LPWAN IOT Product Development for Alarm.com
(Technical Paper)

User Sentiment Regarding Conflicts of Privacy in the IOT Space
(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Allison Renehan
Fall 2019

Technical Project Team Members
Anna Haikl
William Lupton
Corey Nolan
Bryan Rombach
Eric Timmons

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

Signature _____ Date _____
Allison Renehan

Approved _____ Date _____
Reid Bailey, Department of Engineering Systems and Environment

Approved _____ Date _____
Kent Wayland, Department of Engineering and Society

General Research Problem: Developing the Internet of Things

How can actors in the Internet of Things continue to innovate while keeping users safe?

Known also as “smart devices”, the “Internet of Things” is the umbrella term for all technology that enables everyday objects (watches, refrigerators, doors, etc.) to be interactive and connected to a communication network of other devices. These devices contain collections of sensors, actuators, and information processors that are able to transmit, store, and even make decisions from collected data without any human help or chaperoning. The full-scale implementation of the Internet of Things is projected to be the next big component of the technological revolution. This complex network is estimated to have a $6.2 trillion yearly economic impact by 2025 and promises to radically change our relationship with technology (Thierer, 2015, pg 14).

As a socio-technical system, the Internet of Things (IOT) is still very much in the experimental stage of innovation. This stage of development is defined by a flurry of simultaneous activity. While producers are experimenting, designing, and testing out new technologies and uses, regulators are trying to outline what the technology is, its impact, and the strategy needed for safe growth and future development. Users of this new system are in the middle, trying to figure out how to interact with it all. The Internet of Things continues to become more relevant and the differences between the involved groups correspondingly grows in importance. The mutual shaping between what producers can create, what users want, and what regulators will allow will take center stage in determining the ultimate success or failure of the Internet of Things.

LPWAN IOT Product Development for Alarm.com

How can LPWAN technology address a new and valuable problem for Alarm.com?

While some IOT technologies are already pretty well researched and developed, new advances lead to an ever-expanding field. For my technical research project, my team and I will be working in one of the less developed parts: the Low Power Wide Area Network (LPWAN) space. Aptly named, LPWAN is a newly developed classification of communication technologies that is the combination of hardware and software protocols that allow sensors to transmit small amounts of data over long distances while using less power than existing IOT tech (Mekki, 2019). One example of this is SemTech's development of a body temperature and activity sensor that is installed on a cow's ear, allowing for farmers to notice irregular behaviors and diagnose health problems early on (SemTech, 2018). This device uses a type of LPWAN technology called LoRa; it is able to track the cows over the entire grazing areas and send the data back to the farmer. This use would not be possible with other IOT technology unless the farmer had a WiFi or cellular network covering the entire farm, and was able to afford the price of such an installation and upkeep, neither of which are common or reasonable to expect.

While "LPWAN" was not defined until after 2013, the idea of low power wide area communications has been around since the 1980s. However, the advent of cellular networks in the 1990s initially decreased the relevance for the LPWAN predecessor due to the cellular network's ability to send larger packets of data. The majority of these early applications were in the home automation space, where sending as much data as possible was more desirable for the users considering the involved safety concerns. Plus, the cellular network was able to transmit voice and quickly became more accessible, driving down prices compared to the LPWAN-precursor. LPWAN tech started their comeback around 2009 when SIGFOX built the first

modern LPWAN network in France (Ray, 2017). Since then, the area has continued to grow and gain excitement; it is now considered to be the fastest growing communication technology in the Internet of Things (Pasqua, 2018).

Our client for this research is Alarm.com, a current market leader in the IOT home automation space. Home automation usually uses protocols that are not low-powered, since most of the devices have an actuator attached, requiring a good deal of energy. Alarm.com's experimental lab is looking into LPWAN tech for future expansion outside of the home automation market and wants our team to what such an expansion process would look like and if it could add value for the company. For Alarm.com, LPWAN has been identified as the next logical area of IOT to explore because of the buzz it is causing in industry and its low cost, high return on investment potential. The structure of the LPWAN protocols and how they work is already well researched, so my team is focused on addressing how LPWAN can be valuable to Alarm.com.

We will address this problem by doing in-depth market research to focus on specific use cases that have the largest value potential for our client. One example of a use case we are currently exploring, to shed some light, is the idea of remote security sensing for large campuses. Colleges and any other company with large properties could use things like a contact sensor to see if any people have ventured into an area they are not supposed to be in, i.e. if a steam tunnel cover or manhole was opened when no workers are scheduled to be in the area. A non-LPWAN contact sensor, for reference, would either need to be plugged into a power source, requiring a long extension cord, or it would be battery-powered, requiring a battery that needs replacement at least every couple months. Having multiple contact sensors spread throughout a campus that need frequent battery replacement or have long extension cords running to them is again

inconvenient, labor-intensive, and expensive, so LPWAN's advantage of having a years-long battery life is clearly beneficial in these situations.

Once we have identified a use case, we will deduce the best technology to meet its needs. The different technology options are LoRa, NB-IOT, and CAT-M protocols, all of which are low power wide area networks. Each provide different advantages. For example, LoRa has the longest battery life and does not require a cellular network, while CAT-M can send the most data at a time, and NB-IOT is built on an already-established and mostly-common protocol. Since each of the LPWAN protocols perform better in different uses, the "best" technology depends heavily on the desired application.

After determining the use case and type of technology to use, we will design, build, and test a prototype to present a demonstration of the technology and its proposed value to the company and users to Alarm.com's executive team. This presentation is our ultimate deliverable and priority for our project, where our extensive user research will highlight all we learned about the requirements for successfully entering a new market area. By explaining how Alarm.com can make a difference with our envisioned LPWAN device, we hope to clarify what is needed for our client to enter into new markets with such technologies. The research we do along the way will provide the basis for future work in identifying value for clients, defining use cases, and basic LPWAN prototyping.

Themes of User Privacy Conflicts in the IOT Space

How is the conflict over data use shaping the IOT space?

On the social side of the Internet of Things, the newness of this area leads to a multitude of conflicts for the people involved. As the socio-technical system of the Internet of Things

approaches stabilization, this research will seek to discover how appropriate user privacy will be defined in related applications.

As IOT is still developing and continues to change at an extremely rapid pace, the space is largely unregulated or structured. This lack of infrastructure or a code of ethics has created a lot of controversy over who should create it, who should enforce it, and to what extent should these rules be made. Within the umbrella of "ethics", one area of specific concern is user privacy. Everyday objects now equipped with computing capabilities collect massive amounts of data, some of which is extremely personal or sensitive for the user. Regardless of if the data is directly tied to a user's identifiable information or if it is considered actually "personal", there is controversy over how that data should be used. Without a universal IOT code of ethics, companies that produce these devices (referred to as "producers") are not held to a specific standard to store, protect, or use the data and have made decisions unique to their company. This data is sometimes used by the producers to analyze trends and profile users, in order to better predict demand, improve the user experience, or send highly targeted marketing (Allhoff, 2018, p59-60). While some of those might be beneficial to users, not everyone welcomes the use of their data in such a way and, in some cases, are unaware of it being used in that way.

A constant struggle within that disagreement is finding the balance between technology that uses user data to optimize the user experience versus protecting the user from violations of privacy, security, or other harms. A well-known instance of this was brought to light in 2016, when a consumer sued the producer of a smart sex toy when she discovered the device was collecting and storing data on the date and time of use and preferred settings, which were attached to the user's email address. The company claimed the data was to help improve their products and for "diagnostic purposes", while the user felt it was an invasion of personal privacy

(Redden, 2016). There is a multitude of groups in place in vocal support of either side. Every group has many opinions on various aspects of IOT privacy, from the Consumer Electronics Association arguing that the power of IOT devices is in their ability to gather so much data, to the Federal Trade Commission Chairwoman warning producers against storing user data without a specific use for it (Thierer, 2015).

While many watch dog organizations and industry alliances share their opinions on this issue, it is more challenging to find what the users themselves think about this tension between innovation and protection. Sentiments from the two more biased groups (regulators and producers) are available in press releases and are referenced in many scientific journal articles. To discover actual user sentiment and not hypotheses speculated from invested groups, research has to dig a little deeper. One place to look to is past court cases made over privacy conflicts. These can show specific actions or practices by producers that made at least one user uncomfortable. Some research papers that describe the overarching area of privacy in IOT reference these cases, such as Fritz Allhoff and Adam Henschke's "Internet of Things: Foundational Ethical Issues" article in the *Internet of Things* journal, or Adam Thierer's article on "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" in the *Richmond Journal of Law and Technology*. They should also be available through law journals and court documents. These cases are usually more extreme situations and should be screened with that in mind. A less extreme place to look is at user-focused research. Four Princeton students studied users' perception of privacy in IOT home devices by conducting multiple interviews with actual users in their article "User Perceptions of Smart Home IoT Privacy" (Zheng, 2018, p1). Sources with research methods similar to that study would help to properly identify themes of user sentiment. Additionally, sources from the

involved organizations will be helpful to serve as a contrast to what the users are saying themselves, to see if these groups are accurately representing users' desires. Past speeches from the Federal Trade Commission or reports from industry alliances have already shown promise on this front. Once a multitude of sources are collected, their content will be analyzed to determine consistent themes of user concern. These themes and their relation to different actor-groups will be used to see if there are additional sub-user groups to identify and independently consider, in addition to highlighting how the Internet of Things is going to reach a consensus for this aspect of the socio-technical system.

By the end of the project, a thorough examination of the thoughts of the producers, regulators, and users on user privacy of IOT devices will highlight the differences therein. By systematically analyzing these numerous systems, this project will contribute a broader understanding in the stabilizing process of this system. As the Internet of Things and its looming ubiquity will soon force itself upon the general population with its estimated 20-50 billion connected things by 2020 (Allhoff, 2018, pg 1), knowing what users actually feel and want from this system will enable better regulation and corporation practices, not to mention educating potential users on what to expect so they can make informed decisions.

While this body of research aspires to highlight current user sentiment over the ethical development of the Internet of Things, there is a lack of representation for future user groups. That is, people who are currently unable to participate in the IOT due to financial or other such barriers need to also be surveyed and considered when developing new applications or ethical standards so that the Internet of Things can be generally inclusive and avoid systematic bias. In order to fully understand how the socio-technical system will stabilize and unify, such an issue should be considered as the basis for future work.

Conclusion

Whether it be ethical boundaries or uses for emerging LPWAN technologies, the Internet of Things offers a multitude of facets to consider and address as its relevance continues to grow. Exploring this currently limitless space to highlight key issues for future development will ultimately encourage system users, regulators, and producers to be more socially and technically educated. Considering the predicted 4.5 million IOT developers and 7.9% compound annual growth rate by 2020 (Thierer, 2015, pg 14-15), having educated and aware players in this system will have far-reaching affects on the network's future and its soon-to-be pervasive societal impact.

References

Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things*, *1–2*, 55–66. https://doi.org/10.1016/j.iot.2018.08.005

Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, *5*(1), 1–7. https://doi.org/10.1016/j.icte.2017.12.005

Pasqua, E. (2018, September 27). LPWAN emerging as fastest growing IoT communication technology – 1.1 billion IoT connections expected by 2023, LoRa and NB-IoT the current market leaders—IoT Analytics. Retrieved from https://iot-analytics.com/lpwan-market-report-2018-2023-new-report/

Ray, B. (2017, May 3). The History of LPWAN and a Look at its Future. Retrieved October 26, 2019, from IoT For All website: https://www.iotforall.com/history-of-lpwan-look-future-of-lpwan/

Redden, M. (2016, September 14). Tech company accused of collecting details of how customers use sex toys. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2016/sep/14/wevibe-sex-toy-data-collection-chicago-lawsuit

SemTech. (2018, August 15). LoRa Monitors Cow-Health in Real Time. Retrieved from https://www.semtech.com/company/press/semtechs-lora-technology-monitors-cattle-health-in-real-time.

Thierer, A. D. (2015). The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. *Richmond Journal of Law and Technology*, 21(2), 119. Retrieved from http://scholarship.richmond.edu/jolt/vol21/iss2/4.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–20. https://doi.org/10.1145/3274469