Undergraduate Thesis Prospectus

The Struggle for Privacy in Connected Homes

(sociotechnical research project)

by

John DeFranco

May 9, 2025

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.

John DeFranco

STS advisor: Peter Norton, Department of Engineering and Society

General research problem

How can user privacy and security be better secured at minimal cost to usability and convenience?

Users entrust their personal data to a wide range of devices and companies, while maintaining the reasonable expectation that their data will be safe and secure. However, many users also expect new technologies to have high usability and to be conveniently accessible. This leads to a struggle to find a balance between the two. Strong security should not make technology feel awkward and restrictive, but compromising privacy can lead to significant risks to both individual users and society.

Achieving this balance is not only essential for protecting user privacy, but also promoting trust in new technologies. Data breaches created by inadequate security can lead to personal and financial harm to users, causing their trust in technology to waver, and limiting widespread adoption. This trust is critical for advancing technology and its promise of convenience and improved quality of life. Ensuring user privacy and security without sacrificing usability and convenience will require innovative solutions that satisfy user's expectations of both functionality and data protection.

The Struggle for Privacy in Connected Homes

How are users, tech companies, privacy advocates, and regulators competing to determine the privacy standards governing connected residential systems?

Connected residential systems, a subset of the Internet of Things (IoT), have grown increasingly popular over the past decade. In 2015, there were between eight and 15 billion devices connected to the internet, and it is predicted that there will be between 50 and 75 billion devices connected by 2025 (Girard 2020), with many being dedicated to residential use. This sharp increase in popularity has caused tech companies to release an abundance of internet-connected appliances and devices that attempt to improve user's comfort levels, the safety and security of their homes, and potentially assist users with disabilities (Turner, 2018). However, as the IoT continues to expand into personal residences, the competition over how to balance the privacy and security standards governing it grows as well.

Researchers have investigated the privacy and security risks of connected residential systems and IoT devices, such as Amazon's Echo. The popular line of smart speakers is "always on", constantly listening for its wake word, "Alexa". Once activated, Alexa records audio and collects data, which Amazon then uses to improve Alexa's artificial intelligence capabilities. According to Amazon, this collection of data allows Alexa to "remember context and past interactions", but this constant monitoring introduces significant privacy concerns (Williams 2020). While researching the *Echo*, Williams (2020) wrote that, "Alexa may activate itself without actually being summoned by a user and proceed to record conversations and other speech that was never intended to be recorded." These unintended recordings mean that people near an *Echo* device might be recorded without their consent, even if they are unaware of its presence. Such recordings may yield a large and exploitable database of sensitive personal information. In some cases, Amazon employees manually review the audio that Alexa records to improve device functionality, which raises even more privacy concerns (Williams 2020).

Connected residential systems may also introduce physical and security threats. Researchers Uppuluri and Lakshmeeswari (2024) found that unauthorized access to a connected residential system could allow attackers to manipulate sensors and controls, and even grant entry into the residence. This access to a system could result from a variety of attacks, such as a jamming and replay attack, which can disrupt network traffic. Connected residential systems also permit remote use, so they are vulnerable to man-in-the-middle or impersonation attacks. These security breaches could give attackers full control over the entire system, allowing them to manipulate lights, locks, security cameras, and even locks, potentially without the user's knowledge (Uppuluri & Lakshmeeswari, 2024). Unfortunately, these security breaches do occur. In May of 2023, the Federal Trade Commision charged Ring, the popular home security camera company, with compromising its customers' privacy by allowing their employees and outside contractors to view user's private videos and failing to implement basic privacy and security protections, which allowed hackers to take control of accounts, cameras, and videos. The FTC's complaint revealed that despite suffering attacks in 2017 and 2018, Ring failed to implement basic security measures, such as multifactor authentication, until 2019. Even when Ring implemented these security measures, they were "sloppy" and "hampered their effectiveness" (FTC, 2023). This allowed hackers to continue to exploit vulnerabilities, and resulted in the attackers not only accessing user's data, but also using Ring cameras' two way functionality to "harass, threaten, and insult consumers." This complaint by the FTC resulted in Ring being forced to participate in a mandated privacy and security program, being required to delete customer videos and face embeddings, and pay $5.8 million in refunds to consumers (FTC, 2023).

Some governments regulate IoT. For example, Singapore requires tech companies to mark IoT devices with labels that describe the level of security of their design, called the *Cybersecurity Labeling Scheme* (CLS). The CLS has four levels of increasingly demanding security provision tiers. In the first two levels, manufacturers self certify the level of security of their product, and Singapore's Cyber Security Agency can audit compliance if needed. Products that fall under these levels must have security updates and no universal default passwords. Furthermore, manufacturers must follow secure-by-design principles, such as having policies for protecting user data, storing security parameters securely, and conducting threat risk assessments. In the third and fourth levels, all of the previous regulations still apply, and authorized labs conduct penetration tests against the devices in order to fully ensure that they are secure. These labels are valid as long as manufacturers provide the devices with security updates, with a maximum validity of three years (Mitchell et al., 2022). In the United States, the National Institute of Standards and Technology (NIST) issued recommendations for an IoT labeling scheme in 2022. However, the aim of the U.S's criteria is "to describe the ideal components of a labeling scheme, rather than implement this scheme itself" (Mitchell et al., 2022). It is clear that there is a need for privacy standards governing connected residential systems, and it is necessary for participants to compete to determine said standards.

The major participants engaged in this ongoing competition include four main classes: users, tech companies, privacy advocates, and regulators. These participants have different agendas, perspectives, and values, which causes them to compete to determine the privacy standards governing connected residential systems.

Users generally want high usability and convenience, but their stances on privacy and security vary widely. User's privacy concerns often depend on their individual knowledge and understanding of connected residential systems, and their perceived tradeoffs between the usability and privacy risks that are associated with these systems (Haney et al., 2020). Some users might willingly sacrifice certain privacy measures for convenience and ease of use, while others may not be fully aware of the privacy implications that come with the use of these systems, leaving them more vulnerable to security breaches.

Tech companies that develop connected residential systems often prioritize creating products that are easy to use and innovative, as these characteristics tend to drive consumer demand and sales. These companies advocate for self-governance, and in order to avoid restrictive regulations tech companies have established joint initiatives like *Matter*, which is made up of hundreds of tech companies that have shared ideas regarding the IoT (Crawford, 2024).

Comparatively, privacy advocates, such as the Electronic Frontier Foundation (EFF), argue for stronger data protection laws and transparency regarding user data collected by connected residential systems. The EFF insists that consumers often do not understand the extent of the data collected by connected residential systems, and they advocate for policies that require companies to disclose how user data is collected and managed. In general, privacy advocates seek to establish privacy standards that prioritize user rights, while often perceiving voluntary regulations set by tech companies as inadequate. Privacy advocates may also discuss potential privacy risks associated with the use of connected residential systems, and provide their audiences with methods to protect against these risks (Budington, 2022).

Regulators, such as the Federal Trade Commision, are responsible for conducting reports on the IoT. They then use these reports to set privacy regulations and enforce laws regarding data privacy and protection for connected residential systems (FTC, 2015). However, regulator's power can be limited, and sometimes they are only able to operate in an advisory role. Regulators vary by country, with some countries implementing stricter laws and regulations than the United States, emphasizing a lack of global consistency regarding IoT regulation (Mitchell et al., 2022).

Regulatory agencies must develop policies that balance user privacy, security, usability, and convenience. The diverse interests of users, tech companies, privacy advocates, and regulators creates a unique competition for determining the standards that govern residential connected systems, and will play a key role in both our current and future society.

References

Budington, B. (2022, June 30). *Keeping your smart home secure & private.* Electronic Frontier Foundation. https://www.eff.org/deeplinks/2022/06/keeping-your-smart-home-secure-private

Crawford, C. (2024). *Protocol power: Matter, IoT interoperability, and a critique of industry self-regulation. Internet Policy Review, 13*(2). https://policyreview.info/articles/analysis/protocol-power-iot-interoperability

FTC (2015, January 27). Federal Trade Commission. *FTC report on Internet of Things urges companies to adopt best practices to address consumer privacy and security risks.* https://www.ftc.gov/news-events/news/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices-address-consumer-privacy-security

FTC (2023, May 31). Federal Trade Commission. *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users

Girard, M. (2020). *Standards for Cybersecure IoT Devices: A Way Forward*. Centre for International Governance Innovation. JSTOR.

Haney, J. M., Furman, S. M., & Acar, Y. (2020). *Research report: User perceptions of smart home privacy and security.* NIST. https://www.nist.gov/publications/research-report-user-perceptions-smart-home-privacy-and-security

Mitchell, P., Rowley, L., Sherman, J., Agah, N., Young, G., & Zuo, T. (2022). *Policy challenges to addressing IoT risk.* In *Security in the billions: Toward a multinational strategy to better secure the IoT ecosystem* (pp. 7–17). Atlantic Council. JSTOR.

Turner, L. (2018). *Houses that think: Are smart homes really a smart idea? ReNew: Technology for a Sustainable Future*, 144, 42–47. JSTOR.

Uppuluri, S., & Lakshmeeswari, G. (2024). *Review of security and privacy-based IoT smart home access control devices. Wireless Personal Communications, 137*(3), 1601–1640. SpringerLink.

Williams, D. M. (2020). *Power accrues to the powerful: Amazon's market share, customer surveillance, and internet dominance.* In J. Alimahomed-Wilson & E. Reese (Eds.), *The cost of free shipping: Amazon in the global economy* (pp. 35–49). Pluto Press. JSTOR.