Mobile App Development: Behind Every Iphone Is A Non Disclosure Agreement For The Next Software Update

Surveillance In The Smart Home: The Differing Perspective Of Technology Advancement Between Big Tech And Civil Rights Groups

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Liliana Gomez

December 9, 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.

ADVISORS

MC Forelle, Department of Engineering and Society

Briana Morrisson, Department of Computer Science

Introduction

Big Technology companies have come to dominate the development and trajectory of the technologies we use in our daily lives. “Silicon Valley’s access to data makes the [technology] industry different in some important ways”, where the monopolies of Apple, Google, and Amazon have user data to curate consistently influential products within their field (Fung, 2020). I am incredibly interested in how these companies have maintained their influence without providing complete transparency into how they make and use these products behind the scenes. Non-disclosure agreements (NDAs), a document employers sign to pledge they will only discuss company information within their teams, create a barrier between the public and the company, and this opaqueness may be at the detriment of the public. For instance, many user lives were saved because tech workers at Theranos, the creators of Elizabeth Holmes’ fraudulent blood testing device, risked breaking their NDAs to expose the faultiness of the device (Ovide, 2022). There have also been many instances where users’ data was leaked from large companies, some including Facebook’s failure to notify their individual users after 530 million users’ personal data was stolen and Amazon falling short to tell a user that their audio recorded by Alexa had been sent to a user, complete with all the conversations they had with Alexa since its purchase (Bowman, 2021; Murnane, 2018). If these significant technology companies are refraining from sharing these leaks of privacy, what else aren’t they telling their users and the public?

I had the opportunity to focus on two different topics within this curiosity of the influence of Big Tech companies. For my technical project, I was able to write about my software engineering internship at a large technology company, and focus on the impact of the Non Disclosure Agreement on my work and others’ within similar companies. My STS project shifts focus from within the companies, to within the homes of the users. I analyze surveillance within

smart homes, and the differing opinions on this new development between Big Tech companies that produce this technology and civil rights groups.

Mobile App Development: Behind Every iPhone Is A Non Disclosure Agreement For The Next Software Update

A new feature for an app that is downloaded to every iPhone was developed during the summer of 2022. However, the Cupertino-based technology company requires a Non-Disclosure Agreement from its employees and interns, so the feature may never see daylight until its still unannounced release. During my summer internships with this Cupertino-based technology company, I came in with many ideas for possible new features and worked with my team members to craft and narrow down the project with the most potential. Over the course of twelve weeks, I coded in Xcode using Objective C and Swift to build out the feature to a working prototype. While the end result was not perfect, the idea was pitched successfully, establishing the potential the app could grow into if the feature were adopted and developed further. While it was not tested on real users due to the confidentiality, there was much feedback that would be resolved with this feature, so I anticipate it would be well accepted by the public. Additional work on the feature will have to include more debugging and polishing so that it will be ready for future release.

Every day, there is a brilliant idea that an engineer creates. They may share it with excitement to their team at work, and further develop it there, collaborating to form an even more innovative solution. When the engineer returns home that evening, and their family and friends ask about their day, it was just a typical day. As much as they would like to share their million dollar idea with their closest circle and hear their opinions on it, the engineer signed a

non-disclosure agreement with their company to pledge they will not spill company secrets to undisclosed individuals. Over one third of today's U.S. workforce is legally bound to an NDA (Lobel, 2018).

This summer I was able to develop a new feature for an iOS application; however, since it has not been released yet, and since I too signed a non-disclosure agreement, I am unable to share the details. I wonder what could have been developed if I had been able to brainstorm with even more individuals, and how the limitations of my creative circle may have limited my innovation. In an article about non-financial disclosures' impact on corporate social responsibility, a researcher on cross-national corporate governance, Jackson, et. Al. discusses the idea that self-regulation within companies, while providing flexibility for the companies to "develop best practices…can also lead to complacency if the firms feel no external pressure" (Jackson, et. al, 2020). This again touches on the impact of secrets with the company and society, and begs the question: how is this affecting possible collaboration in the workplace? We also know that collaboration is essential in the workplace because everyone benefits from each others' talents, but why can't we collaborate outside of the workplace (Indeed 2022)?

Surveillance In The Smart Home: The Differing Perspective Of Technology Advancement Between Big Tech And Civil Rights Groups

As technology is becoming more and more ingrained into our daily lives, more people are adopting the internet of things, having their phone connect to their fridge, thermostat, speakers, and lights. However, this has also led to a normalization of surveillance. When mental health was taboo, there was a widespread shift destigmatizing mental health, changing the infrastructure of emergency services, noted in STS scholar Susan Leigh Star's work, the Ethnography of

Infrastructure (Star 1999). The change in infrastructure brought something swept under the rug into the light: it is no longer normalized to stay silent about mental health, it is encouraged to talk about. It is time that those privileged enough to own smart homes start talking about how they or others may be affected negatively by the surveillance in their homes, and how Big Brother is tracking their data. The companies behind smart home development also need to work on their conversation around surveillance, where they consider collection of data to help personalize the user's experience and make it more enjoyable, and are indifferent to a larger range of impact other than their direct users. I would like to consider Star's study of infrastructure to consider the master narrative, the voice that speaks for the general public, in this case, the Big Technology companies' narrative on the safety of smart homes, and challenge it against the perspective of civil rights groups that consider the smart home's impact on minority groups. How have civil rights groups and major technology companies differed in their assessment of this advancement in technology?

In the past, there have been technologies that are developed to benefit the majority despite its harm to the minority. For example, in the 1970s a mechanical tomato harvester was invented, and "benefit[ed] a handful of private interests [at the] detriment [of] farmworkers, small farmers, consumers, and rural California generally" (Winner, 1980 p.126). Similarly, there exist users and non-users of smart homes that have had their privacy infringed upon due to the surveillance of IoT. I would like to explore the transfer of power between the Big Tech companies to the home, and how they may be influencing the actions of its users. Cressman, as he considered Latour's Actor Network Theory (ANT), discusses that "we act as we do, not by some idealistic notion of free choice, but because our actions are bounded by technologies that delegate how and what we can do within a sociotechnical network" (Cressman, 2009 p.10). I will

consider ANT to explore the connection between the smart home companies, users, and non-users, and building upon the theory, I will consider the power transfer and disparities between the actors.

In addition, Cressman considers a black box, the concept that to users, a device simply does what they want it to do and they do not see the details behind the function that the designers may see. The smart home is so often treated as a black box, where while 74.4% of users are aware of the devices listening to their conversation, and 50% of customers are fairly concerned about the use of their data, as they are unsure of how their data is handled (Frick, 2021 p.8; Lippett, 2022). I would like to consider this concept of the black box in how the two perspectives at the center of my research, the company and civil rights groups, may see the smart home device at different depths. The companies know exactly how data is moving within their networks, and the perspective of the civil rights groups' perspective may be more representative of the public's where the operations of the smart home are more opaque. It is important to educate users on their device as well as possible vulnerabilities if the company isn't able to protect them fully from risks like network level issues... [and] device and application level issues, all leading to "man in the middle" attacks or eavesdropping (Duezguen, 2021 p.997). Perhaps the disparity in perspective of the smart home reflects the disparity between the user and the programmers, where many of the programmers are privileged white men, to whom surveillance affects differently and may assume users already know about possible internet vulnerabilities and how to protect against or avoid them (Woolgar, 1990 p.78). The knowledge about "encryption and other security measures… can help support the right of freedom of expression, association, and assembly-- especially among vulnerable people groups" (Sloan, 2020).

Research Question And Methods

In response to surveillance within Smart Homes, how have civil rights groups and major technology companies differed in their assessment of this advancement in technology? I would like to explore this issue through internet articles from the *New York Times*, *CNN,* and some tech organizations like *IoT For All,* where their focus is on the public's privacy and the influence of Big Technology companies. Additionally, I would like to find big companies, like Amazon's, Google's, or Apple's, initial announcements of their smart home products and analyze their commitment to privacy. For example, Apple claims that they "believe strongly in fundamental privacy rights — and that those fundamental rights should not differ depending on where you live in the world", while Facebook, a company with a failed smart home device, doesn't preach privacy but more transparency, with a tool that lets people "manage and view a summary of information Facebook receives about their activity on other apps and websites" (Legal, 2021; Fowler, 2021). I will also research leaks in privacy, breaches in the company's promises to the public, that have occurred since the smart home's launch, civil right organizations' response, and how the companies adapted. For example, I would explore how Amazon deals with their "low-level employees… using their data privileges to snoop on the purchases of celebrities,... [and] taking bribes to help shady sellers sabotage competitors' businesses, doctor Amazon's review system, and sell knock-off products to unsuspecting customers" (Evans 2021).

Conclusion

The findings from my technical project should help Big Tech companies consider their reasoning behind NDAs, and consider the potential of more transparency. The findings from my 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 indicate that civil rights groups are indicating that surveillance has a negative impact on a minority of society, and organizations are fighting for the right to privacy, but I hope to find that simultaneously engineers and designers of the Smart Home are more deeply considering those affected to lessen its detriment.

Resources

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

Bowman, E. (2021, April 10). After data breach exposes 530 million, Facebook says it will not notify users. Retrieved October 28, 2022, from https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users

Cressman, D. (2009). A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation.

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. Retrieved October 28, 2022, from https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/

Fowler, G. (2021, September 24). Perspective | there's no escape from Facebook, even if you don't use it. Retrieved October 28, 2022, from https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

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

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

Indeed Editorial Team. (2022, July 12). 10 reasons why collaboration is important in the Workplace. Retrieved October 28, 2022, from https://Www.Indeed.Com/Career-Advice/Career-Development/Why-Is-Collaboration-Important

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

Lippett, M. (2022, May 06). Privacy, intelligence, agency: Security in the smart home. Retrieved October 9, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/05/05/privacy-intelligence-agency-security-in-the-smart-home/?sh=5b41ff074aac

Lobel, O. (2018, January 30). NDAs are out of control. here's what needs to change. Retrieved October 28, 2022, from https://hbr.org/2018/01/ndas-are-out-of-control-heres-what-needs-to-change

Murnane, K. (2018, December 20). Amazon does the unthinkable and sends Alexa Recordings to the wrong person. 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

Ovide, Shira. 2022. An Obsession With Secrets - The New York Times. The New York Times. Retrieved September 23, 2022 from https://www.nytimes.com/2021/07/27/technology/nondisclosure-agreements-tech-companies.html

Sloan, H. (2020, June 01). Human rights and IOT: The right to privacy. Retrieved October 9, 2022, from https://www.iotforall.com/human-rights-iot-right-to-privacy

Star, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), 377–391. https://doi.org/10.1177/00027649921955326

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121–136. http://www.jstor.org/stable/20024652

Woolgar, S. (1990, May). Configuring the user: The case of usability trials. Retrieved October 29, 2022, from https://journals.sagepub.com/doi/10.1111/j.1467-954X.1990.tb03349.x