The Role Privacy Plays in the Greater Sociotechnical System of the Internet of Things

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jiafu Li

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

Executive Summary

The Internet of Things (IoT) has been around since 1999, and it is a system in which different machines and technologies can talk to each other using sensors. Both projects contained in this portfolio, a technical report and an STS research paper, focus on IoT. The technical report explores using infrared light to transmit and receive data across IoT. Whereas the STS research focuses on the privacy of the IoT network. The two projects go hand in hand because good technologies should also be safe to use. Engineers must be able to put into consideration many factors to ensure their technologies are not causing more harms than good. The two projects are complementary because managing safety concerns should always be a top priority in technology creations.

The capstone project explores IoT from a technical aspect and answer questions such as what kinds of communication is best suited for an IoT network. There already exists many different communication protocols for IoT, some of these includes WIFI, Bluetooth, Zigbee, and many more. Each of these protocols have downsides such as shortness of range, high power consumption, high latency, etc. Engineers continue to pursue new ways to improve IoT communications, and one such idea is the use of Optical Communication. Optical Communication uses infrared light to carry data, and my research team built a small model using Arduino to demonstrate what the system would look like. The data sent via Arduino's infrared light network showed promises for Optical Communication. However, this technology is highly subject to interferences, and future work is needed to ensure that the multi-communication network does not suffer packet loss. Additionally, scaling the system to test longer distances would also be required. Optical Communication is still relatively new and very early in its

development phase, many more researches and tests need to be conducted before putting it to use.

The subject of my STS research paper focuses on how the security of IoT can be improved. IoT refers to the connection of physical devices which allows them to collect and exchange data in real time and can make our environments more connected. However, with the growing number devices and the volume of data IoT generates, it is also much easier for cybercriminals to discover vulnerabilities and take over the network. IoT is changing how society collects and exchanges data. The framework technological determinism is used to discuss how exactly IoT has influenced the creation of Smart Cities and are used in critical applications such as healthcare, transportation, and industrial control systems. IoT has demonstrated its value and it is too important to not use this network out of fear of cyber-attacks. The question then becomes how much risks are users willing to accept in order to continue the usage of IoT. Risk analysis is used to discuss the security, privacy, reliability, and regulatory compliance of IoT devices and systems. It is essential to implement strong security protocols such as encryption and vulnerability testing to maintain regular security updates. The privacy and security of the users can then be protected and will raise the reliability of IoT.

Working on both projects simultaneously has helped me defined what it means to be an engineer. It is important to consider not only the technical aspect of the technology, but also how a particular piece of technology may bring about changes to the society. The web and internet are still relatively new as it has only been around for four decades. Most internet users may be aware of the dangers of the web and data leakages, but most users also do not consider that as their top priorities with regards to using internet connectable technologies. As long as the users are achieving what they want to achieve via the web, they often do not mind or neglect altogether the

dangers of data privacy in the web. Nonetheless, that does not mean engineers can also disregard safety protocols. Every engineer must create new technologies with safety in mind. New functionalities are always great to have, but it is also important to evaluate what potential harm these new functionalities may bring.