information they give out by their purchacing decisions.

IoT devices present a huge amount of new information that can be analyzed using data mining and thus give companies more control of their customers privacy. The data from a IoT lighting system could be used to tell when people get home from work, when they go to bed, and when they get up in the morning. Smart fridges that detect what food items you regularly eat could potentially tell how much you likely weigh, whether or not you are lactose intolerant, whether or not you have diabetes, or if you have heart problems by the you eat. Since companies would store and have access to this information they would have a lot of control of their customers’ privacy.

***Supporting Argument 3***

***Section claim:*** Technology companies that store data collected from their users have historically misused and insufficiently protected the data collected about their users and IoT device makers will likely behave similarly.

***TODO – Flesh out***

***Conclusion – Not yet reached…***

***TODO – Finish other parts of the paper and make recommendations***

***References – So Far***

Chen, L. (2017). *Security Management for The Internet of Things* (M.A.Sc.). University of Windsor (Canada), Canada. Retrieved from <https://search.proquest.com/docview/1886841984/abstract/1DF89E7F2A5B4581PQ/2>

Corrigan, H. B., Craciun, G., & Powell, A. M. (2014). How Does Target Know So Much About Its Customers? Utilizing Customer Analytics to Make Marketing Decisions. *Marketing Education Review*, *24*(2), 159–166. <https://doi.org/10.2753/MER1052-8008240206>

Donahue, L. K. (2006). Anglo-American Privacy and Surveillance. *Journal of Criminal Law & Criminology*, *96*(3), 1059–1208.

Elkin-Korerd, N., & Haber, E. (2016). Governance by Proxy. *Brooklyn Law Review*, *82*(1), 105–162.

Federal Trade Commission. (2015). *Internet of Things: Privacy & Security in a Connected World.* Staff Report. Retrieved from <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>

Frizell, S. (2014). What Is Uber Really Doing With Your Data? *Time.Com*, N.PAG.

***TODO – When the full article arrives, make sure that the citation is formatted correctly!!!***

Keating, B. (2008). The Journal of Business Forecasting; Flushing 27.3: 33-35.