Ethics in the Self-Powered Internet of Things

A Research Paper in STS 4600

Presented to the Faculty of the School of Engineering and Applied Sciences
Unviersity of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

Author

Nojan Sheybani
April 27, 2020

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 _____

Approved _____ Date _____
Rider Foley, Department of Engineering and Society

Introduction

The Internet of Things (IoT) has been described as the next technological revolution (Feki, 2013). The IoT is a collection of wireless sensor nodes that interact with each other in order to achieve a common goal or monitor a certain environment. This networked technology can be applied in myriad contexts, from turning on a light with your Alexa to monitoring the amount of lux in all the rooms of your house. Some of the other fields in which IoT is applicable include social networking, healthcare, industrial plants, and many more widespread domains (Atzori, 2010). IoT is a groundbreaking movement in the technological field and by 2025, assuming current trends continue, there will be 75 billion IoT devices in the world (Bera, 2019). While this is an exciting statistic, there is a high chance that this milestone will not be achieved due to a common component of most IoT systems: batteries. At approximately 50 billion devices, we will plateau in our production of IoT systems due to their reliance on batteries (Calhoun, 2019). This problem is currently being addressed through research, development, and commercialization, from local companies such as Everactive, of self-powered and internet-connected devices.

A more appropriate name for self-powered systems would be environment-powered systems as self-powered systems are defined as technological devices, such as an IoT device, that is powered by ambient energy that is harnessed from the environment of the system (Glynne-Jones, 2001). There are many sources of energy from the environment that can be utilized in a self-powered system, such as vibrations, solar, and heat. While there are many harvesting modalities that a self-powered system can use, none of these modalities provide the constant power to a system that a battery has the power to do. Self-powered systems do not rely on

batteries and their harvested power fluctuates due to the randomness of the environment (Wang, 2010).

To achieve the expected growth of the IoT, the cost and scalability of battery replacement must be taken out of the equation. Self-powered systems provide a battery-less approach to the standard design of IoT nodes, but the power budget, which is the maximum amount of power that can be used by a system before it can no longer operate, that is introduced can significantly hinder the solutions towards the ethical implications of the IoT, such as security and privacy. For instance, many IoT nodes use computation and power-heavy techniques to protect data, but the power budget introduced in the self-powered IoT makes these techniques nearly impossible. The IoT itself has many ethical implications that have been researched thoroughly, so the self-powered IoT will adopt these ethical implications and present new, more challenging ones to consider. This research examines the ethical implications associated with the adoption and implementation of the self-powered IoT.

Ethics in the self-powered IoT

The IoT is often discussed in a technical sense, but due to the ethical implications that surround the implementation of IoT, this technology must be viewed through a sociotechnical lens (Ghaffari, 2019). A sociotechnical system consists of four interactive elements: technology, structure, tasks, and actors. The development of IoT consists of all of these elements and the interactions between them. Technology is the physical artifacts, such as hardware, software, and network and security. Structure consists of the formal regulations, rules, and standards for IoT development, as well as the informal norms, expectations and behaviors. Tasks in this sociotechnical system are defined as the actions that need to be taken in order to make progress

in the development of the IoT. A very important task for IoT is research and development, which is where the feasibility and prototyping of IoT systems are presented. Finally, actors are any entities that influence or are influenced by the IoT. Four of the most prominent actors in the IoT are the government, industries, consumers, and entrepreneurs. One of the key aspects of the elements of a sociotechnical system is the interaction of the elements with each other. For instance, the actor-structure interaction is crucial to the development of IoT. Governments create rules and regulations for the development of IoT that industries and entrepreneurs must adhere to when proposing new advancements for the IoT. Customers also have a strong relationship with structure, as structure allows standards and regulations to be declared pertaining to a customer's data privacy and security (Ghaffari, 2019). This framework, which focuses on the four elements of a sociotechnical system and their interactions, will be used to analyze self-powered IoT systems.

The self-powered IoT will be evaluated using a normative framework, *responsible innovation*. Responsible innovation is formally defined as "taking care of the future through collective stewardship of science and innovation in the present" (Stilgoe, 2013, p.1570). The self-powered IoT will be evaluated to ensure that the presented technology will affect positive change in the environment. Responsible innovation consists of four dimensions: anticipation, reflexivity, inclusion, and responsiveness. Anticipation is asking "what if?" questions about new innovations. Foresight and technology assessment must be utilized in in order to avoid unforeseen detrimental implications of growing technological systems. The reflexivity dimension forces innovators to consider the "socio-ethical context of their work". Reflexivity encourages scientists to enforce morality throughout their innovation process. For example, codes of conduct can be set in the laboratory setting to ensure that morals and external values are connected to the

practice of innovation. The inclusion dimension is concerned with getting the wider public and stakeholders involved in the discussion and practice of innovation. The use of conferences, focus groups, and citizen panels/juries are a few examples of practicing inclusion in responsible innovation. Finally, the responsiveness dimension considers the ability of an innovation to pivot in response to stakeholder opinions or changing circumstances. Responsiveness can be approached in many different ways, such as regulation and standards, to ensure that an innovation will be able to change directions when needed. In order for responsiveness to be correctly analyzed and responsibly governed, it is important that the product and purpose are considered (Stilgoe, 2013). These four dimensions of responsible innovation will be used to evaluate the analysis of self-powered systems as sociotechnical systems, with a focus on the ethical implications of security and privacy in self-powered systems.

When analyzing the self-powered IoT as a sociotechnical system, all of the sociotechnical elements have connections with security and privacy. There must be tasks that are clearly defined to drive IoT development in a direction that emphasizes security and privacy. The correct technological approach must be taken in order to provide actors with products that ensure that a customer's privacy and security is safe. Structure must be provided in the form of rules and regulations that affect the interaction of actors with the self-powered IoT. For instance, rules and regulations (structure) pertaining to security and privacy that are set by the government (actor) influence the products that entrepreneurs and industries (actor) build, which become a part of consumers' (actor) everyday lives. This is a good example of an actor-structure interaction within a sociotechnical system. Security and privacy issues must be taken into consideration in the analysis of the self-powered IoT as a sociotechnical system and in the evaluation of self-powered systems as responsible innovation.

Case Context

A self-powered IoT node, in design, is not very different from a battery-powered IoT node. The main addition to self-powered IoT nodes are energy harvesting transducers, such as solar cells, a power management unit (PMU), and an energy storage device, such as a capacitor. A PMU extracts energy from the transducer and, if necessary, performs AC-DC conversion, with a certain efficiency, then stores that energy in the energy storage device. The energy storage then provides power to the rest of the system, as a battery would in a battery-powered IoT node. The PMU, transducer, and energy storage are the self-powered IoT's equivalent to a simple battery in the battery-powered IoT. While the additions of these provide a layer of complexity to designing IoT nodes, a battery-less approach provides an efficient way to avoid the cost and scalability challenges that are associated with battery replacement.

As self-powered systems are relatively new, the energy harvesting technologies have not reached amazing efficiencies yet. For instance, standard silicon solar cells can successfully harvest only about 15% of the available power from the environment on average (Murmson, 2017). This tends to work well for applications that can support huge solar cells, such as powering a home by placing solar cells on the roof. This is because the bigger a solar cell is, the more power it can harvest. IoT nodes boast a small form factor, so the solar cells must be relatively small, which poses a problem when trying to continuously power the system from harvested energy. This means that a PMU must be chosen that can deliver as much energy as possible from the transducer to the energy storage device, which can sometimes be difficult. The struggle of efficiencies with the components that build self-powered systems combined with the fluctuation of the harvested power as the environment changes introduces a strict power budget to self-powered systems. This power budget is the basis of many of the tradeoffs that

characterize the self-powered IoT, such as latency vs. power consumption and sampling frequency vs. power consumption. Low latency results in the node taking a longer time to transmit data, but it also results in lower power consumption. Similarly, low sampling frequency results in the node collecting data at a lower rate, but it also results in lower power consumption. Self-powered systems revolve around tradeoffs concerning the strict power budget, but it is important that these systems are still able to address ethical implications with this power budget.

The IoT has many ethical implications that require solutions. Security and privacy are the most challenging ethical implications to address (Dutton, 2014). Analyzing security and privacy in self-powered IoT systems is especially difficult, due to the aforementioned strict power budget. This strict power budget brings security into question as most security techniques, such as encryption, require a lot of computation, so a self-powered system, which can also be referred to as an "energy-starved" system, may not be able to provide the same level of security as a battery-powered system (Schaumont, 2017). For self-powered systems, the issue of security has been a very prevalent one that has few solutions. Currently, one of the main techniques for security is energy-optimized cryptography, but this is not as reliable as standard cryptography techniques (Schaumont, 2017). While security and privacy are widely viewed as a social problem within the IoT, the solution to these risks in the self-powered IoT requires clever technical advancements and applications of energy harvesting and power management within self-powered IoT nodes.

Research Question and Methods

The presented research answers the following question: What is causing the shift towards the self-powered Internet of Things (IoT) systems and what are the ethical implications

associated with this shift? Answering this question is important to highlight the sociotechnical components associated with this shift and the future ethical implications that can be addressed as the shift occurs. This will allow for foresight and responsible innovation to be employed to mitigate the ethical issues that arise from the shift towards self-powered systems.

Data was collected in the form of in-person interviews with entrepreneurs and professors in this field, Dr. Benton Calhoun and Dr. Dennis Sylvester, as well as public interviews that were recorded prior to this research. Ben Calhoun is a professor at the University of Virginia, principal investigator (PI) of the Robust Low Power Very Large Scale Integration (VLSI) lab, and co-founder and co-CTO of Everactive, a Charlottesville, VA startup with the mission of commercializing self-powered devices that connect to IoT systems. One of his most highly cited works focuses on a self-powered IoT node that can acquire, process, and transmit electrocardiogram, electromyogram, and electroencephalogram data. This work was published in a very prestigious chip design journal, the IEEE Journal of Solid-State Circuits (Zhang et al., 2013). Dennis Sylvester is a professor at the University of Michigan, PI of a low-power integrated circuit (IC) design lab, and founder of Ambiq Micro, a startup with the mission of commercializing low-power ICs. One of his most highly cited works focuses on a self-powered IoT sensor system that utilizes solar energy to try to achieve an infinite lifetime. This work was presented at the most prestigious chip design conference, IEEE Solid-State Circuits Conference (Chen et al., 2010). I estimate that there are about 35 established experts in the field and I was lucky to talk two of the most prominent figures in the field. These interviews were used to inform several different case studies, such as development of the IoT in Korea and ethical issues faced by the Amazon Ring. The self-powered IoT is analyzed as a sociotechnical system and evaluated with the framework for responsible innovation.

Results and Analysis

Over my college career, I have been quite involved in self-powered IoT systems through research and coursework with Professor Calhoun and building a self-powered system with a team for our technical capstone project. With this experience in hand, I came into this research with some assumptions about ethical concerns of the self-powered IoT, specifically that security and privacy issues would be amplified with the shift towards the self-powered IoT due to the introduced stringent power budget. The interviews helped me address these assumptions to determine if they were valid.

In a public interview, Ben Calhoun describes Everactive as "a start-up semiconductor company that has developed and is commercializing very, very low power wireless sensors that can harvest energy from their surroundings and power themselves" (Tom Tom, 2014). In my interview with Calhoun, he said that Everactive is one of the only companies in the industry focusing on commercializing end-to-end self-powered systems, so I asked why he believes that this shift towards the self-powered IoT is a necessity to innovations in the IoT:

> Scale – for the large-scale, next generation IoT to meet its promise will require trillions of distributed devices. Even with 10-year battery life, which is nearly impossible today, 1-trillion devices would require 274 million battery changes a day. The only way to achieve a scale of trillions is to remove the batteries.

With this in mind, I wanted to validate my aforementioned assumptions about weakened security and privacy due to the stringent power budget introduced in self-powered systems. Calhoun said that, although there is less power available, they can still provide "node-level security that is appropriate for their context". Following up with this, he mentioned that "the true

security (and privacy) provided by a system is provided by the full system solution, including the sensors, the networks, the gateways, the software, the cloud backend, and the people who maintain and use them." He then discussed the misuse of these secure systems and how these "small, long lasting devices could be deployed for unwanted surveillance or eavesdropping." My initial assumptions about weakened security and privacy were wrong, but I was introduced to a new security risk: the misuse of these self-powered systems.

The remainder of my interviews with Professors Calhoun and Sylvester focused on learning more about the ethical advantages and disadvantages. Professor Calhoun stated that the self-powered IoT does not have major ethical limitations:

> As I mentioned earlier, self-powered systems have a lot of advantages, ethically. For example, batteries use materials that are both environmentally challenging to mine and are difficult to dispose of, whereas self-powered systems do not. Self-powered sensors also enable efficiency improvements that reduce energy consumption and carbon footprint. For example, Everactive uses self-powered sensors to monitor steam distribution systems and lead to huge savings in steam loss, reducing both water and energy use.

Calhoun mentioned that there currently are some technical limitations that are being addressed through his research and industrial work, specifically "lowering power consumed by the electronics enough to match with the small amounts of harvestable power available, while also providing the needed system capabilities." Professor Sylvester shared the same sentiments as Professor Calhoun, emphasizing the fact that self-powered systems do not suffer from a lack

of security and privacy. He also mentioned that an ethical advantage of self-powered systems is the shift away from battery use, which heavily lowers the amount of electronic waste (e-waste).

Calhoun and Sylvester both, independently, informed me that self-powered systems can provide the standard amount of security and privacy that a battery-powered IoT system can, but security vulnerabilities in the battery-powered IoT are not uncommon. Although the self-powered IoT does not introduce weaker security and privacy, I followed case studies to show what security and privacy concerns the self-powered IoT inherited from the battery-powered IoT and to provide evidence of the shift towards the self-powered IoT.

Case Study 1: Developing the IoT in South Korea

The first case study analyzes the development of the IoT in South Korea. The security and privacy threats that are described are due to the rapid development of the technology in South Korea. Due to this fast-paced scaling, the author of this case study believes that the complex technical challenges to ensure security and privacy are not being appropriately considered, which could lead to the IoT being increasingly vulnerable to cyber-attacks. The author states that security is a big concern in the development of the IoT, especially when dealing with personal information (e.g. medical). Also, privacy is a concern from the consumers, because the consumers are not truly aware of what and how much data is being collected. This quote from the case study highlights a potential privacy threat in the IoT: “Edward Snowden disclosed that National Security Agency has illegally collected massive data using advanced IoT technologies,” (Shin, 2014). This quote reminded me of Professor Calhoun describing a potential security threat in the self-powered IoT being the ability to place self-powered systems anywhere for unwanted surveillance.

Case Study 2: Amazon Ring's Ethical Issues

The next case study outlines the security breach that faced the Amazon Ring, an IoT security camera. Amazon Ring provides the functionality for users to place cameras all over their household, even offering a smart doorbell, and offers a central hub to look through all of the cameras at once. A recent security breach has allowed hackers to take over users' Amazon Rings, watch users through the cameras, and even speak to the users through the system. For instance, one hacker broke into an Amazon Ring that was in an eight-year old girl's room, a Ring that was placed there by her parents for security, and repeatedly shouted racial slurs at her (Vigdor, 2019). If the man chose to stay silent, he could sit there and watch the eight-year old girl's room twenty-four hours a day, without ever being noticed. The Ring can be hacked from anywhere, no matter how far, and provide a live feed of the whole house with only a small blue light indicating that someone is watching the feed (Cox, 2019). The Amazon Ring is a prime example of the security and privacy concerns that are highlighted in the previous case studies. Consumers do not know what and how much data is being recorded by these IoT devices that they place around their homes and environments, and they also do not know who is accessing that data. This technical shortcoming by Amazon breached the privacy of the consumers of the Amazon Ring, which shows the security and privacy concerns of adopting the IoT. The self-powered IoT inherits these concerns, and somewhat amplifies them. As Calhoun mentioned, self-powered systems are long-lasting devices that can be deployed anywhere for data collection. If this technology were to be used for malice, it could put the security and privacy of many people at stake.

Case Study 3: LocationSmart Leaking Location Data

In 2018, geolocation data firm developed a product demo that allowed users to locate any cell phone based on the cell phone number. This was listed as one of the biggest IoT security failures of 2018 by technology news source TechRepublic (Sanders, 2018). This was uncovered when Securus, a smartphone tracking tool, was hacked. Securus's backend was provided by LocationSmart. It was later discovered that major cell phone companies, such as Verizon, AT&T, T-Mobile, and Sprint were selling their users' location data, without explicit consent from the consumers, to LocationSmart, which is how these mobile phones were able to be located at real-time when Securus was hacked (Whittaker, 2018). This means that users of these of major telecom companies were unaware of their location data being sold until Securus was hacked and the news story made these unethical acts public. This highlights a major security flaw in the self-powered IoT that was highlighted by Calhoun and Sylvester: long-lasting devices transmitting personal data to an unknown/untrusted party without the user knowing. While the LocationSmart data breach was bad, cell phones could not be located once they ran out of battery. With a self-powered system, the lifetime is theoretically infinite, which means that if a user does not know that a malicious actor is gathering their data, that party will be able to gather one's personal data forever. This is a prime example of how the self-powered IoT amplifies security and privacy issues that are associated with the battery-powered IoT.

Case Study 4: Advanced Self-Powered Systems of Integrated Sensors and Technology (ASSIST)

This case study provides evidence for the shift towards the self-powered IoT. The Advanced Self-Powered Systems of Integrated Sensors and Technology (ASSIST) Center consists of top research universities, such as University of Virginia and University of Michigan, and top research professors, such as Professor Calhoun, pursuing the center's core vision: "To create self-powered sensing, computing, and communication systems to enable data-driven

insights for a smart and healthy world." This research center has acknowledged that the battery-powered IoT will soon plateau in its growth, which is why they have brought together the best minds in the self-powered IoT to promote growth and innovation in the field, with a focus on healthcare applications. With many close ties to industry and academia, ASSIST has been able to spearhead advancements in many new applications of self-powered systems, such as wound monitoring and metabolic tracking. This research center also provides undergraduate research opportunities and a pre-college outreach program to teach K-12 and undergraduate students about the self-powered IoT. ASSIST is funded by the National Science Foundation (NSF), a governmental research institution, meaning that the development of the self-powered IoT is an objective that is acknowledged and encouraged by the United States government (ASSIST, 2020).

Discussion

Sociotechnical relationships evolve when moving from the battery-powered IoT to the self-powered IoT. The actor-structure relationship, for instance, must change. The self-powered IoT has more regulations that must be set to ensure that these long-lasting devices are not collecting data for malicious intent and without a consumers' consent/knowledge. This requires employing foresight, which falls under the anticipation dimension in responsible innovation, to ensure that structure is in place to protect actors in the self-powered IoT. The technology-task relationship also evolves, as there are new research and development tasks required to advance the self-powered IoT that did not exist when working with just the battery-powered IoT. These specific examples show that the sociotechnical relationships have evolved as the battery-powered IoT shifts towards the self-powered IoT to meet the dimensions of responsible innovation.

To show that the self-powered IoT is affecting positive change in the environment, the technology has been evaluated using the framework for responsible innovation. The anticipation dimension is highlighted by the e-waste problem mentioned by Calhoun and Sylvester. The foresight employed in the innovation of the energy harvesting components of the self-powered IoT helps avoid considerable damage to the environment that was looming due to the mining, manufacturing, and disposal of electronics, including batteries (Lepawsky, 2019). There is no clear evidence of the reflexivity dimension in the self-powered IoT, but I believe that there has been morality in the innovation process for this new technology. Due to the ethical implications that are present in the IoT (e.g. e-waste), innovators in the self-powered IoT, such as Ben Calhoun and Dennis Sylvester, have been making a conscious effort to address those implications. Also, labs and companies that are innovating in this field have codes of conduct that are enforced by larger organizations, such as the Institute of Electrical and Electronics Engineers (IEEE), that ensure that morals and external values are connected to the innovations. The inclusion dimension is present in this field through the presentation of advancements in the self-powered IoT in college curriculums and technical conferences.

College coursework allows students to learn about the technology and become more involved in the practice of innovation. Presentations and publication at technical conferences allow for stakeholders and the wider public to be exposed to the newest technologies that are at the forefront of the self-powered IoT. Finally, the responsiveness dimension is demonstrated by the more recent commercialization of self-powered systems. Starting with just replacing a battery with an energy harvesting unit, innovation in the self-powered IoT has been able to pivot in many different directions when the needs and inputs of the stakeholders have been presented. The ability for this innovation to pivot has paved the way for companies like Everactive to be

able to innovate and build specialized systems that are unique to their stakeholders' desires. As all four dimensions are present in the research and development of self-powered IoT, this technology can be considered a responsible innovation, at this time.

This research was limited by the number of interviews that were able to be conducted. The self-powered IoT is a relatively new field, so the number of experts in the field are a bit numbered. I was also only able to interview people that I have a professional relationship with. Due to the coronavirus pandemic, interviewing other experts in the field and conducting follow-up interviews proved to be a challenge because of the dramatic schedule and workload changes that resulted. Some experts that I believe would be able to provide valuable information about the self-powered IoT are Patrick Mercier at the University of California San Diego, Joshua Smith at the University of Washington, and Anantha Chandrakasan at the Massachusetts Institute of Technology. I believe that having more interviews would strengthen the conclusions that were made in my research, and potentially even introduce new implications that my interviewees did not address.

In the future, I would definitely conduct more interviews, present more specific case studies of commercial IoT security breaches, and survey consumers of the IoT. I would survey consumers first to see what they think the biggest ethical risks of implementing the IoT in their lives would be. Using these survey results, I would ask more focused questions to my interviewees and see how they are addressing those risks. Finally, case studies would be used to provide more evidence of ethical problems that have been demonstrated in commercial IoT products.

I plan on focusing on the self-powered IoT as I pursue my PhD, so this research informed me of the technological and ethical shortcomings of the field. I will use the knowledge I gained through this work to inform the research I choose to conduct in graduate school. If I work with other technology, I will use the techniques employed in this research to provide myself with the sociotechnical depth that is necessary to ethically innovate.

Conclusion

This research presents the reasoning behind the shift towards the self-powered IoT and the ethical implications that are associated with this shift. The battery-powered IoT's growth will slowly hit a plateau, due to the shortcomings inherent in batteries. This is why the self-powered IoT has started becoming such a prominent solution. One of the most positive ethical implications of the self-powered IoT is the reduction of electronic waste, due to the removal of mining, manufacturing, and disposal of batteries that is associated with the battery-powered IoT. Due to self-powered systems being powered by the environment, there is a relatively strict power budget that is introduced. Even with a power budget, the self-powered IoT is able to provide the same level of security as the battery-powered IoT.

This does not mean that the self-powered IoT is safe from security and privacy issues. The self-powered IoT inherits many of the security and privacy concerns that are associated with the standard IoT, and even amplifies some of them. One of the biggest concerns is the idea of maliciously leaving a self-powered node in a place that can last for a long time and can be small enough to be undetectable to collect unwanted data on people. The next steps of this work are to monitor the growth the self-powered IoT in academia and industry and observe the ethical issues that are brought to the public's attention. This work has shown that the self-powered IoT is

necessary for the growth of the IoT, but there are still ethical implications in the IoT that have not been solved.

References

Aspencore Network (2019, May 2). Battery-less IoT could soon be a reality with Bluetooth multi-sensor platform – IoT Times. Retrieved October 30, 2019, from https://iot.eetimes.com/battery-less-iot-could-soon-be-a-reality-with-bluetooth-multi-sensor-platform/

ASSIST. (2020). *Home—Center for Advanced Self-Powered Systems of Integrated Sensors and Technologies (ASSIST)*. Retrieved April 3, 2020, from https://assistcenter.org/

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Bera, A. (2019, February 25). 80 IoT Statistics for 2019 (Infographic). Retrieved September 22, 2019, from SafeAtLast.co website: https://safeatlast.co/blog/iot-statistics/

Calhoun, B (2019). ECE 6501: Self-Powered Systems, Virginia, VA

Chen, G. et al. (2010). Millimeter-scale nearly perpetual sensor system with stacked battery and solar cells. *2010 IEEE International Solid-State Circuits Conference - (ISSCC)*, 288-289. https://ieeexplore.ieee.org/abstract/document/5433921

Cox, J. (2019, December 17). We Tested Ring's Security. It's Awful. *Vice*. https://www.vice.com/en_us/article/epg4xm/amazon-ring-camera-security

Dutton, W. H. (2014). Putting things to work: Social and policy challenges for the Internet of Things. Info, *16*(3), 1-21. https://doi.org/10.1108/info-09-2013-0047

Feki, M. A., Kawsar, F., Boussard, M., & Trappeniers, L. (2013). The Internet of Things: The Next Technological Revolution. *Computer*, *46*(2), 24–25. https://doi.org/10.1109/MC.2013.63

Ghaffari, K., Lagzian, M., Kazemi, M., & Malekzadeh, G. (2019). A socio-technical analysis of IoT development: An interplay of technologies, tasks, structures and actors. *Foresight*, 21(6), 640-653. https://doi.org/10.1108/FS-05-2019-0037

Glynne-Jones, P., & White, N. M. (2001). Self-powered systems: A review of energy sources. *Sensor Review, 21*(2), 91-97 https://doi.org/10.1108/02602280110388252

Lepawsky, J. (2019, November 8). *Our Tech Addiction Is Creating a 'Toxic Soup.'* Medium. https://onezero.medium.com/our-tech-addiction-is-creating-a-toxic-soup-fdeb36bdcc51

Tom Tom. (2014, December 28). *Dr. Benton Calhoun, Cofounder of PsiKick*. https://www.cvilletomorrow.org/articles/dr-benton-calhoun-cofounder-of-psikick

Schaumont, P. (2017). Security in the Internet of Things: A challenge of scale. *Design, Automation Test in Europe Conference Exhibition vol*, 674–679. https://doi.org/10.23919/DATE.2017.7927075

Shin, D. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the IoT. *Telematics and Informatics*, *31*(4), 519–531. https://doi.org/10.1016/j.tele.2014.02.003

Murmson, S. (2017, April 25). *The Average Photovoltaic System Efficiency*. Sciencing. https://sciencing.com/average-photovoltaic-system-efficiency-7092.html

Sanders, J. (2018, December 17). *5 biggest IoT security failures of 2018—TechRepublic*. TechRepublic. https://www.techrepublic.com/article/5-biggest-iot-security-failures-of-2018/

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy, 42*(9), 1568–1580. https://doi.org/10.1016/j.respol.2013.05.008

Vigdor, N. (2019, December 15). Somebody's Watching: Hackers Breach Ring Home Security Cameras. *The New York Times*. https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html

Wang, Z. L. (2010). Towards self-powered sensor networks. *Nano Today, 5(6), 512-514.* https://doi.org/10.1016/j.nantod.2010.09.001

Whittaker, Z. (2018, May 14). *US cell carriers are selling access to your real-time phone location data*. ZDNet. https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/

Zhang, Y. et al. (2013). A Batteryless 19 uW MICS/ISM-Band Energy Harvesting Body Sensor Node SoC for ExG Applications. *IEEE Journal of Solid-State Circuits, 48(1), 199-213.* https://ieeexplore.ieee.org/abstract/document/6399579