INTERNET OF RISKY THINGS:
INVESTIGATING THE SOCIAL CONSTRUCTION OF IOT DEVICES

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

By

John Chrosniak

March 28, 2022

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
Catherine D. Baritaud, Department of Engineering and Society

Internet of Things (IoT) devices have continuously grown in popularity throughout the past decade. These devices, often embedded in everyday objects, can collect data through various sensors to wirelessly display data to the user and perform physical actions that benefit the user. Digital assistants, remote-access surveillance systems, and other smart-home technologies such as Amazon Alexa and Ring doorbell have quickly become common household accessories. According to Kumar et al. (2019), a team of researchers studying the societal and technical impacts of IoT devices, 40.2% of households worldwide have at least one IoT device, with 71.8% of households in North America and 57.2% in Western Europe falling under that category (p. 7). Projections also indicate that the market for IoT devices will continue to grow rapidly over the coming years, with an anticipated threefold increase in the worldwide number of IoT devices from 2018 to 2023 (Dahlqvist et al., 2019). While these devices have immense potential for improving consumers' quality of life and optimizing industrial processes, IoT devices also face many barriers that hinder widespread adoption.

Privacy concerns have been a prominent issue surrounding IoT systems. Devices are typically located within a personal residence or worn by the user, collecting data from the surrounding environment using various sensors. Given that these devices simultaneously connect to the internet, it leaves the possibility for unwanted personnel to gain access to private information such as video footage and medical records. Second, shortcomings in security have also inhibited the adoption of IoT devices. The internet was intentionally designed to require that applications implement all the necessary security features, yet many released IoT products have been found to not have acceptable measures to protect themselves from malicious agents, inherently putting consumers at risk. Third, IoT devices typically operate as a "black box," hiding the internal processes and explanations behind decisions from consumers. This lack of

transparency can appear concerning to users, as humans generally hesitate to use technology they do not understand. Finally, IoT devices operate in constantly changing environments. When combined with the possibility of internet outages, sensor failures, and loss of wireless connectivity, reliability emerges as another concern for consumers.

Although these issues differ in the concerns they provide consumers, they all share a common impact that limits the adoption of IoT devices: damages in consumer trust. Users will not trust a device that violates their privacy, poses an unacceptable risk of harm, hides detailed innerworkings, or fails to meet performance expectations. This research project aims to address the adoption concerns of IoT devices through both a technical and human factors perspective, motivated by the need for more trustworthy technology. The technical project, under the guidance of Professor Harry Powell and accompanied by Arthur Given, Derek Martin, and Jamison Stevens, focuses on developing an IoT home security system that allows homeowners to manage temporary access to their residence and view surveillance footage of guests entering and exiting. The tightly coupled sociotechnical project analyzes the current obstacles that restrict the adoption of IoT devices and how these obstacles impact consumer trust using the Social Construction of Technology framework founded by Bijker and Pinch (1984). The framework evaluates how "social groups" shape the development of a technology over time, viewing technological development as an iterative process that continuously adapts to meet societal expectations. In the context of the Internet of Things, these social groups consist of device manufacturers, device consumers, regulatory bodies, and academic researchers. This paper focuses on synthesizing consumer studies and news reports noting the issues of IoT devices with proposed legislation and academic research that provide potential solutions to investigate the beginning of the social construction of IoT devices.

ADOPTION CONCERNS OF IOT DEVICES

Failure to design a product that aligns with the wants and needs of consumers is often the largest source of failure of a technological innovation. The recent explosion in consumer and industry oriented IoT devices has led to a rapid and constantly increasing diffusion of these new technologies. This rapid spread, however, has raised concerns related to the unexplored sociotechnical impacts of IoT devices that will affect the current use and future shaping of the technology. Although there are a wide variety of sociotechnical issues associated with these devices, this paper will focus on privacy, security, transparency, and reliability concerns associated with the Internet of Things.

DEFINITIONS

In order to analyze the shortcomings of a device, proper metrics must be established to specify what exactly the device lacks. As such, the paper will use the following definitions when discussing the issues with IoT devices:

- Privacy: the extent to which a device protects users from observation through sensors and personal data.
- Security: the extent to which a device protects users against malware or other harmful actors
- Transparency: the extent to which a device explains its internal processes and the decisions behind any actions made
- Reliability: the extent to which a device operates according to its specified performance

LACK OF CONSUMER TRUST

Consumers arguably have the most influence on the social construction of a technological device. Therefore, engineers must thoroughly consider the desires of their targeted consumer group throughout the design process if they wish for consumers to adopt their technology. Although IoT manufacturers have developed products to provide meaningful services for consumers, many unanticipated and ignored issues have caused decreases in consumer trust and device adoption rates. These issues, discussed more below, present the first iteration of feedback for IoT manufacturers to consider during future development.

PRIVACY VIOLATIONS

Digital invasions of privacy have been a consistent fear of consumers since the introduction of the internet. IoT devices further worsen this fear through the introduction of various sensors that collect and store consumers' personal information while connected to their personal wireless network. Although many device manufacturers assure their products do not harvest unauthorized data, some consumers remain hesitant. For example, Lau et al. (2018), a team of researchers studying IoT adoption at the University of Michigan, conducted a series of in-depth interviews with users and non-users of the Amazon Alexa digital assistant. They found that privacy concerns acted as a major deterrent for adopting the digital assistant, as consumers feared that the microphone would allow Amazon or another malicious actor to "listen in on their homes" (p. 10). Ponciano et al. (2017), researchers at the Federal University of Campina Grander studying human-computer interaction, reached similar conclusions from their case study examining consumers' perceptions of privacy within IoT devices. The authors cited data collection, inference of detailed personal information, and the exchange of information with third parties as the primary sources of privacy concerns.

Many of these fears stem from recent news releases related to the deceptive data collection and handling practices from device manufacturers. Chen (2021), the lead consumer technology writer for The New York Times, discusses how technology giants such as Facebook and Google have been collecting consumers' personal data without direct consent in hopes of providing more targeted advertisements within their applications. These practices have severely damaged consumer trust in IoT manufacturers and thus limited the adoption of the technologies they produce. In addition to sacrificing their privacy to corporations, consumers also fear IoT systems sacrifice their privacy, and potentially safety, to hackers and other malicious agents.

SECURITY VULNERABILITIES

Security continues to be a pervasive issue, as many potential sources of failure exist within IoT devices that could allow malicious agents unauthorized access to sensitive data or the behavior mechanisms of the device. On top of the existing concerns associated with sensor networks and the internet, a whole new set of concerns arise when combined with the issues of privacy protection, access control rights, and information storage (Zhao & Ge, 2013, p. 1). Mendez et al. (2018), researchers at Purdue University studying information security in IoT devices, analyze the various sources of security vulnerabilities that arise from this combination. They investigate the standard three-layer architecture of IoT systems, shown in Figure 1 on page 6. The perception layer contains various sensors and actuators used to collect information from the surrounding environment, which the device then uses to influence its operation. Following data collection, the network layer transmits any necessary information from the device to a remote server through the internet. The user can then view any relevant information and interact with their device through the application layer, which may send messages back to the device through the network layer.

The authors discuss how engineers have designed the protocols used in each layer to require fewer computing resources to accommodate for the smaller processors onboard IoT devices. As a result, many of these protocols lack in-depth security measures to enforce proper authentication, authorization, and encryption of data. Other security issues stem from the rate of growth within the industry. According to Alladi et al. (2020), a team of researchers studying the intersection between IoT devices and network security, some companies have chosen to "compromise on security measures to keep pace with market needs" (p. 1).

The severity of these issues will continue to grow as more consumers and industries begin to adopt IoT devices. Kozlov et al. (2012), a team of information technology researchers at the University of Jyväskylä, describe many new use cases of IoT devices in various industries, most notably healthcare, banking, and home security. They discuss how these new use cases present the added risk of processing and storing highly sensitive data (pp. 3-4). Some devices not only leave the opportunity for hackers to access data, but to control the operation of the physical device as well. For example, the Federal Drug Administration (FDA) discovered that cardiac devices produced by St. Jude Medical in 2016 had vulnerabilities that let hackers remotely control the device (Larson, 2017). According to Larson,

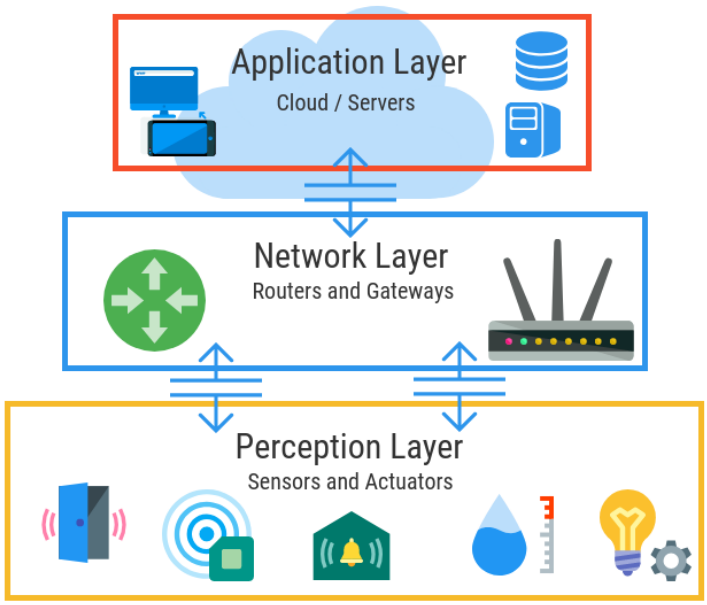

Figure 1. The three-layer architecture of IoT devices, consisting of the perception, network, and application layers (Cahilman, 2019).

studies found that hackers could potentially “deplete the battery or administer incorrect pacing or shocks” (para. 1). Although no patients were harmed as a result of this security failure, ensuring that devices can protect users from malicious agents remains an essential task to mitigating potentially disastrous issues. Despite these needs, the research into developing IoT devices has significantly outpaced the research into securing them. As seen in Figure 2, there were approximately six times more publications related to the development of IoT than publications related to IoT security from 2014 to 2016 (Mendez et al., 2018). To further complicate matters, many consumers remain unaware of these issues due to manufacturers hiding the risks associated with their devices.

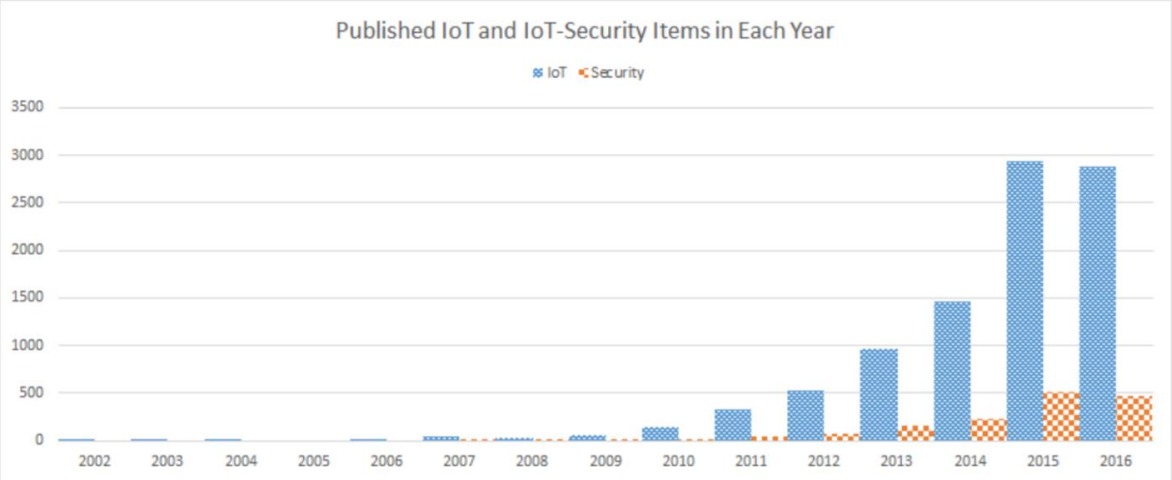

Figure 2. Published IoT and IoT-Security Items in Each Year: Research in the area of IoT security has not matched the growth of research in the field, raising concerns for the security of present and future devices (Mendez et. al, 2018).

TRANSPARENCY SHORTCOMINGS

IoT device manufacturers have a poor reputation for abstracting all information detailing how their device works away from the user. This knowledge gap has been observed to create a trust barrier between devices and humans, decreasing the likelihood consumers will adopt certain devices (Kounelis et al., 2014). Humans have evolved to seek an understanding of their

surroundings, which explains why the black-box structure associated with the Internet of Things can appear frightening to some. Additionally, many IoT devices deploy machine and deep learning algorithms to assist with their daily operation. Although these algorithms can surpass human-level performance in a variety of tasks, the complex representations of data they learn cannot be easily explained to humans. Doshi-Velez & Kim (2017), computer scientists researching the ethics of machine learning, emphasize the interpretability shortcomings with classic machine and deep learning algorithms. The authors stress that a variety of ethical issues can arise from deploying these models in a real-world environment, as there is no guarantee that they will operate safely or without forms of discrimination.

In conjunction with the lack of explanations of device innerworkings is the lack of clarity companies provide regarding the risks associated with their devices. The majority of IoT users have little technical understanding of the risks they accept when agreeing to the terms and conditions of a device, assuming they even read these conditions. This issue is complicated further by the addition of the sensitive information that devices may collect from users, as is commonly seen in the healthcare industry. According to O'Connor et al. (2017), a team of researchers investigating information technology in healthcare settings, IoT devices need to provide users with the "information they need to make informed choices" (p. 2). Without this information, users cannot provide informed consent to the activities performed by their device. Finally, IoT devices suffer further distrust from consumers due to notable performance inconsistencies.

RELIABILITY CONCERNS

IoT systems suffer from reliability issues due to the inherent instability in their environment and the resources they depend upon. Unreliable service and resource constraints

often inhibit the reliability of IoT devices (Li et al., 2012). Devices are expected to function in a variety of changing environments while maintaining a consistent wireless connection to the internet. Hardware failures have also been a frequent occurrence, as the small, embedded computers within devices have low computational capacity and memory, limiting their performance capabilities. Moore et al. (2020) argue that these issues also factor into the reliability of a device's application layer when "anomalous data is sent from the device through the network into the application layer" (p. 153). Devices do not commonly have resources dedicated to detecting these anomalies, which can in turn cause unexpected and unintended behavior. These potential sources of device failure further contribute to the loss of trust between consumers and IoT devices and will need solutions to increase consumer adoption rates. Governmental organizations often provide another source of influence on the construction of technology, but there has been a notable absence of regulation on the technology used in the Internet of Things.

LACK OF REGULATIONS

Another source of issues related to the shortcomings of IoT devices stems from minimal regulatory oversight on device manufacturers. In his article "Ro Khanna says Congress has failed to regulate the tech industry. He's offering a path forward," Cristiano Lima summarizes a conversation he had with Congressman Ro Khanna (D-Calif.) regarding the lack of accountability technology companies face (2022). Large technology corporations have been under severe public scrutiny lately due to their increasingly prominent anti-competitive practices and lack of clarity regarding the usage of consumers' personal data. Although many congressional hearings have been held with these companies, very few changes in legislation have occurred. Rep. Khanna cites the "technological illiteracy" of Congress as the main reason

for this lack of legislation (Lima, 2022, para. 3). He argues that without a concrete understanding of the technology that needs regulation and the implications behind its use, Congress will struggle to create impactful legislation that addresses the necessary problems.

SOCIAL CONSTRUCTION OF IOT DEVICES

The issues mentioned in the previous section have already begun creating new areas of research dedicated to designing more trustworthy IoT devices. This section will explore the current research within these areas and regulatory actions that highlight the beginning of the iterative social construction of IoT devices.

DESIGNING FOR TRUST

Trust is not a physical trait that can be built into a system. Thus, IoT developers have varying perspectives on how to design a trustworthy system. Kounelis et al. (2014) propose that trust between humans and computers is best established through "agency, namely the individual ability to intervene and tailor the system" (p. 74). The authors discuss how agency should be embedded within IoT systems by empowering users with choices on how and to what extent the system performs its role. This can range from controlling how the device stores and shares personal data to prohibiting the device from executing certain actions. The authors argue that granting the user customizable control over the device opens the black box of the devices innerworkings, establishing a relationship of trust.

Related to improving device transparency, a new research area has emerged dedicated to providing explanations behind the predictions of machine and deep learning models. Many interpretation methods have evolved in recent years to generate predictions for a variety of machine and deep learning models, such as models that use language or images as inputs (Du et al., 2019). For example, an explanation for a model's reasoning when classifying the sentiment

of a sentence is displayed in Figure 3. The explanation uses sentence fragmentation and color to help the viewer diagnose the reason behind the model classifying the input sentence to have a negative connotation. These techniques have demonstrated strong capabilities for offering explanations behind decisions made by artificial neural networks to end users. Detailed explanations of machine learning models provide benefits for both consumers and developers. Consumers can better understand how their devices work, leading to more established trust, while developers can use these explanations to identify any deficiencies or biases in their models to promote security and fairness.

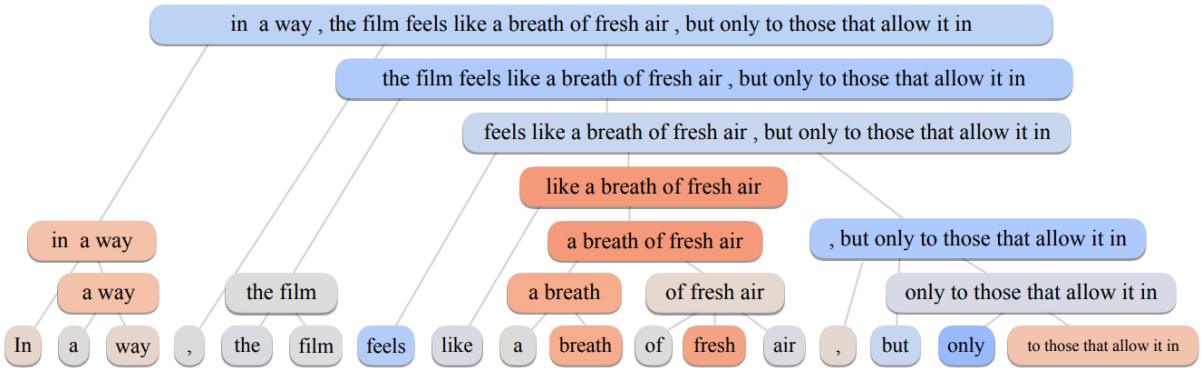

Figure 3. A hierarchical explanation generated to explain a model's reasoning behind classifying the sentiment of a sentence. Blue indicates a negative connotation while red indicates positive (Jin et al., 2019).

Threat detection has been another growing research area due to its promise in identifying security breaches early to minimize the potential effects of a cyberattack. For example, Boncea and Bacivarov (2016) propose a new system architecture for IoT devices that logs any notable security concerns for easy diagnostics and early threat detection. Their framework provides users with helpful insights on the security of their devices and reassurance that the device has the best interest of the user in mind. Researchers have also investigated a variety of ways to increase the performance capabilities of IoT devices. Alam (2018) presented a communication framework designed to better handle the intermittent connectivity of IoT devices, increasing reliability in

unreliable conditions. Although aimed at addressing the known technical issues with IoT devices, these methods work towards developing more trustworthy devices that will likely experience higher rates of adoption from consumers.

REGULATORY INVOLVEMENT

Legislation regulating technology companies has been slow to pass, but recent landmark laws passed in Europe and California show promising measures governments have taken to protect consumers. The General Data Protection Regulation, passed by the European Union in 2016, offers an insight into what future legislation on technology firms may look like (Regulation 2016/679). The bill provides a list of rights to protect individuals from unethical practices related to their data, as well as a series of responsibilities and liabilities of corporations accompanied by penalties should these not be met. Technologists, such as Goodman and Flaxman, agree that this legislation will create many new challenges for engineers, but see it as "good problems to have" (2016, p. 7).

Although no legislation has yet been passed at the federal level in the United States, the California Consumer Privacy Act (CCPA) passed in 2018 guarantees consumers extensive data protection rights (California Consumer Privacy Act, 2018). This includes the right to know all personal information a company collects, delete any personal information collected, and opt-out of the sale of information. In response to this act, Apple announced new privacy features built into their devices that block applications from collecting personal information without the explicit consent of the user (Chen, 2020). Other companies will need to enact similar protections if they plan on doing business in California, and eventually this will expand to the United States if Congress passes the expected legislation.

SUMMARY OF WORK

No matter the application, every technology will have an impact beyond its intended use. It is therefore imperative that engineers continue to assess and monitor the impacts that their designs have on the world around them. The rapid diffusion of IoT devices has proven to be a challenge for engineers, as there has not been an adequate period of iterative testing before the Internet of Things reached a global scale.

Through the lens of the SCOT framework, this research paper has analyzed four of the major adoption concerns IoT devices face from a sociotechnical perspective and how these concerns have impacted IoT development. Figure 4 depicts the iterative feedback loop discussed throughout the paper. The process starts with IoT manufacturers introducing new devices for consumers to use. Consumers have then voiced their concerns with using these devices, identifying privacy, security, transparency, and reliability as inhibitors of trust. In response to

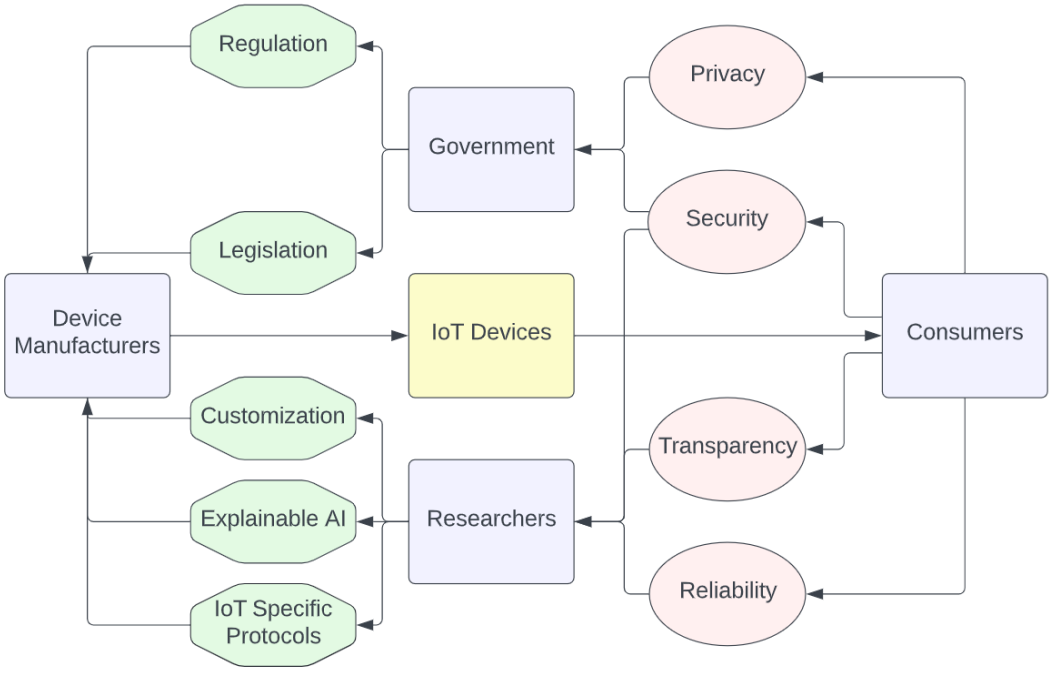

Figure 4. The social construction of IoT devices: The interaction between social groups (purple), problems (red), solutions (green), and artifacts (yellow) in the context of the Internet of Things (Chrosniak, 2022).

consumer concerns, governmental bodies and academic researchers have worked to develop solutions through regulation and new technological developments. IoT manufacturers will soon start to incorporate this feedback into the design of new devices to reiterate through the social construction process, moving towards more capable and trustworthy technology.

FUTURE RESEARCH

Another sociotechnical issue surrounding IoT devices that this paper did not explore is access to devices. High costs, for example, reserve the benefits of the Internet of Things for those with a higher socioeconomic status. Areas of lower income are also less likely to have reliable access to the internet, further preventing them from reaping the benefits of IoT systems. Political factors have also prevented access to the services of IoT devices, as some countries limit the internet services of their residents. While this paper touched upon the social dilemmas and recent change in the design approaches of the Internet of Things, future research into the fairness of device access will provide a more holistic picture of the sociotechnical impact of the Internet of Things.

REFERENCES

Alam, T. (2018). A reliable communication framework and its use in Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*, 8.

Alladi, T., Chamola, V., Sikdar, B., & Choo, K.-K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, *9*(2), 17–25. https://doi.org/10.1109/MCE.2019.2953740

Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and perceptions of IoT security in critical societal services. *IEEE Access*, *4*, 2130–2138. https://doi.org/10.1109/ACCESS.2016.2560919

Bijker, W. E., & Pinch, T. J. (1984). The social construction of facts and artifacts. *Social Studies of Science*, 14, 399–441. https://doi.org/10.1177/030631284014003004

Boncea, R., & Bacivarov, R. (2016). A system architecture for monitoring the reliability of IoT. *Proceedings of the 15th International Conference on Quality and Dependability*, 143–150. https://www.researchgate.net/publication/309040744

California Consumer Privacy Act, Cal. Assemb. B. 375 (2017-2018), Chapter 55 (Cal. Stat. 2018).

Calihman, A. (2019, January 30). Architectures in the IoT civilization. *NetBurner*. https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/

Chen, B. X. (2021, September 16). The battle for digital privacy is reshaping the internet. *The New York Times*. https://www.nytimes.com/2021/09/16/technology/digital-privacy.html

Chen, B. X. (2020, June 23). Apple announces new privacy features. *The New York Times*. https://www.nytimes.com/2020/06/23/technology/apple-announces-new-privacy-features.html

Chrosniak, J. (2022). *The social construction of IoT devices.* [Figure 4] *STS Research Paper:* Internet of risky things: Investigating the social construction of IoT devices (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *ArXiv:1702.08608 [Cs, Stat]*. http://arxiv.org/abs/1702.08608

Du, M., Liu, N., & Hu, X. (2019). Techniques for interpretable machine learning. *Communications of the ACM*, *63*(1), 68–77. https://doi.org/10.1145/3359786

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation." *AI Magazine*, *38*(3), 50–57. https://doi.org/10.1609/aimag.v38i3.2741

Jin, X., Wei, Z., Du, J., Xue, X., & Ren, X. (2019). Towards hierarchical importance attribution: Explaining compositional semantics for neural sequence models [Figure 3]. *ArXiv:1911.06194 [Cs, Stat]*. http://arxiv.org/abs/1911.06194

Kounelis, I., Baldini, G., Neisse, R., Steri, G., Tallacchini, M., & Guimaraes Pereira, A. (2014). Building trust in the human-Internet of Things relationship. *IEEE Technology and Society Magazine*, *33*(4), 73–80. https://doi.org/10.1109/MTS.2014.2364020

Kozlov, D., Veijalainen, J., & Yasir, A. (2012). Security and privacy threats in IoT architectures. *Proceedings of the 7th International Conference on Body Area Networks*. 7th International Conference on Body Area Networks, Oslo, Norway. https://doi.org/10.4108/icst.bodynets.2012.250550

Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R., & Durumeric, Z. (2019). All things considered: An analysis of IoT devices on home networks. 1169–1185. https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak

Larson, S. (2017, January 9). FDA confirms that St. Jude's cardiac devices can be hacked. *CNNMoney*. https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/index.html

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 102:1-102:31. https://doi.org/10.1145/3274371

Li, L., Jin, Z., Li, G., Zheng, L., & Wei, Q. (2012). Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach. *2012 IEEE 19th International Conference on Web Services*, 584–591. https://doi.org/10.1109/ICWS.2012.25

Lima, C. (2022, January 28). Ro Khanna says Congress has failed to regulate the tech industry: He's offering a path forward. *Washington Post*. https://www.washingtonpost.com/politics/2022/01/28/ro-khanna-says-congress-has-failed-regulate-tech-industry-he-offering-path-forward/

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, *2*(2), 12:1-12:25. https://doi.org/10.1145/1985347.1985353

Mendez, D. M., Papapanagiotou, I., & Yang, B. (2018). Internet of Things: Survey on security and privacy. *Information Security Journal: A Global Perspective*, *27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258

Moore, S. J., Nugent, C. D., Zhang, S., & Cleland, I. (2020). IoT reliability: A review leading to 5 key research directions. *CCF Transactions on Pervasive Computing and Interaction*, *2*(3), 147–163. https://doi.org/10.1007/s42486-020-00037-z

O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by design: Informed consent and Internet of Things for smart health. *Procedia Computer Science*, *113*, 653–658. https://doi.org/10.1016/j.procs.2017.08.329

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the Internet of Things era. *IT Professional*, *17*(3), 32–39. https://doi.org/10.1109/MITP.2015.34

Ponciano, L., Barbosa, P., Brasileiro, F., Brito, A., & Andrade, N. (2017). Designing for pragmatists and fundamentalists: Privacy concerns and attitudes on the Internet of Things. *Proceedings of the XVI Brazilian Symposium on Human Factors in Computing Systems*, 1–10. https://doi.org/10.1145/3160504.3160545

Regulation 2016/679. *General Data Protection Regulation*. European Parliament, Council of the European Union. https://gdpr.eu/

Zhao, K., & Ge, L. (2013). A survey on the Internet of Things security. *2013 Ninth International Conference on Computational Intelligence and Security*, 663–667. https://doi.org/10.1109/CIS.2013.145