Jonathan Lowe

jl4ge

10/8/2017

STS4600

Full 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, ZAhas 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 present privacy risks that did not previously exist. ***TODO – DISCUSS PRIVACY IN MORE DETAIL*** 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 the 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 have 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 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 effectively 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. 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. If you share personal information about yourself, like severe health problems, to a friend, you would not expect them to share that with others. If they did share such personal details, without appropriate reasons, it would violate the social norm of keeping private information about one’s friends secret. Another example is when you go to a medical professional. They are expected to not disclose your medical history; this social norm is enforced by law.

Contextual Integrity will act as a framework for analyzing privacy for IoT systems. I will use it to highlight that IoT systems mostly lack social norms sharing data and will likely be used in ways data is used in other related industries. I will also show that related industries lack sufficient legal protection for consumers when contextual integrity is violated. I will also cover how related industries can violate contextual integrity in new ways using data mining.

***Supporting Argument 1***

***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 exist between members of a certain data points (Keating, 2008). Companies are already using data mining to find out the interests of their consumer's 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 et al., 2014). This is at least slightly disturbing. Many people don’t think about what information they give out by their purchasing 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 customer's privacy. The data from an 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 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 2***

***Section claim:*** Once corporations collect information from IoT devices about their users, they will effectively have exclusive control it. The control that companies have over the data collected about their customers includes the right to sell it, mining it for more information, and releasing it to governments and other third parties. This allows companies to release information inappropriate contexts and thus violate contextual integrity. As it stands now, companies in different and related industries can effectively do whatever they want with the data they collect about customers.

Search engines are an example of companies that collect information about their users and effectively have exclusive control that information. Not too long ago, Aol released search results to the public that were organized by user ID and people were identifiable from the results (Barbaro & Zeller, 2006). This violated contextual integrity because the information about their user’s search history is expected to be kept only by the search engine. Aol did not face legal consequences for this release and any attempt to peruse such action would probably fail. According to James Grimmelmann a law professor at Cornell Tech and Cornell Law School, once search engines collect information about you they can do practically anything they want without significant legal ramifications (Grimmelmann 2007). It may not even be a significant legal risk for a search engine to use their user’s data in a way that is against their own privacy policy (Grimmelmann 2007). This effectively allows search engines to violate the contexts that they themselves have defined in their privacy policy without any ramifications.

Other companies like data brokers collect, buy, and sell personal information legally. Data brokers are companies that collect information on consumers, mine it for additional information, and sell it. Data broker companies typically are not very widely known; Acxiom and Datalogix are two of them. Their customer range from antivirus companies to political campaigns (Rostow, 2017). In a 2014 Federal Trade Commission report, the data brokers that were studied gather information from publicly available sources, such as government records and social media, as well as commercial sources; none of them collected information directly from people (Federal Trade Commission, 2014). The data that data brokers collect while validly used in their original contexts, like publicly available records and information collected about costumers by companies for their internal use, it is not necessarily appropriate in this new context. Data brokers sell information for different purposes including marketing, risk mitigation, and people search without hardly ever interacting with the people they collect information about (Federal Trade Commission, 2014). Thus, most people don’t see that information about themselves is being bought and sold, which raises questions about whether or not it is appropriate for companies to share information in this new context.

Buying and selling information about consumers is perfectly legal. With a few exceptions, there are no laws regulating the data broker industry United States on the federal level (Rostow, 2017). Even on the state level, there has been little done to regulate the data broker industry (Rostow, 2017). This highlights the fact that if these companies violate the contextual integrity of consumer’s data, they will likely not face any legal repercussions. Given the amount and value of the data produced by IoT systems, it is likely that data brokers will want to get a hold of IoT data either by buying it or acquiring IoT device manufacturers. Also, IoT service providers will be tempted by the amount they can pad their profit margins. This would give them a new source of data that was previously unavailable and new opportunities to violate the contextual integrity of their users’ data.

Since existing companies, which bear a striking resemblance to IoT service providers, have control over consumer data, IoT service providers will likely have the same control over data produced by their customers and appropriate the social norms of sharing consumer data. All this information might seem like I am arguing that companies shouldn’t have control over consumer data; shouldn’t companies be able to use information about their customers to improve their services, effectively market to their customers, and come up with new products? Yes, companies should have control over their consumer's data, but they should not sell, release it to third parties, or reveal it in inappropriate social contexts a without their customer’s knowledge or consent.

***Supporting Argument 3***

***Section claim:*** 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. Such misuse involves releasing personal information about their costumer’s in appropriate contexts without the costumers’ knowledge or consent and using it inappropriately. While even the most robustly developed software ends up having security vulnerabilities, companies have exposed their user’s data to hackers by not sufficiently building in sufficient security measures into their products, thus allowing unauthorized third parties to access and release information in inappropriate contexts.

Companies have released have released personal data without their users’ knowledge or consent to different parties. PRISM was a secret government program by which the FBI obtained information on people directly from IT companies (Gellman & Poitras, 2013). Companies like Yahoo, Google, and AOL have participated in the FBI’s surveillance program (Gellman & Poitras, 2013). This was an edge case of where contextual integrity was violated. Law enforcement should have access to private information in criminal investigations even without the person they are investigating’s knowledge or consent, but there should be some restrictions on that power. For example, it is the current norm that police should have a warrant before obtaining information from someone’s private email account. Some other examples include firstly the time when Aol released search results to the public, while not apparently identifiable, but ended up being so (Barbaro & Zeller, 2006). Another is when Wells Fargo recently and inadvertently gave sensitive information on their wealthiest clients to a third party, who could have easily released it to the public (Kovaleski & Cowley, 2017). InfoUSA sold the information on elderly people which ended up being used by criminals to steal their life’s savings (Duhigg, 2007). These incidents show that companies giving out information that they should not is not an isolated rare occurrence, but it happens somewhat regularly.

Companies in the past have insufficiently secured their customer’s data, thus inadvertently providing third parties access sensitive information. From May through July, a credit reporting agency called Equifax had a massive security breach in which hackers stole the names, social security numbers, birth dates, addresses of U.S. customers (“Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes,” 2017). Initial estimates stated that 143 million Americans were affected by this breach (“Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes,” 2017). The scale of this breach is concerning to say the least. According to their website, the security team was aware of the security vulnerability when it was disclosed by Apache Struts and were taking measures to secure their vulnerable systems (“Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes,” 2017). This seams a little bit implausible. Apache announced this vulnerability on March 7, 2017 and released a patch for it the same day (“MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® StrutsTM Exploit : The Apache Software Foundation Blog,” n.d.). Equifax had two months to secure their applications, but they only patched their applications after they discovered the method of attack (“Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes,” 2017). If Equifax prioritized protecting consumer data, they would have patched their web applications sooner. This incident shows a limitation of contextual integrity. Contextual integrity does not cover the responsibilities of persons to ensure that the information that they have is not taken by other parties as Equifax has here. Contextual integrity would do well to add some expectations of how securely the parties involved should keep data secret.

In its relatively short life so far IoT companies have already left customer’s data at risk by insecurely storing and communicating it. A few years ago, TRENDnet, Inc. marketed and sold baby monitors, which are IoT devices, that were not so secure (Riga, 2017). When the baby cameras were hacked in 2012, the footage was posted on the internet and an investigation was launched that found that login information was not encrypted when it was being transmitted and thus capable of being read by attackers (Riga, 2017). This situation is likely to continue. According to a report by the Federal Trade Commission, IoT faces unique security challenges including new IoT companies lacking security experience, the inability to update device software, and the lack of willingness of companies to secure and fix low cost low profit margin devices (Federal Trade Commission, 2015). This situation will allow many more third parties, in this case hackers, to access and disseminate information outside of their proper social norms than if more effort was put into security.

Since existing technology and large companies have historically misused and insufficiently protected their customer’s data, IoT companies will likely do the same. All of this evidence might suggest that companies can’t be trusted with consumer data; aren’t there companies that are trustworthy? Yes, there are many companies that have taken adequate measures to protect their customer’s data and don’t misuse it, but there have been several notable instances where the information released is damaging. So, there should be some legally binding expectations about how they will use it and protect it.

***Conclusion***

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. Corporations can gain access to more personal information about their users’ than what they explicitly given them by using data mining. If the data that IoT companies collect is misused, the users that produced that information will have little to no legal recourse. In the past, companies abused consumer data, such as insecurely storing it, and this will likely continue.

This new technology now currently lacks existing social norms for the flow of personal information. In many cases it will likely borrow contexts from existing ones: biometric information will likely borrow contexts from existing medical practices and the like. In some cases, this will be adequate, but many are not, examples of which are above. Therefore, new informational sharing norms should be formed. Companies should be able to collect and mine data on their customers so that they can improve their services, but they should be limited in what that can do with it. For example, companies should not be able to sell or release it on a whim. Corporations should also have the explicit legal responsibility to protect their consumer data from malicious hackers.

This paper has some limitations and future directions its research can take. For one, I did not look at case or tort law for privacy. There could have been additional factors I did not consider. I could have used other STS frameworks such as AND or SCOTT, that could have been better perspectives on the topic. Future research that can be done on the topic includes looking at existing legal principles on privacy or framing the problem in ANT to get a better perspective on the parties involved.

***References – So Far***

Barbaro, M & Zeller, T. (2006, August 9) A face is exposed for AOL searcher no. 4417749. *New*

*York Times.* Retrieved from http://www.nytimes.com/

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. [ht tps://doi.org/10.2753/MER1052-8008240206](https://doi.org/10.2753/MER1052-8008240206)

Duhigg, C. (2007, May 21). Firms sell elderly Americans’ data to telemarketing con artists. *The New York Times*. Retrieved from <https://www.nytimes.com/2007/05/21/world/americas/21iht-data.1.5803543.html>

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.

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes. (2017, September 15). Retrieved October 9, 2017, from <https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/>

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>

Federal Trade Commission (2014). *Data Brokers: A Call for Transparency and Accountability*. Washington, District of Columbia: Federal Trade Commission.

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

Gellman, B. & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S.

Internet companies in broad secret program. *The Washington Post.* Retrieved from

<https://www.washingtonpost.com/>

Grimmelmann, J. (2007). *The Structure of Search Engine Law.* *Iowa Law Review*, *93*, 1–64.

Keating, B. (2008). Data Mining: What Is It and How Is It Used?. *Journal of Business*

*Forecasting*, 27(3), 33 - 35.

Kovaleski, S. F., & Cowley, S. (2017, July 21). Wells Fargo Accidentally Releases Trove of Data on Wealthy Clients. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/07/21/business/dealbook/wells-fargo-confidential-data-release.html>

MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® StrutsTM Exploit : The Apache Software Foundation Blog. (n.d.). Retrieved October 9, 2017, from <https://blogs.apache.org/foundation/entry/media-alert-the-apache-software>

Riga, S. A. (2017). Two Breaches, Two Enforcement Actions, and a Ddos Attack: Data Security and the Rise of the Internet of Things. *Journal of Internet Law*, *20*(9), 3–7.

Rostow, T. (2017). What Happens When an Acquaintance Buys Your Data?: A New Privacy

Harm in the Age of Data Brokers. *Yale Journal on Regulation*, *34*(2), 667–707.