REGULATING SMART HOMES DEVICES: A CO-REGULATION APPROACH

Mohan (Jeffrey) Peng

INTRODUCTION

In 1950, Ray Bradbury wrote "There Will Come Soft Rains," a short story about an automated house that wakes the family in the morning, cooks breakfast, and cleans itself.[1] The automated house runs perfectly even after the human occupants have been obliterated in a nuclear war. Although the story is set in 2026, new technologies such as the Internet of Things (IoT) have already made smart homes closer to becoming a reality.

IoT is the network of interconnected devices that are equipped with sensors that constantly collect data, which are exchanged with other devices and systems over the internet.[2] While interconnected devices can range from wearables such as fitness bands to self-driving vehicles, smart home devices stand out as one of the most practical and promising applications of IoT. Smart home devices automate homes by controlling domestic appliances through internet-connected systems. The sensors on the appliances collect data on the users, which is uploaded to a central server for storage and pattern analysis. The pattern would then be transferred to other devices via the internet so that when certain situations arise, the corresponding appliances would perform specific actions. For instance, if the system of a smart speaker has identified the pattern that the occupant likes to play music once he gets home, the speaker would automatically switch on once the occupant returns home. Going further, the type of music that the speaker plays may even differ depending on the time of arrival.

Many consumers have started to embrace smart home devices. While 47% of US-based millennials have at least one smart home product in their homes, approximately 90 million smart home units have shipped worldwide in 2018 and more than 555 million voice-assistance devices will reach homes by 2024.[3] As smart home devices continue to proliferate, the laws and regulations have not been developed at the same pace. Due to the lack of regulation, smart home companies have collected vast data on users without offering these users transparency in what data are being collected

---

[1] Ray Bradbury, *There will come soft rains*, COLLIER'S WEEKLY, May 6, 1950, at 34.

[2] Oracle, *What is IoT*, https://www.oracle.com/internet-of-things/what-is-iot/.

[3] Smijanic Stasha, *An In-Depth View into Smart Home Statistics*, Policy Advice (Feb. 5, 2019), https://policyadvice.net/insurance/insights/smart-home-statistics/.

and how they are used. Therefore, it is crucial to develop regulations that can protect consumers' interests.

This essay sheds light on the policy implications of smart home devices' data collection practice in the United States. First, we discuss the vastness of those devices' data collection practice and their deeply revealing nature, highlighting the need for regulations. Second, we propose a regulatory framework that combines both federal regulations and soft governance.

I. REGULATION IS NEEDED

The convenience that a smart home device provides relies on machine learning and artificial intelligence, which would not be possible without vast data collection. The sheer volume of data that a device can collect is tremendous: Jeff Haigan, CEO of SmartThings, remarked in the Federal Trade Commission's Internet of Things workshop that fewer than 10,000 households using the company's IoT home-automation devices can generate "150 million discrete data points a day" or "approximately one data point every six seconds for each household."[4] Considering that a household often has more than one smart home device, the actual volume of data collected is likely to be much greater.

Data collection by a smart home device is not only vast but also non-targeted.[5] Deloitte suggests that the devices of many manufacturers "operate under a 'collect if you can' basis."[6] In other words, the scope and amount of data that smart home devices collect are purposely broader and greater than necessary for their core functions. In a 2018 investigation, investigative journalist Surya Mattu monitored the smart home devices installed in his apartment and discovered that those devices collected much more data than is

[4] Federal Trade Commission Staff Report, *Internet of Things: Privacy and Security in a Connected World*, FTC (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[5] Luben Boyanov & Zlatogor Minchev, *Cyber Security Challenges in Smart Home*s, Institute for Information and Communication Technologies of Bulgarian Academy of Sciences (Oct. 12, 2013), http://smarthomesbg.com/files/lb_zm_book_chapter_nato_arw_ohrid_jine_10-12_2013.pdf.

[6] Ifran Saif et al., *Safeguarding the Internet of Things: Being Secure, Vigilant, and Resilient in the Connected Age*, Deloitte (2015). https://www2.deloitte.com/content/dam/insights/us/articles/internet-of-things-data-security-and-privacy/DUP1158_DR17_SafeguardingtheInternetofThings.pdf.

required to deliver the service in question.[7] One of the main reasons why such a practice is allowed to happen lies in the manufacturers' privacy policy. The data collection clauses in their privacy policies often include the term "includes but not limited to," extending the potentials of data collection.[8] Agreeing to these terms, which users often must do in order to use the devices, inadvertently grants the companies unrestrained access to and usage of data additional to the ones that are explicitly stated in the policy. Courts also recognize the validity of such terms. In *Myer v. Uber Technologies*, Meyer sued Uber for illegal price-fixing even though he signed the user agreement that included a mandatory arbitration clause.[9] The court determined that by agreeing to the terms either via a physical or digital signature, the users signal their acceptance of the terms and are subject to them.[10]

The data that smart home devices collect are inherently more sensitive, intimate, and revealing than almost everything that consumers divulge online. Depending on the device, the data could include voice commands, conversations, dietary restrictions, medical information, exercise routines, child behavior, sleeping patterns, and even sexual activities.[11] Besides the data that are directly collected by the devices, advanced data analytics have given companies access to additional insights into consumers' behaviors. Data analytics methodologies aggregate and correlate different datasets to identify patterns that may reveal private information that the consumers never directly shared.[12] For instance, combining a user's streaming history with an exercise routine can be used to generate inferences on the individual's shopping preferences.[13] Although such inferences can be used to offer even greater convenience to the consumers, they could be misused in ways that hurt the consumers' interests. The Organization for Economic Co-operation and Development (OECD) suggests that technology businesses (tech companies) may create detailed individual profiles

---

[7] Guy Sheetrit, *Smart Home and Data Protection: Between Convenience and Security*, Readwrite (Nov. 20, 2020), https://readwrite.com/2020/11/20/smart-home-and-data-protection-convenience-and-security/.
[8] *Id.*
[9] *Meyer v. Uber Techs., Inc*. 868 F.3d 66, 67 (2d Cir. 2017).
[10] *Myer*, 868 F.3d at 75.
[11] Noah Apthorpe et al., *Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic*, arXiv (Aug. 16, 2017), https://arxiv.org/abs/1708.05044.
[12] F. Ramparany, *Semantic Approach to Smart Home Data Aggregation Multi Sensor Data Processing for Smart Environments*, Sensorportal (2016), https://www.semanticscholar.org/paper/Semantic-Approach-to-Smart-Home-Data-Aggregation-Ramparany/f822918fe9052954538695537c63238fc0ac61ab.
[13] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

that could be used to discriminate against customers based on their perceived value.[14]

The problem is compounded by a tech company's unrestrained access to users' data and the lack of transparency in data usage. A 2016 study conducted by 25 data protection regulators found that six in ten IoT devices do not properly disclose to consumers the ways in which their data are used.[15] The lack of clarification allows businesses to use the data in ways that the consumers would not otherwise consent to. For example, in 2015, Samsung's Smart TV collected personal and other sensitive information on users, which was shared with a third party for processing despite the privacy policy's failure to mention such practice.[16]

Considering the vastness of data collection and the private, sensitive nature of the information that comes directly and indirectly from the data, it is crucial to regulate the data collection of smart home devices. At the very least, regulations should require a high degree of clarity regarding privacy policies so that consumers know what data are being collected by smart home devices and how they will be used by the companies. On one hand, there should be regulations that narrow the scope of data collection so that businesses do not have unrestrained access to users' data that is granted by the current privacy policy or terms of service. On the other hand, regulations should be in place to make businesses clarify the ways in which users' data are used in its terms and conditions.

Nonetheless, regulations should still have a degree of flexibility. The smart home industry, along with many others driven by IoT, is still developing, and effective competition is a key mechanism for promoting a better quality of services, which benefits consumers. Regulations that are too rigid may limit businesses' incentive to innovate and compete, which ultimately hinders consumers' access to a better quality of service, products and lower prices.[17] An OECD study found that regulatory frameworks consisting of government regulations alone tend to be too rigid and

---

[14] OECD Directorate for Science, Technology and Innovation, *Consumer Policy and the Smart Homes*, OECD (Feb. 8, 2018), https://one.oecd.org/document/DSTI/CP(2017)8/REV1/en/pdf.

[15] iGOV, *Regulators Find Internet of Things Privacy Shortfalls*, iGOV (Oct. 3, 2016), http://www.igovnews.com/#!/news/view/Regulators-Find-Internet-of-Things-Privacy-Shortfalls.

[16] Mohit Kumar, *Samsung Admits Its Smart TV is Spying on You*, The Hacker News (Feb. 8, 2015), https://thehackernews.com/2015/02/smart-tv-spying.html

[17] Tillväxtverket, *Regulation and Growth*, Swedish Agency for Economic and Regional Growth (2015), https://tillvaxtverket.se/download/18.7b586e5115b13ff864b24615/1490965697446/Regulation+and+Competition+-+170331_hela.pdf.

reduce businesses' incentives.[18] For example, rigid regulations have hindered the growth of the energy industry, particularly the natural gas sector by limiting the industry's ability to react to market conditions and to adjust to price signals.[19] Therefore, it is critical to regulate the data collection of smart home devices with more than just rigid rules established by government agencies.

II. REGULATION PROPOSAL

Currently, in the United States, the federal laws and regulations on data privacy are enacted by different agencies, leaving a confusing mixture of rules with inconsistent regulatory or legal direction. The existing federal laws target only specific types of data in limited circumstances. For instance, the Electronic Communications Privacy Act restricts communication monitoring by employers and government agencies, yet the Act was passed before the Internet became popularized, making it obsolete and ineffective. [20] Similarly, the Federal Trade Commission Act empowers the Federal Trade Commission (FTC) to go after companies that violate their privacy policies and those that fail to meet privacy-related standards.[21] For example, the FTC issued a complaint against Flo, a health-tracking application, for failing to keep the promise of keeping users' data private. [22] A similar complaint was filed against Zoom when the company provided a lower level of security than the 256-bit encryption it touted. [23] However, federal laws are sectoral, tend to target specific populations and regulate strictly within this realm. Specifically, the Children's Online Privacy Protection Rule imposes limits on companies' data collection for children under the age of 13.[24] It does not establish guidelines for the data collection on the rest of the population.

Overall, none of the existing federal laws or regulations offer a consistent guideline on the transparency of data collection and usage for companies. This has allowed tech companies to use catch-

---

[18] 3 OECD, *Competition Assessment Checklist*, OECD Publishing (2016).
[19] Committee on Appropriations, *Energy and Water Development Appropriations for 1991: Hearings* 1710 (1990).
[20] 18 U.S.C. §§ 2511(2)(a)(1).
[21] 15 U.S.C. §§ 45c(b)(2)(A).
[22] FTC, *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data*, FTC (Jan 13, 2021), https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc/.
[23] FTC, *FTC Requires Zoom to Enhance its Security Practices as Part of Settlement*, FTC (Nov. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement/.
[24] 15 U.S.C. §§ 6501(1).

all provisions such as "including but not limited to" to expand their data collection and use the data, without legal repercussions, in ways to which customers would not have consented. This situation must change.

An effective regulation on the data collection and usage of smart home devices should rely on both traditional regulations and soft governance. First, there should be a new federal regulation that offers a consistent and comprehensive guideline on the disclosure of the data that a smart home device collects and how the data are used. Specifically, such a regulation would require any tech company to specify the types of data that its devices will collect, when they will be collected, and how they will be used. The regulation should also limit the use of catch-all provisions in the data collection and usage clause in the privacy policy or terms of service. Such a limit will prevent businesses from gaining unrestrained access to and usage of data additional to the ones that are explicitly stated in the policy.

Second, the new federal regulation should outline the unacceptable usage of the information collected by smart home devices, which includes data that are both directly collected and inferred from aggregated data. As mentioned in the previous section, such information can be extremely revealing and sensitive; it could even be used to target individual users. The regulation should prevent discrimination against certain customers based on not only protect categories but also perceived values. The language of this section of the regulation should be broad and adaptable as opposed to the previous section. Its broad nature allows the meaning to change dynamically, which enables the regulation to cover not just the existing analytical approaches and ways of using the data, but any future cases that involve even more advanced data analytics and usage.

However, traditional legal and regulatory instruments alone, such as the regulation proposed above, are not sufficient. The World Economic Forum states in its white paper that "relying on government legislation to ensure the right outcome" is ill-advised because they cannot keep up with the pace of technological developments. [25] For instance, Facebook permitted Aleksander Kogan to mine data, which were later sold to Cambridge Analytica to "identify the most persuadable voters and the issues they cared

[25] WEF, *Values and the Fourth Industrial Revolution: Connecting the Dots Between Value, Values, Profit and Purpose*, World Economic Forum White Paper (Sep. 2016), https://www3.weforum.org/docs/WEF_Values_and_the_Fourth_Industrial_Revolution_WHITEPAPER.pdf.

about."[26] Cambridge Analytica then "sent targeted messages to them at key times to move them to action."[27] By manipulating users' behaviors, the practice had a substantial impact on the outcome of the 2016 US presidential election.[28] However, the legislation that addresses this issue, the Honest Ads Act, was not proposed by the U.S. Senate until October 2017.[29] This case demonstrates that traditional regulations, such as statutes, are likely to be outdated by the time they are implemented.

Therefore, it is critical to complement traditional regulations with soft governance, which refers to regulation through a self-regulatory organization (SRO). In this case, an SRO is a national organization that is composed of the industry's firms and consumer groups, which can exercise some degree of regulatory authority over the industry by establishing regulations and monitoring firms' compliance. By regulating the transparency of data collection and usage, an SRO can be especially effective based on factors of effective regulations suggested by the International Organization of Securities Commissions: industry-specialized knowledge, industry representation, industry motivation, and contractual relationship.[30]

First, the IoT industry, especially the smart home sector, is highly complex and technical. Considering that it is composed of industry actors, an SRO would have a thorough and specialized knowledge of the industry, which would be highly beneficial. Their expertise would enable the guidelines and standards set by an SRO to be effective and up to date with the latest technological developments, as opposed to the laws enacted by politicians who typically have no background in technology. For instance, California's Internet of Things Law is considered to be largely ineffective because it only addresses device security at a shallow

[26] Daniel Malan, *The Law Can't Keep Up with New Tech. Here's How to Close the Gap*, World Economic Forum (Jun. 21, 2018), https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/.
[27] *Id.*
[28] Scott Detrow, *What Did Cambridge Analytica Do During the 2016 Election*, NPR (Mar. 20, 2018), https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election.
[29] Interview with Sen. Mark Warner, Mary Louise Kelly, NPR (Oct. 19, 2017), https://www.npr.org/2017/10/19/558847414/what-you-need-to-know-about-the-honest-ads-act.
[30] IOSCO, *Model for Effective Regulation*, OICU.IOSCO (May 2000), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD110.pdf.

level, while technology professionals understand that IoT devices include other more complex interfaces that require protection.[31]

Second, an SRO allows for a high degree of industry representation, which is an integral element of regulatory schemes. Industry representation refers to the involvement of the industry's firms and experts. While industry representation "provides the knowledge and assistance to react to emergency situations quickly and effectively," the knowledge and background of the actors allow them to identify trends and determine the regulator implications of new trends.[32] In this case, by including manufacturers of smart home devices with depth of knowledge in the IoT industry, an SRO provides a high degree of industry representation that allows it to react quickly and flexibly to changes in the industry.

Third, smart home tech companies may have stronger motivation to follow regulations and standards set by an SRO. On one hand, technology sectors and businesses in the related industries are overwhelmingly in favor of self-regulation. IoT companies argued that additional IoT-specific regulations would add a considerable burden, given the already complex legal landscape.[33] On the other hand, reputation is a powerful motivating force for sustained proper behavior, and compliance with standards set by an SRO directly affects a company's reputation. In today's global environment where the spread of information is far-reaching and rapid, the failure to comply with certain standards can damage a company's global regulation and may even affect its market shares abroad. For instance, during the 1990s, Nike continuously used sweatshop factories in Southeast Asia, breaching the International Labor Organizations' standards.[34] Because of it, Nike suffered tremendous reputational damage and lost its "ubiquitous popularity."[35] As a result of an incentive to protect its global reputation, regulations set by an SRO may be more easily accepted by the regulated parties. For instance, industry-led initiatives and best-practices guidelines for sensitive data handling, such as the European Cyber Security Organization, have been successful at

---

[31] Matthew Wilson, *State Laws on IOT Security: A Good Start*, BTB Security, https://www.btbsecurity.com/blog/state-laws-on-iot-security-a-good-start.

[32] *Model for Effective Regulation, supra* note 24, (May 2000).

[33] Huw Berverly-Smith et al., *Internet of Things: How the U.S.'s Regulatory Plans Could Raise Compliance Standards*, The National Law Review (Aug. 12, 2020), https://www.natlawreview.com/article/internet-things-how-uk-s-regulatory-plans-could-raise-compliance-standards.

[34] Richard M. Locke, *Can Global Brands Create Just Supply Chains*, Boston Review (May. 21, 2013), https://bostonreview.net/forum/can-global-brands-create-just-supply-chains-richard-locke/.

[35] Ashley Lutz, *How Nike Shed Its Sweatshop Image to Dominate the Shoe Industry*, BUSINESS INSIDER (Jun. 6, 2015), https://www.businessinsider.com/how-nike-fixed-its-sweatshop-image-2015-6.

setting regulations and ensuring their compliance.[36] Therefore, the strong motivation for compliance makes an SRO an ideal complement for the proposed regulations.

Fourth, the contractual relationship between smart home tech companies and an SRO allows for more effective enforcement of regulations.[37] An SRO comprised of both international and domestic businesses can have a global reach, which gives it the unique ability to establish regulations that traverse national boundaries. Additionally, different from statutory law, a regulation established by an SRO may require the observance of ethical standards.[38] The contractual relationship with an SRO would compel its members to follow the regulations regardless of the jurisdiction that their business practice is in. Therefore, the contractual relationship between an SRO and its members would help enforce regulations that are more far-reaching and comprehensive.

CONCLUSION

The data collection of smart home devices is vast, and the data can be more sensitive, intimate, and revealing than almost everything that consumers divulge online. This ultimately puts the privacy of the consumers at risk and can lead to other grave consequences. However, the lack of federal regulations on the transparency of data collection has allowed such practice to continue. As the industry continues to grow and smart home devices become more prevalent, it is crucial to establish frameworks to protect the privacy of consumers. We believe that a combination of federal regulations and a self-regulating organization composed of smart home tech companies can establish effective protection for consumers. While federal regulations set a consistent standard on the disclosure of data collection and usage, an SRO, with its unique characteristics, establishes regulations that not only are up to date but also ensure compliance. With such regulations in place, consumers could perhaps truly enjoy the convenience smart home devices provide.

---

[36] ECS, *ESCO Looks Back at a Successful Year and Sets the Scene for a Cyber 2022*, ECS (Dec 2021), https://ecs-org.eu/newsroom/ecso-looks-back-at-a-successful-year-and-sets-the-scene-for-a-cyber-2022.
[37] *Model for Effective Regulation, supra* note 24 (May 2000).
[38] *Id.*