Surveillance in the Smart Home

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

Liliana Gomez

Spring 2023

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

MC Forelle, Department of Engineering and Society

I. Introduction

The smart home has a silent presence, ready to be at the service of its user and process their commands effectively and accurately. With its silent presence though, the user may not realize how much it listens to the home, how much it surveils. In 2018, an Amazon consumer requested to access the data that Amazon possesses of theirs and received back many files: including WAV audio files with recordings from the shower and revealing detailed information about their job, use of public transport and smart-home devices, musical tastes, their girlfriend, and the names of some of their friends (Murnane, 2018). That catch though, was that the consumer didn't own an Amazon smart home device. In fact, these weren't recordings from the consumer's home-- Amazon had sent someone else's audio and data files to them. The consumer told Amazon of the mistake, and then reached out to a magazine to help track down the person who the files belonged to (Murnane, 2018). They realized Amazon hadn't alerted the owner of the files of the breach, despite the law that Amazon must notify the "data protection authorities within 72 hours of discovering the breach" (Murnane, 2018). Once Amazon did acknowledge their mistake, they did not assure how this incident would be prevented in the future (Murnane, 2018). To compound this, in 2018, Georgetown University conducted a study that determined Amazon was the "second-most-trusted institution in the United States" and one of their core values "is to be Earth's most customer-centric company" (Evans, 2021). If this massive technology company, one of the most trusted, was so discrete and disregarding of their mistake, let alone negligent in not alerting the affected, how is the public to know that there aren't more breaches that they simply haven't disclosed?

Smart home devices have become increasingly available and affordable in the United States-- almost 1 in 2 homeowners are also owners of smart home devices, where 46.5% of

American households contain this technology (Lin, 2023; Zheng, 2018). A smart home device is a domestic device, enabled through internet connected devices, such as smart speakers, cameras, thermostats, televisions, or even baby monitors and fridges (Urquhart, 2022). The smart home has developed within a greater concept, the Internet of Things, that consists of providing connectivity and interactive communication for physical and virtual devices including cars and mobile phones (Leloglu, 2017). Specifically, smart home devices have become increasingly popular in the American household, where the number of households with smart home devices have increased 3% since 2022, making up about 60.4 million households in the US using smart home technology (Lin, 2023).

The smart home has normalized a form of surveillance within American households. Notably in the past, there have been technologies that were developed to benefit the majority despite its harm to the minority, and similarly, there exist users and non-users of smart homes that have had their privacy infringed upon due to the surveillance of IoT. Public surveillance has systematically harmed minority groups where misuses such as “criminal abuse”, “institutional abuse”, “abuse for personal purposes”, “discriminatory targeting”, and “voyeurism” occurred and are topics that civil rights groups fought, and continue to fight, against (American, 2022). Comparably, within the home, various internet connected devices are able to track and collect “private user information, communication patterns, … shopping patterns, [and] dining preferences” which can be analyzed to create a profile of their lifestyle and be used for commercial purposes (Frick, 2021, p1). This “data they’ve gathered on consumers” have allowed tech to maintain their monopoly status in the market, and even the House of Representatives have acknowledged this power shift (Fung, 2020).

In response to the adoption of Smart Homes, civil rights groups and major technology companies have differed in their opinion of the smart homes in how they approach the scope of privacy, knowledge gaps, and existing regulation and solutions. I carried out a thorough literature review and content and thematic analysis to draw these conclusions: The literature review dives into surveillance and how it can be detrimental to underrepresented groups, privacy as a human right, and security of data within smart homes. This data is collected from published articles, statistics, and anecdotes from the creators of smart home devices, such as Amazon and Apple, and civil rights groups such as the American Civil Liberties Union (ACLU) and Algorithmic Justice League (AJL). After executing the content and thematic analysis, my Science and Technology in Society (STS) research will be important to the conversation around smart homes, where there will be a greater consideration for all users and non-users that could be influenced by the technology. I expect my findings will exhibit that civil rights groups are indicating that surveillance has a negative impact on a minority of society and are fighting for the right to privacy, but I hope to also find that engineers and designers of the smart home are more deeply considering those affected to lessen its detriment.

II. Literature Review

Civil rights groups are against surveillance because it can be detrimental to underrepresented groups, meanwhile in order for smart home devices to work properly, the devices must actively listen to its users. According to a 2021 research study on the perceived surveillance of conversations through smart devices, a survey showed that a wild 74.4% of the participants, all smart homeowners, are aware of their devices listening to their conversations (Frick, 2021). Surprisingly, in a different domestic study, Princeton University found that their

participants prioritize the connectedness and convenience of their smart home rather than their privacy, where they trust the device manufacturers to protect their privacy without verifying these protections (Zheng, 2018). This belief is not universal as the smart home can be more harmful and unsettling for some users than others: “women, sexual minorities, and nonwhites continue to bear the disproportionate burden of… harms, such as surveillance” (Geeng, 2022). For example, too many times before, when the government has gotten into surveillance of the public, it disadvantages underrepresented groups (Impact, 2016). The US government has surveilled Martin Luther King Junior during the civil rights movement, the Black Lives Matter movement, and in New York, the NYPD “engaged in religious and racial profiling” and infiltrated Muslim student groups, restaurants, and businesses. The NYPD even sponsored youth soccer clubs in order to spy on the kids on the team (Impact, 2016). Unsurprisingly, in the aforementioned Princeton study, the participants were most concerned with the government having access to their data, though they “did not mind the manufacturers of their [smart home] devices collecting and analyzing data, acknowledging that it is necessary to improve the product and user experiences” (Zheng, 2018). Even so, legal scholar Citron argues that “it is easy for tech companies to design products and services without thinking about risks to vulnerable communities” because “we [as a society] fail to recognize the practical and moral significance of privacy” and tend to exclude women and minorities from tech innovation (Citron, 2022).

Oversights in design or bad actors can lead to breaches in privacy in the smart home, even if privacy is advertised to be upheld by their companies. In the Universal Declaration of Human Rights from 1948, created by the United Nations, the document claims that “no one should be subjected to arbitrary interference with [their]... privacy” and this needs to be upheld seventy-five years later with the increase of technology. Internet of Things For All, an

organization working to make IoT accessible to everyone, discusses how this document and definition of privacy needs “to evolve the idea of a right to privacy in this digital age”. (Sloan, 2020) Privacy risks in the *digital age* include network level issues, such as unencrypted exchange over wifi, device and application level issues, like weak authentication or granting more privilege than needed, all leading to “man in the middle" attacks or eavesdropping, creating a device akin to spyware (Duezguen, 2021). Moving forward, the internet of things could increase its privacy protections through “encryption and other security measures… [which] can help support the right of freedom of expression, association, and assembly-- especially among vulnerable people groups” (Sloan, 2020). Vendors of smart homes should also educate their users on security and privacy risks, to close the knowledge gap between the Big Tech companies and the users (Duezguen, 2021).

Since users lack knowledge on the architecture of the smart home, they can be curious about where their data goes, and sometimes there are errors with security of data within the Big Technology companies. According to a study by Deloitte, a large consulting firm, in 2020 “63% of consumers consid[er] connected devices “creepy” in terms of data collection and behavior, while 50% of... consumers were “fairly concerned” about the use of their data” (Lippett, 2022). Cloud connectivity and the always-on power model raises significant ethical concerns with consumers, where the consumers are concerned that every word is recorded and transferred online” (Lippett, 2022). In Frick’s 2021 study, some of the participants even experienced scenarios where they mentioned something, and later their personal device would suggest a similar topic (Frick, 2021). While some common preventative solutions to protecting the data on these devices include active blocking devices such as firewall, intrusion prevention systems, and in-line network antivirus appliances, some users don’t have this knowledge unless they seek out

third party advice and instructions on controlling security and privacy settings of smart homes (Aikins, 2019; Geeng, 2022). One reliable outside source for users is published by the Electronic Frontier Foundation (EFF), an organization defending digital privacy, free speech, and innovation (Budington, 2022). In an article called "Keeping Your Smart Home Secure and Private" on the EFF website, it recommends technology from Mozilla to "search your own smart devices for what they may be sending to the cloud" (Budington, 2022). The article also warns users about a dog nanny device that can "collect any audio, video or pictures you create, upload, save or share", important information the user may have missed if not for reading the privacy policy with caution or utilizing the recommended "*privacy not included" source (Budington, 2022). MIT Technology Review, another third party technology evaluator, helped beta testers of Roomba, a smart vacuum, realize that iRobot was collecting sensitive information from their homes and leaking to social media sites like Facebook, a clear security breach (Guo, 2023).

A Science and Technology in Society framework that helps frame this topic is Pinch & Bijker's Social Construction of Technology Framework (SCOT). SCOT discusses how technology and society are co-constructed, and how relevant social groups have an influence on how technologies are designed, used, and redeveloped. These relevant social groups are defined as institutions, organizations, or unorganized groups of people that "share the same set of meanings" of a specific artifact (Pinch & Bijker, 1984). In this case, the different social groups include Big Technology companies, the users and non-users of the smart home devices, civil rights groups and regulatory groups. Each of these social groups come to different definitions of surveillance in the smart home based on their experience and knowledge of the device. With conversation and compromise between the different groups, they could come to closure by redefinition of the problem of the smart home device's use within the home-- where a single

definition is decided upon, bringing stabilization to the topic, or a high degree of agreement among these groups on the use of smart homes. An alternative that's brought up in the paper is rhetorical closure, where the "relevant social groups [perceive]... the problem as being solved", their example being that the safety marketing of the bicycle convinced those concerned by the device that it had "almost absolute safety" and laid the skeptical conversation around the bike to rest (Pinch & Bijker, 1984). This exact situation may parallel the status of the smart home today, where the marketing from the devices' companies have convinced the users of its safety.

III. Methods

I will be using Pinch & Bijker's Social Construction of Technology Framework (SCOT) to help explore my research question: In response to the adoption of smart homes, how have civil rights groups and major technology companies differed in their opinion of the smart homes? I will examine the following evidence with a content and thematic analysis using the SCOT framework: I will look for common themes in the way the different organizations look at surveillance, how the different groups engage with these themes, and how they change over time.

In regard to how I collected the proper background and supporting information to resolve my research question, I covered a wide variety of topics: opinions on smart homes of civil rights groups, like the ACLU, Algorithmic Justice League, and the Electronic Frontier Foundation, and Big Technology groups, like Apple, Amazon, and Google. I also investigated the development of these smart home devices, as well as any privacy or security promises that their creator companies gave to their consumers. Questions including were the company promises held, what happened when the promises were broken, and who uncovered the breaches guided the search of primary and secondary sources. The primary resources include printed materials and published

materials, as well as advertisements from Big Tech companies and articles from civil rights groups. Google was used to uncover these resources. Secondary resources include academic journal articles, media or journalistic accounts, and reviews of smart home devices. Many of the journals were provided with resources from the University of Virginia's library and Google Scholar.

IV. Results and Analysis

Civil rights groups and Big Tech companies have differing opinions on the surveillance in smart homes because of the difference of their perceived scope of privacy. Big Tech companies believe that protecting the privacy of the house is sufficient, while the civil rights groups believe that the privacy reaches more than the house because their private surveillance intrudes on the public. In Apple's privacy website, it claims that "Privacy at home is more important than ever. That's why your Home app data is stored in a way that Apple can't read it. Your accessories are controlled by your Apple devices instead of the cloud, and communication is encrypted end-to-end. So only you and the people you choose can access your data" (Home, n.d.). Apple also provides "data and privacy information embedded in [their] products… that ask to use your personal data", however Apple claims that the scope of the privacy is within the home only, even though the "personal data" that is collected is not only from within the home but also of their surrounding neighborhood (Legal, 2021). The HomePod can connect to security cameras, or even outdoor speakers that can double as microphones. A more blatant example of private data including public data is from Amazon's Ring device, a smart home security system. There exists a relationship between the Ring device and the police, where the police department may post a "request for assistance" on the Nextdoor app, a Ring affiliated app, where the user may submit

their footage directly to the police (Priest, 2021). “Ring devices are slowly transforming public space into *surveilled* space and allowing Ring owners to decide on behalf of their whole neighborhood to share their recordings of that public space with police”, the data that their device recorded is data on the public (Priest, 2021). Experts at consumer advocacy groups like the Electronic Frontier Foundation and the American Civil Liberties Union have followed this case, and believe that while the police are unable to contact the users directly, there exists too much of a connection between them and the user (Priest, 2021). Another example of a smart home device going bad was when one woman faced extreme consequences after her ex-partner hid a smart baby cam in her room, releasing highly personal footage to the internet and her family (Citron, 2022). These cases prove that surveillance devices have the ability to turn negative, parasitic. While some may say that if the user uses the smart home against the public or if a user’s home isn’t private to start with, it is out of the company’s control, but a responsible company should consider users, non-users, and any way they could interact with the device. These Big Tech companies should take these cases and create fail safes to protect the home and the people around them where “instead of pretending to erase difference”, they create a device that “recognizes, respects, and specifies difference” (Costanza-Chock, 2020).

Another difference that’s been overlooked is the disparity of knowledge between what the company has on the smart home, and what everyone else knows. This disparity drives the differing views on the smart home between the civil rights groups and Big Tech companies. The companies that create the smart homes have knowledge of where the smart home device data is going and how they are processing the data, however they fail to share with their users and non-users a detailed description to quiet their doubts of misuse. For example, because vendors of smart homes do not thoroughly educate their users on their device, many smart home users were

found to have a “limited perception of security and privacy risks" (Duezguen, 2021). While Google has a website for their privacy in their Nest device, the content ranges from vague to inaccessible (Nest, n.d; Data, n.d.). From the demographics collected by Coldwell Banker, a real estate company, we know that mostly millennials and more men own smart homes (Lupis, 2017). The disparity of ownership between the younger generation of American homeowners and the older generation spurs from the gap in technological knowledge, further proving the difference between company resources and the resources that they provide to the users and non-users of the smart home devices. This has led to rhetorical closure of the smart home’s controversy within its users, where the users believe that the smart home is safe enough because the Big Tech companies claim that it’s secure and hide when they have failed these claims. The civil rights groups are not as easily convinced, continuing to attempt to educate users and non-users alike of the vulnerabilities of smart homes.

Finally, at the core of civil rights groups and Big Tech companies, they have differing understanding and acceptance of existing regulations and solutions, causing the rift in how they view surveillance in smart homes. There are organizations like IoT For All that address that privacy is a human right, yet cases like Amazon failing to alert a user of their data files being shared to someone else still occurs (Sloan, 2020; Murnane, 2018). On Amazon’s Alexa Privacy webpage, they address the user, writing that “you have control over your Alexa experience” and “Amazon designs Alexa and Echo devices with multiple layers of privacy and security-- from built-in protections to control and features you can see, hear, and touch” (Designed, n.d.). Even still, they failed to alert the user whose data they’d compromised within their 72 hour regulated buffer time (Sloan, 2020). The civil rights groups and the Big Technology companies simply do not agree upon which regulations to uphold, and even if they are accepted, there’s not enough

accountability within the companies. Privacy infringements include surveillance that can "concentrate knowledge in the hands of the powerful few", therefore devices like smart homes that could be used in this capacity must be regulated such that the users can be preserved (Sloan, 2020).

V. Conclusion

Big Tech's idea of their scope of responsibility for the privacy of the public has allowed them to focus only on the user, such that they may market a safe home with their device, where only the privacy of the house is preserved. While a safe device is marketed, some Big Tech companies have neglected certain regulations that would uphold those security standards they promised to the public, leading to more controversy of the impacts of the smart home. The civil rights groups advocate for more technical or safety knowledge to the users and non-users and speak out to hold the companies accountable. While rhetorical closure has been reached on surveillance in the smart home with the privacy marketing of the Big Technology companies, civil rights groups continue to dig deeper to address all those affected and work to educate the public of the realities of their devices-- turning the user's black box smart home white, making the device's data use more transparent.

Future social or computer science researchers may use this paper for background information as they are researching how America's tech users' perceptions of surveillance affects their purchase of smart home devices. They could also use this to build upon to answer how the companies' perceptions of surveillance shape the design of their smart home. This specific STS topic could be expanded to all Internet of Things, finding more companies that make the devices, and more civil rights groups with opinions on them. Eventually, the hope is that Big Technology

companies and civil rights groups work together to make smart homes beneficial for everyone, and continue to work towards no breaches of privacy, no data leaks, and no unwanted surveillance.

References

Aikins, S.K. (2019). *Managing Cybersecurity Risks of SCADA Networks of Critical Infrastructures in the IoT Environment*. In: Mahmood, Z. (eds) Security, Privacy and Trust in the IoT Environment. Springer, Cham. Retrieved April 20, 2023, from https://doi.org/10.1007/978-3-030-18075-1_1

American Civil Liberties Union. (n.d.). *What's Wrong With Public Video Surveillance?* Retrieved September 18, 2022, from https://www.aclu.org/other/whats-wrong-public-video-surveillance

Budington, B. (2022, July 13). *Keeping your smart home secure & private*. Electronic Frontier Foundation. Retrieved April 23, 2023, from https://www.eff.org/deeplinks/2022/06/keeping-your-smart-home-secure-private

Citron, D. K. (2022). *The fight for privacy: Protecting dignity, identity, and Love in the Digital age*. W. W. Norton and Co.

Costanza-Chock, S. (2020). *Directions for Future Work: From #TechWontBuildIt to #DesignJustice*. In Design Justice (1st ed.). https://designjustice.mitpress.mit.edu/pub/ev26fjji

Geeng, C. (2022). *Analyzing Usable Security, Privacy, and Safety Through Identity-Based Power Relations.* Scholarly Publishing Services - UW Libraries. Retrieved April 22, 2023, from https://digital.lib.washington.edu/researchworks/handle/1773/48894

Designed to protect your privacy. Amazon. (n.d.). Retrieved March 4, 2023, from https://www.amazon.com/b/?node=19149155011&tag=googhydr-20&hvadid=352456913457&hvpos=&hvnetw=g&hvrand=417397490744704515 7&hvpone=&hvptwo=&hvqmt=e&hvdev=c&

hvdvcmdl=&hvlocint=&hvlocphy=9008337&hvtargid=kwd-568076830233&ref=pd_sl_9g20ttlk7a_e

Duezguen, R., Mayer, P., Berens, B., Beckmann, C., Aldag, L., Mossano, M., . . . Strufe, T. (2021). *How to increase Smart Home Security and Privacy Risk Perception*. 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). doi:10.1109/trustcom53373.2021.00138

Evans, W. (2021, November 18). *Amazon's dark secret: It has failed to protect your data.* Wired. Retrieved October 28, 2022, from https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/

Frick, N. R., Wilms, K. L., Brachten, F., Hetjens, T., Stieglitz, S., & Ross, B. (2021). *The perceived surveillance of conversations through Smart Devices.* Electronic Commerce Research and Applications*, 47*, 101046. doi:10.1016/j.elerap.2021.101046

Fung, B. (2020, October 10). *'near-perfect market intelligence': Why A house report says Big Tech monopolies are uniquely powerful* | CNN business. Retrieved October 28, 2022, from https://www.cnn.com/2020/10/10/tech/apple-amazon-facebook-amazon-monopoly-data/index.html

Google Nest Security & Privacy Commitments - Google Safety Center. (n.d.). Retrieved March 3, 2023, from https://safety.google/nest/

Google. (n.d.). *Data Security and privacy on devices that work with assistant*. Google Nest Help. Retrieved March 3, 2023, from https://support.google.com/googlenest/answer/7072285?hl=en#zippy=

Guo, E. (2023, January 11). *Roomba testers feel misled after intimate images ended up on Facebook*. MIT Technology Review. Retrieved April 23, 2023, from https://www.technologyreview.com/2023/01/10/1066500/roomba-irobot-robot-vacuum-beta-product-testers-consent-agreement-misled/

Home app. (n.d.). Apple. Retrieved March 3, 2023, from https://www.apple.com/home-app/

Impact of government surveillance on Muslim Americans and communities of color (2016). Friends Committee on National Legislation. Retrieved October 9, 2022, from https://www.fcnl.org/updates/2016-10/impact-government-surveillance-muslim-americans-and-communities-color

Legal - Apple Privacy Policy (2021, October 27). Apple. Retrieved October 28, 2022, from https://www.apple.com/legal/privacy/en-ww/#:~:text=Apple%20may%20collect%20data%20about,to%20share%20data%20with%20Apple.

Leloglu, E. (2017). *A review of security concerns in internet of things*. Journal of Computer and Communications. Retrieved April 20, 2023, from http://dx.doi.org/10.4236/jcc.2017.51010

Lippett, M. (2022, May 6). *Council post: Privacy, intelligence, agency: Security in the smart home*. Forbes. Retrieved October 9, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/05/05/privacy-intelligence-agency-security-in-the-smart-home/?sh=5b41ff074aac

Lin, Y. (n.d.). *US Smart Home Statistics (2018–2025) [updated Jan 2023]*. Oberlo. Retrieved March 1, 2023, from

https://www.oberlo.com/statistics/smart-home-statistics#:~:text=The%20latest%20smart%20home%20statistics,were%20using%20smart%20home%20devices

Lupis, J. C. (2017, July 5). *Who owns smart home technology?* Marketing Charts. Retrieved March 3, 2023, from https://www.marketingcharts.com/industries/technology-63952#:~:text=Among%20the%20one%2Dquarter%20who,%25)%20than%20female%20(43%25).

Murnane, K. (2018, December 20). *Amazon does the unthinkable and sends Alexa Recordings to the wrong person*. Forbes. Retrieved October 9, 2022, from https://www.forbes.com/sites/kevinmurnane/2018/12/20/amazon-does-the-unthinkable-and-sends-alexa-recordings-to-the-wrong-person/?sh=9c9604c3ca5d

Pinch, T. J., & Bijker, W. E. (1984). *The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other.* Social Studies of Science, 14(3), 399–441. Retrieved March 20, 2023, from http://www.jstor.org/stable/285355

Priest, D. (2021, September 27). *Ring's police problem never went away. Here's what you still need to know*. CNET. Retrieved March 14, 2023, from https://www.cnet.com/home/security/rings-police-problem-didnt-go-away-it-just-got-more-transparent/

Urquhart, L., Miranda, D., & Podoletz, L. (2022). *Policing the smart home: The internet of things as 'invisible witnesses'*. Information Polity*, 27*(2), 233-246. Retrieved November 14, 2023, from doi:10.3233/ip-211541

Zheng, S., Apthorpe, D., Chetty M., & Feamster, N. (2018). *User Perceptions of Smart Home IoT Privacy.* Proc. ACM Hum.-Comput. Interact. 2, CSCW. Retrieved April 21, 2023, from https://doi.org/10.1145/3274469