­­Jonathan Lowe

jl4ge

9/24/2017

STS 4600

Research Outline

I. Introduction

A. Frame the problem that your research investigates.

* Introduce IoT with examples
* Huge number of devices producing large amounts of data and a lot of the data collected is possibly extremely personal
* Define privacy
* Collection and retention of this data presents privacy risks from governments, corporations, and cyber-attacks. Provide examples
* Question: How should the data produced by IoT systems affect personal privacy?

B. Your main claim about that problem (or your best guess if you’re not sure of your main claim yet)

* The widespread use of IoT devices will make corporations effectively own (ownership as in legal control over) 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.

C. How you will support that claim (i.e., an outline of your paper’s subtopics)

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

II. Supporting Argument 1

1. Define this section’s claim. How does it relate to your overall 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.

B. Describe the reasons and evidence that support this claim. This section should be multiple paragraphs long, so for each planned paragraph:

a. Write a complete sentence as the topic sentence (claim) of the paragraph.

* Retail stores have used data mining has been used to infer private information
* Corporations are using data mining on the information that they have to infer private information
* 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.

b. Briefly describe the evidence you will use to support this claim, with citation(s).

* Through customer purchase history, Target sent pregnant women with baby clothes adds with a lot of accuracy. (Corrigan, Craciun, & Powell, 2014)
* Netflix gave a prize to people who could predict ratings on other movies using ratings users gave on other movies. (Bennett & Lanning, 2007) (Maybe remove)
* Netflix is using data mining to find shows that will be popular. (RESEARCH) (Maybe remove)
* sExamples of potential uses of IoT and how data mining could be used.

III. Supporting Argument 2

A. Define this section’s claim. How does it relate to your overall claim?

* Once corporations collect information from IoT devices about their users, they will effectively have exclusive control it.

B. Describe the reasons and evidence that support this claim. This section should be multiple paragraphs long, so for each planned paragraph:

a Write a complete sentence as the topic sentence (claim) of the paragraph.

* As of now search engines collect information about their users and pretty much exclusively control that information
* Other companies like data brokers collect buy and sell personal information without many legal repercussions

b. Briefly describe the evidence you will use to support this claim, with citation(s).

* Once search engines collect information about you they can do practically anything they want without significant legal ramifications. (Grimmelmann 2007)
* Aol released search results identified by user ID and people were identifiable from the results. (Barbaro & Zeller, 2006) There were no legal ramifications for AOL.
* Data brokers sell information to both companies and individuals (Federal Trade Commission, 2014).
* 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).
* With a few exceptions, there is no laws regulating the data broker industry in the United States (Rostow, 2017).j

IV. Supporting Argument 3

1. Define this section’s claim. How does it relate to your overall 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.

B. Describe the reasons and evidence that support this claim. This section should be multiple paragraphs long, so for each planned paragraph:

a. Write a complete sentence as the topic sentence (claim) of the paragraph.

* Tech companies have released personal data without their users’ knowledge or consent to different parties.
* IoT companies have insecurely stored and communicated customers’ data leaving it at risk

b. Briefly describe the evidence you will use to support this claim, with citation(s).

* Aol released search results identified by user ID and people were identifiable from the results. (Barbaro & Zeller, 2006)
* Companies like Yahoo, Google, and Aol released user information to the FBI surveillance program PRISM (Gellman & Poitras, 2013)
* 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 IoT face challenges to security that can prevent security measures from being put in place (Federal Trade Commission, 2015).

V. Conclusion­­­­

A. Synthesize and summarize your supporting arguments with your overall argument. In other words, explain how your supporting arguments make your overall argument believable.

* The widespread use of IoT devices will make corporations effectively own (ownership as in legal control over) 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.
* Data mining can also give corporations more private information than what their users gave.
* If the information that IoT companies collect is misused, the users that produced that information will have little legal support.
* In the past, there were abuses of consumer data by corporations which will likely continue.

1. Discuss the implications and limitations of your overall argument.

* The ownership of personal information by technology companies will likely not change unless there is an intervention or a significant number of users have a problem with it.
* There could be other factors not accounted for.
* Didn’t look directly at case law or future legislation
* Could have looked at other privacy definitions
* Could have used STS framework like ANT and SCOTT

VI.      Reference List (So Far not in order)

* Grimmelmann, J. (2007). *The structure of search engine law. Iowa L. Rev., 93*, 1.
* 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/
* Bennett, J., & Lanning, S. (2007, August). The netflix prize. In *Proceedings of KDD cup and workshop* (Vol. 2007, p. 35).
* 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/>
* 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>
* 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.
* Keating, B. (2008). Data Mining: What Is It and How Is It Used?. *Journal of Business Forecasting*, 27(3), 33 - 35.