Empowerment of Users: Privacy and Security Implications of Smart Devices

A Research Paper submitted to the Department of Engineering and Society

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

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

Beatrice E. Li

Spring, 2021

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 __________
Beatrice E. Li, Department of Engineering Systems and Environment

Approved ____ Date __________
Sean Ferguson, Department of Engineering and Society

Not only do public Wi-Fi networks number to hundreds of millions today, but they are projected to grow even more along with the number of Internet of Things (IoT) connections in the coming years (*Cisco Annual Internet Report*, 2020). Internet of Things (IoT) refers to the network of connected devices that communicate with each other through a cloud network while being connected to the Internet (Began, 2020). The most well-known IoT devices include the Amazon Echo and smart locks; however, the device that people are most familiar with, the smartphone, is generally not considered an IoT device since they are directly connected to the Internet. Despite the differences, the interactions with a smartphone have very similar privacy, and security concerns as other IoT devices like the Amazon Echo, as many smartphones also happen to be powered by a smart assistant. Amazon, the company behind the most popular smart speaker – Amazon Echo, reported in 2019 that they have sold over 100 million devices powered by their virtual assistant AI, Alexa (Bohn, 2019). With the development and rise in popularity of IoT devices, there is also a growth in privacy and security concerns. People, from Generation X to Gen Z, are connected to their devices more than ever before, especially as technology usage has seen a surge during the COVID-19 pandemic as people find themselves unable to attend in-person events and stay at home more than usual (Vargo et al., 2021). Smart devices have become so integrated with people's lives to the extent to which phones contain almost everything there is to know about a person and perhaps even more. Users tend to perceive themselves as safer than they are in reality, or there is at least a "general willingness to accept risk in lieu of perceived benefit" (Haney et al., 2020; Malkin et al., 2019). The ways consumers interact with devices and networks illustrates the undue trust they place in companies that do not always have their best interests in mind. Consumers need to be educated and equipped with the tools necessary to engage in more informed decision-making regarding the devices and networks they choose to interact with. This paper then explores various types of human-technology interaction before proposing a transparency scorecard as one viable option for consumer education and empowerment.

Research Question and Methods

This research paper considers the importance of educating consumers to care about privacy and security. In getting users to care, the question will then become how can users ensure their privacy and security in the devices and networks they choose to engage with? This paper discusses the knowledge that users should have along with the delivery methods for that knowledge and the guidelines upon which companies should design for, with respect to helping consumers have privacy and security. The methods for this paper will utilize a literature review and policy analysis. The compilation of secondary sources will be based on the following list of keywords: Internet of Things (IoT), cybersecurity, Wi-Fi, security, user awareness, data protection, and risk. The list of keywords is used as they are closely associated with the topic of the question. The literature will include research into user behavior and the security risk associated with the different networks and devices. The use of the literature review will provide context and clarity of the technical concepts. The compilation of literature bridges gaps that may be present in some of the research. Policy analysis will fall under the literature review as the sources will include a discussion of methods to educate users on how to ensure their own privacy and security. The methods utilized will address the complexities of user engagement with networks and smart devices and the impact of public understanding in pursuance of the research question.

This paper explores the much broader question of privacy and security of digital lives by focusing on user and technological device interaction. Given the nature of open networks and smart devices, Actor-Network Theory (ANT) will be used in addressing the topic as it aids in understanding complex relationships. The theory is instrumental in its application to open networks compared to other sociotechnical approaches as it considers both human and non-human actors equally (Cressman, 2009). The consideration of non-human actors is valuable, but that is also the basis of several criticisms in that non-human actors should not be considered of equal importance to human actors as it also may not always be the case. Actor-Network Theory focuses on the study of the associations between actors by also working to define the actors within the system without assuming the size of the network (Cressman, 2009). In the study of associations, or relationships, between actors, networks can be assessed in how they can become more robust and which associations add power to the network. However, there is a flaw in that there is no boundary or stopping point of when to stop adding actors to the network. There are more advantages than disadvantages in the application of Actor-Network Theory as the associations between actors can reveal the impact of user knowledge in open networks. The paper will not only examine existing strategies but propose strategies that advocate for a bottom-up, organic approach to combatting the problematics associated with the usage of smart devices. It is not the case that government and policy do not matter, but this paper places an emphasis on the empowerment of users and that users matter.

Part I: Privacy and Security Concerns of Smart Speaker Assistants

Researchers have found that the simple creation of a malicious Amazon link allows bad actors to access the list of installed Alexa skills and voice history (*Amazon Alexa Security Bug*

Allowed Access, 2020). The security screening of the Alexa skills cannot catch every malignant entity, as found in a large-scale analysis of 90,194 unique skills (Lentzsch et al., 2021; Winder, 2021). If researchers can find these flaws and loopholes, what are the chances that malicious actors have also found them? However, attacks are not the only subject of concern but also how companies design their devices. Referring back to the Amazon Echo, the most popular smart speaker in the U.S., Amazon has designed the device with the objective to collect consumer data that will improve their technology – specifically the artificial intelligence of their Amazon Alexa (O'Flaherty, 2019). Many users are unaware that this is a setting they could change due to how deeply it is hidden within the Amazon Alexa App along with other smart speaker assistants (Malkin et al., 2019). Amazon defaults their devices to collect data in the name of developing their AI, which ignores the privacy of users. However, they are definitely not the only company to do so as Apple and Google have similar voice assistants, but the key difference is within their business models (Benjamin, 2020). The ways in which Apple, Google, and Amazon operate, in comparison to each other, reflect their values of security and privacy. The comparison of these companies reflects the notion that some may be willing to help and support users in the process of ensuring their privacy and security. Apple and Google have made headway in helping users ensure some of their privacy, while Amazon seems to run in the opposite direction by also appearing to design means of sharing user data (Benjamin, 2020; Paul, 2019). It is important to note that the Amazon Echo is a device that is integrated into the environment of the user and is always waiting to listen in – or waiting to be called on, the interpretation depends on how much credence one is willing to give these devices – or the companies themselves (Schönherr et al., 2020). The differences between a smart speaker assistant and a smartphone are significant, particularly in the discussion of data on the scale of the user.

Based on Actor-Network Theory, artifacts matter such that the scale and type of the artifact are essential in the evaluation of relationships between users and artifacts. When privacy and security are considered, the magnitude of such depends on the artifacts' characteristics. As reliant as people are on their smartphones, they are not integrated in the same manner as a smart speaker is (Benjamin, 2020). Smart speakers are intertwined with the physical environment of consumers that then tracks behaviors of engagement that a smartphone cannot. There are specific types of data and behavior patterns that are collected, which are primarily dependent on what devices the users are engaging with. At a command, these virtual assistants can turn on lights and lock doors – they can be thought of as an affordable butler for the ordinary citizen that will seemingly cater to the user's every whim (Mahbub, 2020; Wells et al., 2020). When Amazon first introduced the Amazon Echo, the company advertised it as a standalone unit for a single room. However, it was not long before Amazon evolved the Echo network to extend beyond just one room – but to encompass the whole house. Actor-Network Theory is a worthwhile framework in examining the evolution of artifacts as it can look into the evolving relationships between artifact and user. The convivence of trusting simple actions to technology seems remarkable, but nothing great comes without a cost. The cost can be reflected by the level of trust that users associate with technology; it was found in Cisco survey of over 3,000 consumers that while 53% appreciated the convenience that IoT brings to their life, only 9% have a high level of trust that their data collected by IoT is secure (*Cisco Value Trust Paradox Report*, 2017). It would be the logical assumption that if the consumer has low trust in the security of their data, then they would be more willing to keep the IoT devices out of their lives. However, this is not the case, as 42% of the consumers are unwilling to part with IoT devices due to their value – this is termed the IoT paradox (Aggarwal et al., 2020; *Cisco Value Trust Paradox Report*, 2017). It is often the case where users alter their behavior to suit the technological device rather than the other way around. As the artifact constrains user behavior, it brings up an interesting notion put forth by Actor-Network Theory – scripts and counter-scripts. The framework is interested in how the actor behavior is bestowed upon by the artifact, known as scripts (Ritzer, 2004). Even though there are people who value the benefits of having their data used to develop their AI assistant, there are about just as many who feel the opposite. In either case, there are existing strategies that can be used to address privacy and security – ultimately, empower the user.

Part II: Examination of Proposed and Existing Strategies with Actor-Network Theory

In the case where the privacy and security concerns are recognized, it is then necessary to evaluate the interventions for those concerns and develop counter-scripts. Suppose the current dominant script is to privilege the usefulness of these IoT devices and ignoring their risk threats; education is an intervention attempting to produce counter scripts in the users themselves through Actor-Network Theory. Initiatives to push back on the scripts of these artifacts can cover various areas that include advocating for against the use of smart speaker devices, use of the devices that protect their privacy and ensure security, and advocate to the designers of these systems to protect them.

Educational initiatives can spread awareness to get consumers to care about their privacy and security. The prerequisite for any further actions is to get the users to care; otherwise, there would be no consequential actions. An example that most people can recognize is the numerous anti-bullying non-profits partner up with different schools. One such non-profit is called STOMP Out Bullying that has "collaborated with over 15,000 school partners to raise awareness and educate students" and has assisted millions of students, including saving thousands of lives

(*STOMP Out Bullying 2019 Annual Report*, 2019). Schools have multiple reasons for incorporating programs to educate students on matters of cyberbullying and digital literacy. For example, a Massachusetts law prohibits bullying and mandates schools to incorporate age-appropriate instruction on bullying prevention into the curriculum (*General Law - Part I, Title XII, Chapter 71, Section 37O*, n.d.). Like many other anti-bullying non-profits, STOMP Out Bullying establishes tools to educate both students and teachers along with tools that can provide help to students. Preserving in-home security is absent from these interventions for cyber-bullying, which strive to educate students on the permanence of data once it is out on the Internet. The absence of preserving in-home security from the curriculum is problematic as a student's interaction with the device can include the accidental recording of a problematic conversation, and it can be sent out to a random contact (Huang et al., 2020). As schools are already incorporating cyberbullying interventions within the curriculum as part of their own admission against bullying, the addition of education in ensuring privacy and security with smart devices is only logical. The logic stems from acknowledging that schools cannot control student behavior once they leave the school premises. Hence, students need to be empowered to ensure their own privacy and security, and empowerment only comes through with education.

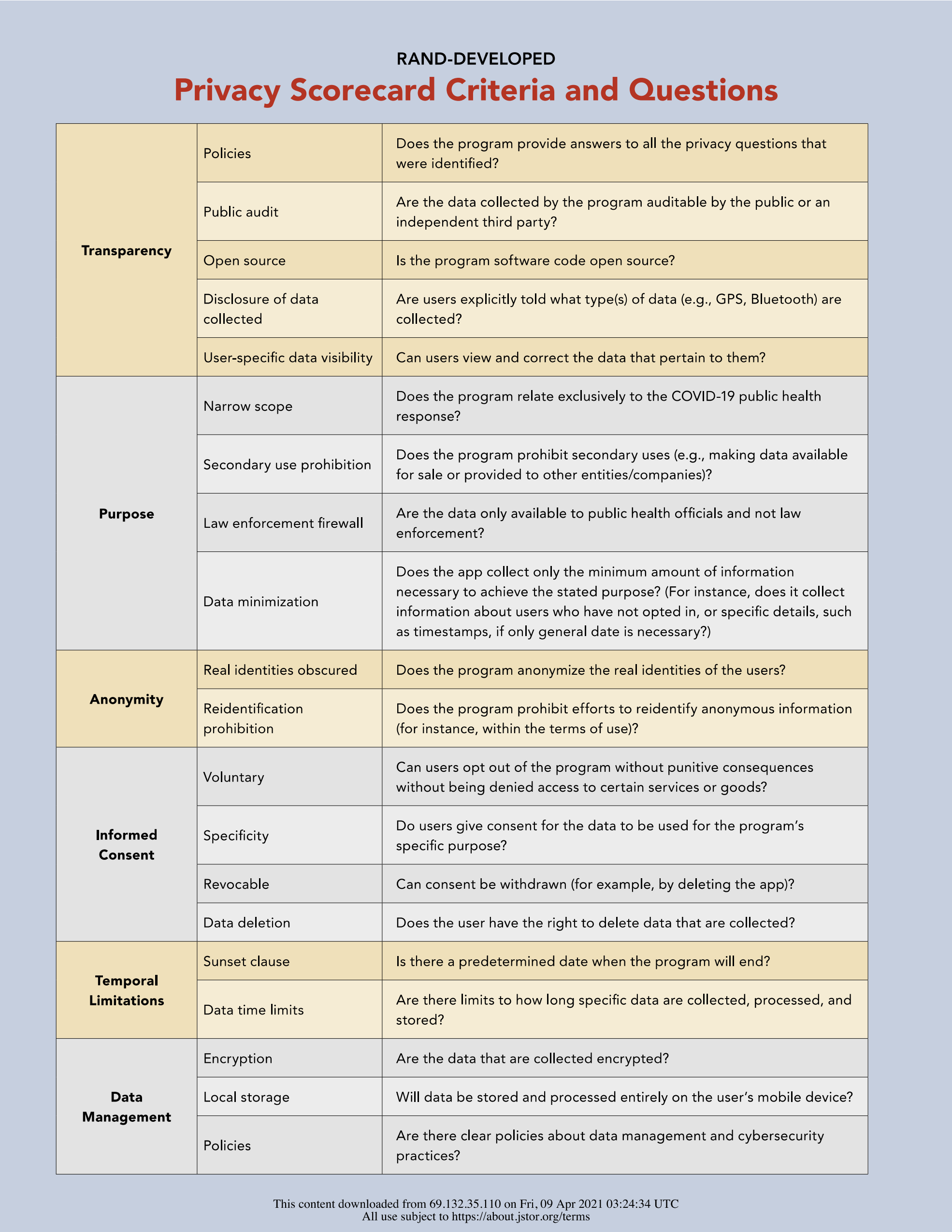
Educational initiatives are one part, but it is essential to discuss industry initiatives. One of the most well-known industry certifications is LEED, Leadership in Energy and Environmental Design. It is a globally recognized certification of sustainability as it provides a framework, a rating system essentially, for healthy, highly efficient, and cost-saving green buildings (*What Is LEED?*, 2021). There is no mandate for buildings to have a LEED certification, but consumers value the sustainability of a building and are more willing to shell out more money (Wilber, 2014). The certification is broken down into four tiers, from lowest to highest: Certified, Silver, Gold, and Platinum – each achieved by meeting a range of points that can be scored with the LEED scorecard. The scorecard is separated into several categories: location and transportation, sustainable sites, water efficiency, energy and atmosphere, materials, and indoor environmental quality. Within each category are items that you can gain points on, which helps to further understand what is being looked at and why. For example, LEED gives points based on the location of the building by basing it off of the proximity to public transit and bicycle facilities ("HOW LEED WORKS," 2011). The framework set forth by LEED can be generalized to that of smart devices such that they hold certifications that indicate how well they handle user data and ensure user privacy and security.

A more recent scorecard that aligns better in the application for technology and smart devices is one that the RAND Corporation developed for COVID-19 contact tracing programs on smartphones. The scorecard aims to strengthen privacy protections by assessing the programs with five categories: transparency, purpose, anonymity, informed consent, temporal limitations, and data management (Boudreaux et al., 2020). The categories are then broken down into various sub-categories with the intent of breaking down privacy policies in terms of data collection for the user in a concise manner (Boudreaux et al., 2020). This scorecard is able to empower users as it allows users to see what privacy protections are in place and in what ways do specific programs meet or do not meet the criteria. However, this scorecard also recognizes the importance of informing users of explanations on privacy trade-offs should there be any – allowing for the people to make an informed decision (Boudreaux et al., 2020). Looking at this artifact through the lenses of Actor-Network Theory, it has the potential to rearrange the network of actors and artifacts, which is what the paper intends to do in the context of users and smart devices.

The discussion of both education and industry initiatives illustrates the impacts of each and their respective advantages. The education initiative will instill awareness in users at a younger age through age-appropriate curriculums. Its effectiveness can be assumed to be similar to that of anti-bullying programs. Meanwhile, the industry initiative of a proposed data transparency scorecard would be effective at reaching users beyond the K-12 education system as it would be included with every device. The semblance of the education and industry initiatives to current symbolically powerful programs, such as anti-bullying and LEED, can prove crucial in establishing these as tools to gain more power over smart IoT devices. The two categories of initiatives will increase accessibility to understanding privacy policies, which would bring more awareness to the concerns over smart IoT devices as well.

Part III: Transparency Scorecard in the Frame of Actor-Network Theory

Actor-Network Theory is an advantageous framework to utilize in reshaping the relationships between artifacts and actors. A transparency scorecard should be adapted from the one previously discussed but for the use of IoT devices. This scorecard is an artifact that can help rearrange the existing network of users, laws, regulations, designers, devices, etc. The existing network or rather, the relationships will be redefined to give more power to the consumers by allowing them to have a better understanding of the devices they choose to engage with. The transparency scorecard for IoT devices will employ the same criteria and sub-criteria used in the privacy scorecard for COVID-19 contact tracing applications. For example, to assess the transparency criteria, questions will be asked pertaining to policies, public audit, open-source, disclosure of data collected, and user-specific data visibility.



RAND-DEVELOPED

Privacy Scorecard Criteria and Questions

Transparency	Policies	Does the program provide answers to all the privacy questions that were identified?
	Public audit	Are the data collected by the program auditable by the public or an independent third party?
	Open source	Is the program software code open source?
	Disclosure of data collected	Are users explicitly told what type(s) of data (e.g., GPS, Bluetooth) are collected?
	User-specific data visibility	Can users view and correct the data that pertain to them?
Purpose	Narrow scope	Does the program relate exclusively to the COVID-19 public health response?
	Secondary use prohibition	Does the program prohibit secondary uses (e.g., making data available for sale or provided to other entities/companies)?
	Law enforcement firewall	Are the data only available to public health officials and not law enforcement?
	Data minimization	Does the app collect only the minimum amount of information necessary to achieve the stated purpose? (For instance, does it collect information about users who have not opted in, or specific details, such as timestamps, if only general date is necessary?)
Anonymity	Real identities obscured	Does the program anonymize the real identities of the users?
	Reidentification prohibition	Does the program prohibit efforts to reidentify anonymous information (for instance, within the terms of use)?
Informed Consent	Voluntary	Can users opt out of the program without punitive consequences without being denied access to certain services or goods?
	Specificity	Do users give consent for the data to be used for the program's specific purpose?
	Revocable	Can consent be withdrawn (for example, by deleting the app)?
	Data deletion	Does the user have the right to delete data that are collected?
Temporal Limitations	Sunset clause	Is there a predetermined date when the program will end?
	Data time limits	Are there limits to how long specific data are collected, processed, and stored?
Data Management	Encryption	Are the data that are collected encrypted?
	Local storage	Will data be stored and processed entirely on the user's mobile device?
	Policies	Are there clear policies about data management and cybersecurity practices?

Figure 1: Privacy Scorecard Criteria and Questions (Boudreaux et al., 2020)

However, to place the RAND scorecard in the context of IoT devices, the proposed scorecard will modify the original questions for each sub-criterion and remove those that are deemed irrelevant from the RAND scorecard. The new questions will succinctly convey information revolving around data collection, data storage and management, and data usage. Each criterion will have a score from 1 (not applicable) to 5 (full satisfaction), which will then accumulate in a tiered certification like LEED. Along that same vein, a third party like the U.S. Green Building Council for LEED should be responsible for issuing the certifications for IoT devices. There are high costs with obtaining a LEED certification, but projects are incentivized to do so by the value it brings. The economic benefits are numerous, as LEED-certified apartment buildings command rents 10.2% higher than non-LEED buildings on average (Browne, 2020). This reflects the growing consumer demand for social responsibility, where people are more willing to pay a premium knowing that it has a positive impact. Similarly, like the U.S. Green Building Council, an organization can incentivize companies to implement the transparency scorecard to increase profits and expand their customer base. In the frame of Actor-Network Theory, the transparency scorecard will empower users to advocate or influence the designers to help users ensure their privacy and security.

Conclusion:

This paper explores the sociotechnical impacts of user interactions with smart devices, specifically exploring the privacy and security implications of using smart devices that determines the behavior of users. Despite the increase in usage of smart devices- such as smart speaker assistants like the Amazon Echo – the majority of users are either unaware or do not place importance on the privacy of their data, especially when considering the added value of the smart devices. The proposed transparency scorecard will lend itself to consumers as a means to decipher the data policies that hide behind complex legal jargon and empower users. Many of today’s smart device users unknowingly consent to invasive data collection. This scorecard will ensure that users can give informed consent.

References

Aggarwal, N., Albert, L. J., Hill, T. R., & Rodan, S. A. (2020). Risk Knowledge and Concern as Influences of Purchase Intention for Internet of Things Devices. *Technology in Society, 62*, 101311. https://doi.org/10.1016/j.techsoc.2020.101311

Amazon Alexa security bug allowed access to voice history. (2020, August 13). BBC News. https://www.bbc.com/news/technology-53770778

Began, K. (2020, May 7). Understanding the Differences: M2M vs. IoT. *IoT For All*. https://www.iotforall.com/m2m-vs-iot-understanding-the-differences

Benjamin, G. (2020, January 20). *Amazon Echo's privacy issues go way beyond voice recordings*. The Conversation. http://theconversation.com/amazon-echos-privacy-issues-go-way-beyond-voice-recordings-130016

Bohn, D. (2019, January 4). *Amazon says 100 million Alexa devices have been sold—What's Next?* The Verge. https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-number-100-million-dave-limp

Boudreaux, B., DeNardo, M., Denton, S. W., Sanchez, R., Feistel, K., & Dayalani, H. (2020). *Strengthening Privacy Protections: In Covid-19 Mobile Phone-Enhanced Surveillance Programs*. RAND Corporation; JSTOR. http://www.jstor.org/stable/resrep25384

Browne, N. (2020). *The Effect of LEED Certification on Residential and Commercial Office Buildings in the District of Columbia in 2018* (p. 18). District of Columbia Government. https://cfo.dc.gov/sites/default/files/dc/sites/ocfo/publication/attachments/LEED%20Certification%20Nyanya%20Browne_July%202020.pdf

Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper. (2020, March 9). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Cisco Value Trust Paradox Report (p. 11). (2017). 104 West. https://www.104west.com/sites/104west.com/files/Cisco%20Value%20Trust%20Paradox%20Report%20FINAL_0.pdf

Cressman, D. (2009). *A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation*. https://collab.its.virginia.edu/access/content/group/6ac8ef1f-6b15-4912-a488-d8c7468046db/Readings/Cressman%20-%20Overview%20of%20ANT.pdf

General Law—Part I, Title XII, Chapter 71, Section 37O. (n.d.). The 192nd General Court of the Commonwealth of Massachusetts. Retrieved April 8, 2021, from https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXII/Chapter71/Section37O

Haney, J. M., Furman, S. M., & Acar, Y. (2020). Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (pp. 393–411). Springer International Publishing. https://doi.org/10.1007/978-3-030-50309-3_26

HOW LEED WORKS. (2011, May 27). *LeadingGREEN*. https://leadinggreen.com/how-leed-works/

Huang, Y., Obada-Obieh, B., & Beznosov, K. (Kosta). (2020). Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376529

Lentzsch, C., Shah, S., Andow, B., Degeling, M., Das, A., & Enck, W. (2021, February 21). *Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem*. https://doi.org/10.14722/ndss.2021.23111

Mahbub, M. (2020). Progressive Researches on Iot Security: An Exhaustive Analysis from the Perspective of Protocols, Vulnerabilities, and Preemptive Architectonics. *Journal of Network and Computer Applications*, *168*, 102761. https://doi.org/10.1016/j.jnca.2020.102761

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S., & Wagner, D. (2019). Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies*, *2019*(4). https://doi.org/10.2478/popets-2019-0068

O'Flaherty, K. (2019, April 12). *Amazon Staff Are Listening To Alexa Conversations—Here's What To Do*. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2019/04/12/amazon-staff-are-listening-to-alexa-conversations-heres-what-to-do/

Paul, K. (2019, August 30). *Amazon's doorbell camera Ring is working with police – and controlling what they say*. The Guardian. http://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor

Ritzer, G. (2004). *Encyclopedia of Social Theory*. SAGE Publications.

Schönherr, L., Golla, M., Eisenhofer, T., Wiele, J., Kolossa, D., & Holz, T. (2020). Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers. *ArXiv:2008.00508 [Cs]*. http://arxiv.org/abs/2008.00508

STOMP Out Bullying 2019 Annual Report (p. 24). (2019). STOMP Out Bullying. https://www.stompoutbullying.org/application/files/9116/1592/8940/STOMPOutBullying-Annual-Report-2019.pdf

Vargo, D., Zhu, L., Benwell, B., & Yan, Z. (2021). Digital technology use during COVID-19 pandemic: A rapid review. *Human Behavior and Emerging Technologies*, *3*(1), 13–24. https://doi.org/10.1002/hbe2.242

Wells, A., Usman, A. B., & McKeown, J. (2020). Trusting Smart Speakers: Understanding the Different Levels of Trust between Technologies. *International Journal of Computer Science and Security*, *14*(2), 72–81.

What is LEED? | U.S. Green Building Council. (2021). U.S. Green Building Council. https://www.usgbc.org/help/what-leed

Wilber, H. (2014, October 1). *When consumers talk, businesses listen | U.S. Green Building Council*. https://www.usgbc.org/articles/when-consumers-talk-businesses-listen

Winder, D. (2021, March 7). *Security Researchers Probed 90,194 Amazon Alexa Skills—The Results Were Shocking*. Forbes. https://www.forbes.com/sites/daveywinder/2021/03/07/security-researchers-probed-90194-amazon-alexa-skills-the-results-were-shocking/