The Struggle for Privacy in Connected Homes

An STS Research Paper
Presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

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

The Struggle for Privacy in Connected Homes

Connected residential systems, a subset of the Internet of Things (IoT), have grown increasingly popular over the past decade. In 2015, 8 to 15 billion devices were connected to the internet; Girard (2020) forecast 50 to 75 billion connected devices by 2025, many of them residential. Tech companies claim their connected appliances and devices improve user comfort, and home safety and security. Some may assist users with disabilities (Turner, 2018). Users, tech companies, privacy advocates and regulators are competing to determine the privacy standards governing connected residential systems. To resist regulation, tech companies invoke user convenience, user responsibility, and the controls that empower users to protect their own data. Privacy advocates, however, contend that default settings, system complexity and marketing put users at a disadvantage that can be corrected only through third-party regulation by a public agency.

The major participants are users, tech companies, privacy advocates, and regulators. Users generally want high usability and convenience, but their stances on privacy and security vary. Because users' understanding of connected residential systems varies, they weigh the tradeoffs between usability and security differently (Haney et al., 2020). Manufacturers typically prefer convenient and novel devices that sell well. They favor self-regulation as a means of averting more restrictive public regulation. To this end, tech companies established *Matter*, a joint initiative among hundreds of tech companies in 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. Privacy advocates may also discuss potential privacy risks associated with the use of connected residential systems and discuss methods to protect against these risks (Budington, 2022).

Regulators, such as the Federal Trade Commision, are responsible for conducting reports on the IoT. They use these reports to set privacy regulations and enforce laws regarding connected residential systems (FTC, 2015). Regulators vary by country, emphasizing a lack of global consistency regarding IoT regulation (Mitchell et al., 2022).

Review of Research

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).

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 need for transparency and secure-by-design principles included in IoT devices

The design of many IoT devices prioritizes usability and convenience over privacy, which can lead to the creation of devices that are fundamentally insecure. This dangerous design approach is illustrated by Amazon's Echo. The Echo constantly listens for its wake word, "Alexa," and it often records user's inadvertently without them being aware. Williams (2020) notes that "Alexa may activate itself without being summoned" and can record user conversations and dialogue which were never intended to be captured. Amazon stores these recordings so they can be manually reviewed by employees to improve the Echo's functionality, all without explicit user consent (Williams, 2020). The Echo lacks on-device indicators that show when it is collecting this data, meaning that users cannot easily determine when their data is being collected or transmitted. This ambiguity has contributed to privacy concerns surrounding both the Echo and other IoT devices.

Secure-by-design principles could have prevented previous security violations in connected homes by including privacy protections in the development process. Ring devices have been involved in many serious examples of privacy breaches. The FTC (2023) found that Ring failed to implement basic security measures like multifactor authentication until two years after the company suffered data breaches in 2017 and 2018. However, these features were then implemented poorly, allowing attackers to continue to take control of devices and use the two-way communication feature to harass users (FTC, 2023). Ring employees also accessed

user's private videos without consent. If Ring had followed basic secure-by-design principles in their development process these issues could have been avoided, so why didn't they? Scholars have contested that companies will often underinvest in and ignore security and privacy protections because they are "externalities," meaning that they are risks that users must bear rather than the companies (Gorden et al., 2015). If tech companies are not provided with economic or legal incentives to implement secure-by-design principles, they will often default to insecure designs during development.

Transparency procedures, such as labeling schemes, allow users to make informed decisions when deciding whether to purchase and use an IoT device. Singapore's Cybersecurity Labeling Scheme (CLS) demonstrates how transparency can be effectively implemented in the development of IoT devices. In Singapore, products are labeled based on their security and privacy features, with higher-tier devices undergoing third-party testing to confirm that they are compliant with standards (Mitchell et al., 2022). These labels are designed to inform users and hold device manufacturers accountable for their design choices. Comparatively, The United States has not adopted a similar scheme, despite one being proposed by The National Institute of Standards and Technology (NIST) in 2022. However, the purpose of the NIST's plan was to simply describe an ideal labeling scheme, without actually implementing it. Based on Singapore's CLS, clear indicators of an IoT device's privacy and security features enable users to choose safer devices, while pressuring companies to prioritize the creation of secure designs.

Concerns that secure-by-design requirements will be detrimental to innovation are unfounded and ignore the risks of inadequate privacy protections. There is a case to be made that regulation mandating privacy protections and features could slow down technological innovation and burden tech companies. However, this perspective falls short when compared to the harm

that could be caused by poor designs. Both Amazon and Ring have faced public backlash, federal investigation, and legal consequences due to their failures to promote privacy and security (FTC, 2023; Williams, 2020). Tech companies that protect their user's data from the start will both avoid these problems and gain the trust of their users.

The need for the creation of enforceable privacy regulations

Tech companies delay privacy and security improvements until forced to act by regulators and public pressure. Ring delayed implementing multifactor authentication despite multiple security breaches, and only implemented the feature in 2019 after facing both public and legal scrutiny (FTC, 2023). Similarly, Amazon Alexa devices engaged in continuous data collection without informing users that their voice recordings may be reviewed by Amazon employees (Williams, 2020). It is clear that some companies will continue to prioritize profitability over user privacy unless consequences are imposed upon them.

Self-Regulation initiatives, like *Matter*, lack the enforcement procedures to ensure user privacy and security. Joint initiatives, like *Matter*, are made up of tech companies that have shared ideas regarding the IoT. However, these self-regulation initiatives are voluntary to join. Although initiatives can encourage tech companies to adopt certain practices, they cannot enforce privacy standards and there is no third-party oversight (Crawford, 2024). Tech companies can opt in or out of initiative's principles at will, and there are no real consequences for putting user privacy and security in harm's way. This form of self-regulation allows companies to appear responsible without actually being held accountable for their actions, making enforceable legal privacy regulations necessary.

Inconsistent privacy legislation creates loopholes and hinders consistent protection for users. In the United States, protection of user's privacy can vary state by state. Some states, such as California, offer more privacy protections than others (Jodka, 2025). This lack of fully unified national regulations makes it difficult to hold tech companies to consistent privacy standards. Comparatively, The European Union's General Data Protection Regulation (GDPR) applies consistently to all of its members, providing clear regulations for all stakeholders (Wolford, 2025). Without a coherent federal framework in the United States, tech companies can exploit differences in legislation, and users may unknowingly utilize functions of IoT devices that would be prohibited in other states.

Regulators must be allowed to strongly enforce privacy regulations to ensure that they have a real impact. Privacy laws and regulations without enforcement are simply suggestions. Even when regulations are created, the regulators that designed them can lack the resources to hold violating companies accountable. The FTC's case against Ring shows how important enforcement can be. Following the FTC's investigation, Ring was forced to participate in a mandated privacy and security program and pay $5.8 million in refunds to users (FTC, 2023). However, such enforcements are not always possible or probably, and tech companies could decide that noncompliance with regulations is cheaper than compliance. Regulators should have the power and resources to enforce privacy standards effectively, regularly auditing tech companies to ensure compliance, and then swiftly striking down violations through fines, mandatory programs, and changes to product designs.

The need for an increase in initiatives that will educate users

Users often lack knowledge of how their connected devices collect, use, and share their data, thus preventing them from protecting their privacy effectively. A 2020 study by NIST found that user's understanding of smart home devices varies wildly. Many participants thought that their connected devices only collected data when actively being used, unaware that many IoT devices constantly collect background data (Haney et al., 2020). Recent data still supports this concern. According to a 2019 Pew Research Center study, 79% of Americans say that they are concerned about how companies use their data, but over half of them say that they are unaware of how their data is being collected and used (Auxier et al., 2019). Without a baseline understanding of how devices work, users cannot advocate for themselves or hold tech companies accountable for misusing their data.

Education initiatives from privacy advocates can help to fill the gap in user knowledge left by tech companies and regulators. Advocacy groups, like The Electronic Frontier Foundation (EFF), provide users with guides and articles to help them understand how to secure their privacy, such as how to turn off voice assistants, update the firmware on their devices, or disable cloud syncing (Budington, 2022). These resources help to empower users, increasing their knowledge of connected devices. However, accessing the information provided by advocacy groups often requires users to have previous knowledge of the issues. Users will not seek out ways to protect their personal data and privacy if they are not already concerned about how IoT devices are potentially using their data. The materials put out by advocacies are effective, but they must be made available and accessible to the public.

Tech companies do not prioritize educating their users in their device setup and onboarding processes, tending to leave users confused and underskilled. Connected devices tend

to fail when it comes to clearly communicated their data practices during user setup, oftentimes leading to user confusion and uninformed consent. Many IoT devices utilize *dark patterns*, meaning deceptive interface designs that push users towards making choices that favor the tech companies at the expense of user privacy and security. Some devices do not provide visible terms of service or privacy policies during user onboarding, and some even preselect options that opt users into data sharing by default (Kowalczyk et al., 2023). An Australian government analysis stated that "the default configurations of IoT devices tend to provide suboptimal privacy and security protections, and many users do not change settings from their defaults" (OVIC, 2021). Many interfaces cause consumers to stick with default settings that share more of their data than they realize, due to complex menus and legal jargon which they do not understand. In short, many tech companies intentionally leave users unaware of how their data is collected, seemingly wanting them to be misled and uneducated.

The success of connected home privacy rests on a cultural shift that will lead users to expect and demand privacy as a default. Protecting user privacy and security cannot be limited to technical and legal regulations; it must become something that the public actively cares and fights for. In our current digital world, convenience is often prioritized over consent. The tradeoff between these two concepts is not always questioned by users, since tech companies have normalized extensive data collection as necessary and generally harmless. In order to fight back against this, users must not only be equipped with the technical knowledge to control their privacy, but also with the expectation that privacy is a right. Changing this social dynamic will require collective awareness and action from the general public. Regulators, advocacy groups, and educators must work together to reframe the way we discuss privacy as a society: not as a barrier to innovation but as a core part of living in an increasingly connected world. When

privacy becomes a standard cultural norm, tech companies will feel a greater pressure to meet that demand.

Conclusion

The competition to determine the privacy standards that govern connected residential systems is ongoing and complex; users, tech companies, privacy advocates, and regulators are all engaged in a struggle to determine the future of IoT devices in daily life. As more connected devices are designed, assembled, and purchased, the stakes surrounding user privacy and security grow higher.

The IoT devices that exist in connected residential systems are not impartial pieces of hardware. Their design, implementation, and marketing reflect the priorities of the tech companies that create them. Unfortunately, those priorities tend to favor creating devices that favor usability and convenience, while neglecting the protection of user data. Without strict regulation, tech companies are unlikely to start prioritizing user privacy and security on their own. At the same time, users lack much of the knowledge to defend their privacy without assistance. Many users consent to having their data collected and used because they do not know it is happening, or just because they have accepted that it is the price that comes with using IoT devices.

Ultimately, the struggle over privacy standards in connected residential systems represents a larger issue between user rights, company power, and technological progress. In order to ensure that IoT devices enhance human's day to day lives, all stakeholders must act. Regulators must hold companies to a higher standard, advocacies must continue to educate users, tech companies must do a better job incorporating privacy and security measures into their

products, and users must make informed decisions and demand that their data is kept safe and secure. The combination of all of these efforts is the only way that personal privacy and connected devices can peacefully coexist as we move into the future.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

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). 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.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, *06*(01), 24–30. https://doi.org/10.4236/jis.2015.61003

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

Jodka, S. H. (2025). The privacy tug-of-war: States grappling with divergent consent standards. *Reuters*. https://www.reuters.com/legal/legalindustry/privacy-tug-of-war-states-grappling-with-divergent-consent-standards-2025-03-27/

Kowalczyk, M., Gunawan, J., Choffnes, D., Dubois, D. J., Hartzog, W., & Wilson, C. (2023). *Understanding Dark Patterns in Home IoT Devices*. https://doi.org/10.1145/3544548.3581432

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.

OVIC. (2021). *Internet of Things and Privacy - Issues and Challenges*. Office of the Victorian Information Commissioner. https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/

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

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.

Wolford, B. (2025). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/