Prospectus

Designing an Air Guitar – S.H.R.E.D.

(Technical Report)

Designing Ethical Internet of Things Devices in Public Spaces

(STS Research Paper)

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

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Karan Chawla

Fall, 2019

Department of Electrical & Computer Engineering

Signed: _____

Approved: _____ Date _____

Sean Ferguson, Department of Engineering and Society

Approved: _____ Date _____

Harry Powell, Electrical & Computer Engineering

I. Introduction

The prevalence of Internet of Things (IoT) devices in both the public and private sectors has significantly changed the way that we interact with technology and the information that is readily available to us. The rapid growth and urbanization of cities across the world has prompted a need for waste management issues to be addressed; for a city to sustain growth and have a healthy populus, the resources involved in waste management (people, equipment, energy, etc.) should be reduced. With regards to our team's blueprint, smart waste management has seen an influx in public planning development, with existing platforms based on installing sensors in bins to optimize trash collection and improve the welfare of private citizens through a variety of initiatives (e.g. utilizing solar energy).

While the U.S. Department of Commerce has recommended to enact a "stable, secure, and trustworthy IoT environment" (Hill, 1982), the word "ethics" is absent from their analysis - a fact that is worrying given the decentralized control and infancy of privacy of standardization surrounding the technologies. For instance, in 2017 a fault was discovered in an IoT pacemaker that led to a recall of over 500,000 devices, a flaw that may have allowed a hacker to gain control over the devices (Allhoff, 2007). As such, this paper concerns the ethics involved with implementations of IoT devices in public spaces, with specific reference to smart waste management (our research project), through the lens of the Social Construction of Technology (SCOT) theory.

II. Technical Topic: Designing an Air Guitar - S.H.R.E.D.

S.H.R.E.D. (Sensor Handheld Rock and Roll Electronic Device) is a musical instrument designed to give musicians the experience of playing an air guitar, while providing a realistic sound. The project will involve a phone application that takes the finger positions of the user to determine the chord being played, as well as a distance sensor to determine which frets along the neck of the guitar are being played. An accelerometer will be used to determine when the guitar is being strummed, and all of the sensor and phone application data will be relayed to a National Instruments myRIO board via a printed circuit board with wired connection to the accelerometer and phone. The myRIO board then creates soundwaves for a variety of instrument types using signal processing techniques such as the Karplus-Strong string synthesis algorithm.

Our group chose to explore the musical applications of these gloves due to the overall intrigue and practical application of learning how to play a musical instrument without the burden of paying for expensive equipment. Traditional guitar strings can also be painful to play when a musician has not developed callouses, making a touchscreen-based input appealing to beginners. Another use case of our device is in facilitating airplane travel for music hobbyists and others as booking an extra seat or risking damage to a musical instrument during air travel comes with a large financial risk not found in our product. Building off of this sentiment, our device is also suitable for a public environment in which a user can send the output of their signal to a set of headphones instead of through a speaker, useful for practice sessions in a quiet setting.

Projects that attempt to replace a physical musical instrument with either substitute physical items (smaller hand-held devices, programmable guitar necks, etc.) and/or wearable

gloves have been constructed in the past, however our project differs in several key aspects from these companions. A product currently in the consumer market, *Kurv Guitar*, seeks to reinvent how specific hand-held devices control musical intonation and note-playing, however the project strays into the realm of being a 'new' musical device rather than a substitute for an existing one, the market our device aims to fill.

Misa Digital is a company developing digital guitars with alternatives to standard strings. The guitars are full sized, and rely on a capacitive fretboard that runs up and down the entire neck of the guitar. In order to play the notes, a touch screen is integrated into the body of the guitar where touching the displayed string produces a sound. The touch screen has multiple sections, such that touching different sections produces different synthesized instrumental sounds that can be played at the same time. The touch screen also has different modes, with one of them allowing for one string to be played at a time. This project is similar to ours, although it is housed in a full sized guitar, and their capacitive touch screen is used for playing the notes, instead of the fretboard note selection. Misa Digital has also not implemented accelerometer based strumming into any of their products.

The incorporation of sensors to determine what notes are being played and how loud to play them involves the use of IoT devices in a commercial setting. While our sensors do not use a wireless signal to communicate on a global scale, local communication is used to facilitate note capture. The decision to communicate via wired connection was made due to the latency involved with using wireless communication protocols, for instance, bluetooth communication from an Android device typically involves a 200ms - 500ms delay due to the technology stack involved with Android phones. Furthermore, through using wired connections, we have increased the assurance that only authorized users can access the data transmitted from the phone and sensors to the myRIO, as attackers may otherwise intercept and modify signals sent wirelessly.

III. STS Topic: Designing Ethical Internet of Things Devices in Public Spaces

IoT broadly defines a global infrastructure in which all objects are equipped with smart devices to collect and communicate data through the Internet. Specifically, IoT devices change the way in which we interact with technologies, allowing for increased automation or enabling action-at-a-distance (Allhoff, 2018). The rapid expansion of IoT technologies from 7.0B devices in 2018 to a projected 21.5B devices in 2025 (Lueth, 2018) brings to the forefront the need to consider how devices may best be developed to safeguard personal property and privacy. Furthermore, while the Code of Ethics for the IEEE states it will strive "to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin" (Cortland), the proliferation of these devices may inadvertently increase the gap in the inefficiencies faced by those who can and cannot afford new technologies.

Given the varying use-cases and importance of the domains in which IoT devices will continue to develop, it is important to discuss the data privacy and security issues surrounding the technology. Through the usage of IoT devices such as smart refrigerators, watches, security systems, etc., companies have access to large quantities of private information and consumer habits, thereby inadvertently gaining the privilege to infringe upon consumers - a practice that is somewhat commonplace. Take for example the recent lawsuit filed against Facebook claiming that the company was negligent in the distribution of millions of users' data to a third-party

website without direct user consent. When companies have the ability to generate additional revenue they are more likely to infringe upon our rights (Cortland), and although ACM exists to serve as a guideline of ethics, it is immeasurably difficult to enforce the misuse of technology on a global level.

As highlighted above, the fact that established companies have difficulties adhering to ethical practices only underlines the importance for emerging IoT technologies to have "security built into… the foundation of the IoT solution." (Tzafestas, 2018). Bigbelly, is a smart waste management company based in Massachusetts whose proposed and enacted solutions will be studied as an example case of IoT deployment. Specifically, Bigbelly has installed solar powered "smart" bins in Manhattan, all equipped with a chip that detects when a bin is too smelly or full, is capable of compacting trash itself (up to 5x more space), and can communicate wirelessly to notify when pickup is required (Poon, 2015). Furthermore, some of the containers have had Wi-Fi units installed in them so they may serve as public hotspots. While this technology is promising and has shown tremendous results, ethical concerns regarding these devices with specific mention to property, accessibility, accuracy, and the private use of information must be addressed (Figure 1).

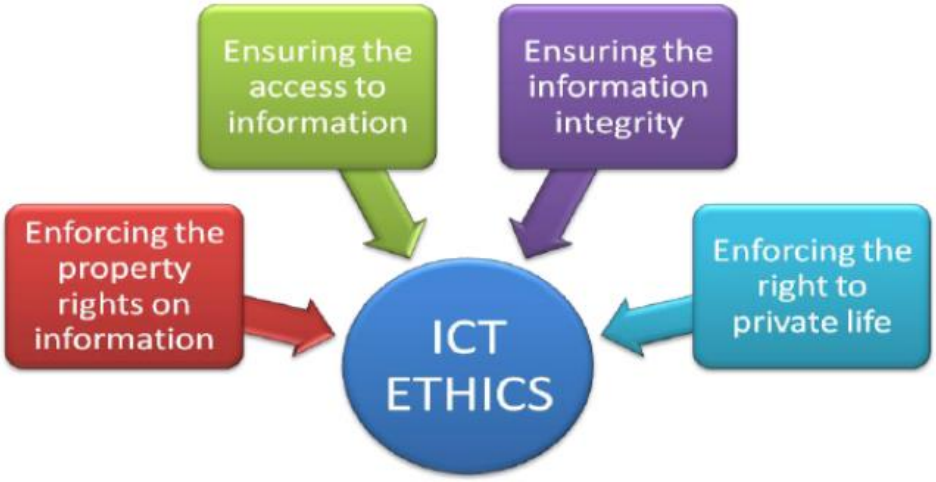

Figure 1. Central ICT Issues (Popescul, 2014)

With regards to the property rights of data and information, the responses to who the owner of the data retrieved is and what parties have access to it should be clearly stated. In the case of Bigbelly, should the company have a right to monitor traffic going in and out of its hotspot networks, and do they have the right to sell this data to third-party platforms such as city governments or ad companies in order to better target consumers? The increasing presence of IoT technologies will lead to the boundaries between the public and private sectors diminishing, and the decrease in the physical size of these devices may result in a lessening of the ability to regularly inspect, audit, and ensure that security standards (such as informed consent) are being met. Critical information, whether it be personal or financial, is additionally at risk of being compromised due to the lack of existing governance and security - according to one report 20% of organizations have experienced at least one IoT attack in the past three years (Gartner, 2018). Furthermore, since IoT devices exist in an ecosystem made up of many different manufacturers,

integrating differing security schemes (authentication, identity, etc.) is a challenge that must be combatted.

On a separate point, many authors have even claimed that access to raw data constitutes a moral right (Lunshof, 2014), a subject which brings to light general principles of ethical design. Baldini (Baldini, 2018) argues that ethical IoT products should have the following features, in addition to informed consent as previously mentioned (control over the collection and distribution of data related to the user); capability to enforce different regulations across time and space, and support dynamic contexts (houses, offices, etc.). Overall, it appears that the ability to develop a device that does not obscure the information it collects, is capable of being modified remotely (e.g. through software updates), and creates an 'opt-in' rather than 'opt-out' policy collecting information addresses these concerns. Additional challenges to ethical designs come from factors not directly related to the technology itself, but from social/political factors. For instance, economic incentives for data protection are limited to the businesses developing these devices and not the users themselves. Furthermore, there may be too much information needed to make a completely informed decision, and the ability for a user to gain immediate benefits may have long-term impacts (greater output of devices with lower security standards).

It appears that the underlying standards of security that must be built into these products include device: registration, authentication, authorization, configuration, fault diagnosis, and monitoring. Device authentication is a must in terms of being able to trust the nodes in a network as one faulty node can compromise the whole, while issues of integrity and confidentiality are more related to the specific application of an IoT device. The configuration of many IoT devices in public also highlights a broader need for industry standards across manufacturers in terms of liability, data privacy, and authorization schemes.

IV. Bibliography

1. Hill, D. A., & Wait, J. R. (1982). National Telecommunications & Information Admin. *Institute for Telecommunication Sciences*.
2. Allhoff, F., Lin, P., Moor, J. H., & Weckert, J. (2007). *Nanoethics: the ethical and social implications of nanotechnology*. John Wiley & Sons.
3. Allhoff, F., & Henschke, A. (2018). The internet of things: Foundational ethical issues. *Internet of Things*, *1*, 55-66.
4. Lueth, K. L. (2018, August 8). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Retrieved from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.
5. Cortland, S. (n.d.). Ethical Issues - The Internet of Things. Retrieved from https://sites.google.com/a/cortland.edu/the-internet-of-things/ethics.
6. Tzafestas, S. G. (2018). Ethics and law in the internet of things world. *Smart Cities*, *1*(1), 98-120.
7. Poon, L. (2015, July 10). Next Time You Want Free Wi-Fi in NYC, Look For A Trash Can. Retrieved from https://www.citylab.com/life/2015/07/new-york-city-wi-fi-trash-cans/398258/.
8. Popescul, Daniela, and Mircea Georgescu. "Internet of Things–some ethical issues." *The USV Annals of Economics and Public Administration* 13.2 (18) (2014): 208-214.

9. Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018. (2018, March 21). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018.
10. Lunshof, J. E., Church, G. M., & Prainsack, B. (2014). Raw personal data: providing access. *Science*, *343*(6169), 373-374.
11. Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical design in the internet of things. *Science and engineering ethics*, *24*(3), 905-925.