Annotated Bibliography

Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times*. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

In the marketing industry, changing a consumers shopping habits, while very hard, is the perfect end state. Working for Target, Andrew Pole (a statistician and economist), did just that. In The New York Times Article, Duhigg outlines the process that Andrew Pole went through to determine if costumers were expecting a baby. Duhigg also goes into detail, with personal narratives, on the establishment of habits, concluding that habits can be broken. How Companies Learn Your Secrets provides an excellent example of how companies use large data sets to determine consumer behaviors without breaking privacy laws, yet consumers still feel like their privacy is being violated.

Wasik, B. (2013, May 14). In the programmable world, all our objects will act as one. Retrieved from http://www.wired.com/2013/05/internet-of-things-2/

Wasik is a senior editor for a technology magazine, Wired, giving him a more biased opinion on the future of the Internet of Things. In a programmable world, Wasik believes in the positives, describing many environmental friendly and safety applications that would result in a brighter future. In order to get to that point, a three step process must be followed. First, more devices need to be connected, followed by the devices being reliant on one another. Lastly, complex interrelationships need to be defined so that the system can be understood. Privacy and Security concerns of the Internet of Things are discussed, in which Wasik states his belief that the human is the downfall in security flaws, and within a programmable world, the human error is mitigated. In outlining the steps to make the Internet of Things successful while providing counterattacks to the common concerns, this Article proves to be strong for both the STS and Technical papers.

Hanson, J. (2015, August 22). Controlling the physical world with Leap Motion and Raspberry Pi [Blog]. Retrieved from http://blog.leapmotion.com/controlling-physical-world-leap-motion-raspberry-pi/

Hanson writes a short blog post containing a tutorial for connecting an embedded system to the Internet of Things. As a programmer Hanson wants to encourage others to take strides in the future he hopes see, advertising to readers his own network for simplistically scaling projects to a data stream infrastructure. The post focuses on the integration and interaction, highlighting the fact that the connected device can be controlled from anywhere on the globe, thus supporting my teams technical project.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. http://doi.org/10.1016/j.clsr.2009.11.008

Weber, who studied at the University of Zurich and at the Harvard Law School, is a professor specialized in teaching and publishing civil and commercial law with an emphasis on the Internet. His background and title give him the credibility of being a nonbiased source, as he writes to inform the public and fellow law advocates of how he believes to define the security of the internet of things. Weber concludes that a global solution complemented by the private sector in which several unique strategies are implemented is how data and privacy can be protected. Questioning the current perception of what privacy versus security is to society, and how private enterprises will play a vital role into the risk management of a connected system, this report will serve as a solid foundation for my STS paper. In outlining the procedures to secure the internet of things, Weber also goes into technical detail about topics such as peer to peer networking and domain name server security extensions, helping group my STS and technical paper.

Cornelius, E. (2014, August 26). Cybersecurity in the age of intelligent energy: Putting the nest thermostat “hack” in context. Retrieved from http://www.greentechmedia.com/articles/read/Cybersecurity-in-the-Age-of-Intelligent-Energy

Cornelius was the former Chief Technical Analyst at the Department of Homeland Security and was interviewed about consequences of cyber security vulnerabilities. What served to be particularly interesting about the interview is that Cornelius, an expert in the field, worries that it remains unclear what the long-term consequences of security vulnerabilities are. The interview agrees with the report done by Weber, in that private enterprises are responsible for security. The Target credit card attack is used as an example to show the cause and effect relationship that businesses have with security integration and operation. As a reliable source with no clear alternative motive, the interview with Cornelius provides distinct examples of the consequences of security vulnerabilities and the businesses role in limiting these repercussions.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. http://doi.org/10.1016/j.comnet.2012.12.018

The purpose of the journals article was to compare and contrast various architectural structures for the internet of things and provide an analysis of the features and security challenges of each approach. Written by senior security researchers, and approved by the journal of Computer Networks, the article is deemed reliable. The three researchers conclude that there are various security challenges to each structure and can be put into the categories such as trust and governance, identity management, and privacy. The article agrees with the New York Times article (on Target gathering information on customers) in that the two sources conclude there needs to be transparency in privacy as well as businesses need to prevent the notion that the internet of things is controlling our lives. Roman, Zhou, and Lopez present the pros and cons of multiple internet structures in a neat presentable manner, even showing the roles and interactions of the actors within each, proving to be moderately useful for both STS and Technical papers.

Moldrich, C. (2015, October 12). New Tesla Model S feature makes long drives more relaxing. Retrieved from http://www.alphr.com/go/1001727

Moldrich reports on Tesla's Model S over the air software upgrade, keeping personal opinions out of the conversation. Already viewed as an innovative company, Tesla added features to their car's touch screen display as well as a $2,500 autopilot package upgrade with a wireless system update. Using the power of the internet, Tesla has transformed the car industry to be more like a smart phone. This source provides an excellent example of how the internet of things will transform companies business models to be more serviceable, and gives additional insight to a the technical capabilities of the Internet of Things.

Hui, G. (2014, July 29*).* How the Internet of Things changes business models. Retrieved from https://hbr.org/2014/07/how-the-internet-of-things-changes-business-models

Hui writes for the Harvard Business Review, warning business owners of potential shifts in product based models that could cause a major disruption. As start-ups take advantage of the internet of things, the mindset for value creation and value capturing shifts. Value Creation shifts from stand alone products to over-the-air updates, as seen in Tesla's Model S upgrade. Value Capturing takes a shift from selling the next product to enabling a recurring revenue, also practiced by Tesla's $2,500 autopilot package. Hui provides an easy to read chart of value creation and value capturing shifts, providing insight on a business shift towards personalization and network loyalty.

Tucker, P. (2014). *The naked future*. New York, NY: Current.

Tucker is a deputy editor for Futurist magazine telling the story of how trends, including big data and the internet of things, are shaping society and businesses. As a science fiction writer, Tucker believes news outlets portray a future of big data and increased computation as a threat rather than a major opportunity. As a society, we must familiarize ourselves with the technology in order to safely use them for better living, and to understand how the future can be abused. Tucker's writing is an easy to read narrative that provides excellent, tangible examples for future interactions between society and technology, both calm and intense.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). Unlocking the potential of the Internet of Things. McKinsey Global Institute. Retrieved from http://www.mckinsey.com

A group of technological consultants estimate the economic value behind the internet of things technology. Working for McKinsey Global Institute, the consultants want to display their domain expertise in their report in order to gain future clients, making them a reliable source. By the year 2025, the McKinsey Global Institute team predicts an economic impact of $4 trillion to $11 trillion per year. While an enormous range, this goes to show just how large yet undefined the future for businesses in the internet of things truly is. The team goes into detail about how certain connected systems can create value in various settings, from homes to retail environments, and human worn to cities. The research compiled by the McKinsey Global Institute provides excellent graphs featuring potential business models, economic sector estimates, and examples of connected applications that will be of great use for both the information provided and building blocks for future research.