Regulating the Gold Rush: Using Analogies to Legislate Data Privacy in Smart Speakers

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

Joshua Sahaya Arul

Spring, 2021

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

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

Over 25% of US households owned at least one smart speaker in 2019, and by 2025, it is projected to increase upwards of 75% (Kinsella, 2019, n.p.). As smart speakers' popularity has increased, so have privacy concerns. How can consumers know for sure that their data is being used responsibly and not stored indefinitely, sold to unwanted third parties, or otherwise? Non-users are avoiding smart speakers altogether primarily due to privacy and security concerns, and even those who have embraced smart speakers do not feel comfortable with their devices (Huang et al., 2020, p. 1; Lau et al., 2018, p. 12). Smart speaker companies have responded by adding privacy features to increase consumers' trust, but to no avail (Cho et al., 2020, p. 9). Studies have shown that privacy concerns have been a reason why users abandon technology (Lau et al., 2018, p. 4). If privacy concerns persist, they may consumers will either never explore the full potential that voice-activated technology has to offer or become numb to having their data harvested and privacy violated.

The government has an opportunity to ensure smart speaker data privacy for the public good where no one else has been able to. In the past, governments have been able to correct unethical behaviors by introducing legislation, but that does not mean the government is the right actor; governments are slow to adapt and can be untrustworthy themselves. Still, as a representation of the people, the government possesses a unique responsibility to evaluate and verify companies' trustworthiness. Using Schwarz-Plaschg's guidelines for analogies, I draw analogies with smartphones and the General Data Protection Regulation to demonstrate how analogies are a powerful tool to understanding and governing smart speakers. Using this method revealed that the government must act by introducing goal-oriented legislation and effective enforcement to hold smart speaker companies accountable and prevent fragmented state

legislation. Policymakers should tackle the smart speaker data privacy problem by applying this method themselves to further understand the problem accurately, learn from previous governmental approaches, and discern their consequences.

Problem Definition: Smart Speaker Privacy Concerns Remain Unresolved

As mentioned in the introduction, smart speakers are growing rapidly, but there is growing apprehension among society towards these devices. Some are buying in but frustrated at the convenience vs. privacy trade-off, while others avoid these devices altogether. Smart speaker companies have tried to respond to these concerns by adding privacy features, but consumers' trust did not increase. The government, however, has been able to bring trust and stability many times in history through regulation. Perhaps it is worth considering in the context of smart speaker data privacy.

Users' Looming Privacy Concerns

Smart speakers collect numerous data points with which anyone can create a detailed user profile. With use, smart speakers collect rudimentary (purchases, music tastes, searches) and sensitive data points (exercise patterns, medical information, child behavior) (Gao et al., 2018, p. 6). Researchers have shown that these data points can be used to extrapolate even more sensitive data such as driving routes, sleep routines, and general interests, with reliable accuracy (Huang et al., 2020, p. 2). Smart speaker data privacy is a real concern because anyone with access to the data could spy, exploit, and/or target users without them knowing.

Consumers now worry about their data, their smart speakers, and the companies that control them. Huang et al. (2020) and Lau et al. (2018) studied users' mental models on their understanding of the smart speaker ecosystem and privacy risks. Some participants did not use smart speakers primarily did so either due to their lack of utility or due to privacy and security

concerns (Lau et al., 2018, p. 10). Most of these non-users "did not trust the smart speaker company to abide by the [terms of service] in perpetuity," and correctly so; companies have collected data without user permission or collected more than needed (Huang et al., 2020, p. 7; Lau et al., 2018, p. 11). A couple of non-users also "posited that since major companies like Yahoo and other IoT devices like baby monitors have been hacked, it is highly unlikely that smart speaker companies can guarantee safety from hackers" (Lau et. al, 2018, p. 10). Since companies could not protect data from hackers and exploited data themselves, these participants decided to actively resist purchasing and using smart speakers.

Others balance the trade-off between maintaining their privacy and the convenience afforded by the technology, yet they still express varying degrees of resignation (Lau et al., 2018, p. 14). Many smart speaker users in the study were consciously making a compromise between utility and privacy and were "[frustrated] about such an all-or-nothing trade-off" (Huang et al., 2020, p. 9). Despite adopting the technology, Figure 1 depicts that these users are just as

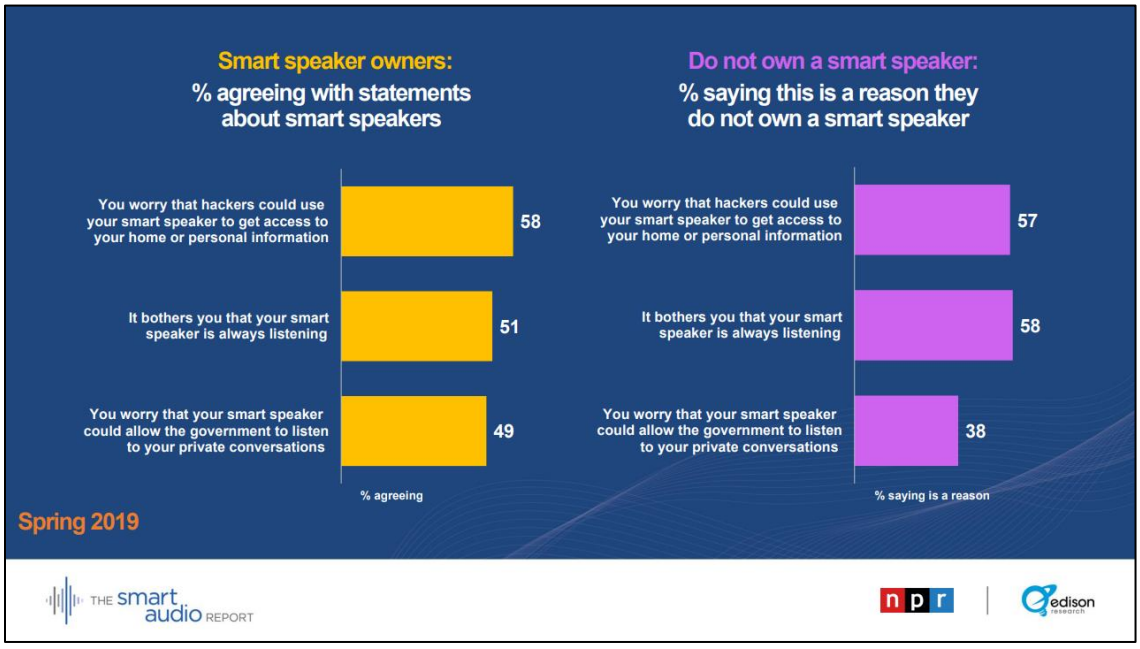

Figure 1. Smart Speaker Users and Non-Users Are Equally Worried. In a survey of 1,002 adults from May-June 2019, smart speaker owners and non-owners were about equally concerned about hackers, always-on listening, and government surveillance (National Public Radio & Edison Research, 2019, p. 30).

concerned, if not more so than non-users (National Public Radio & Edison Research, 2019, p. 30). These users cope with their concerns by taking advantage of the extra security features (e.g. two-factor authentication) and trust the companies to play their role, while others feel helpless that these companies do already have or will have whatever information they want through any means necessary (Huang et al., 2020, p. 9). The point is that even though smart speaker sales are rising exponentially, there is a large body of legitimately worried consumers among users and non-users alike, indicating a need for change.

Smart Speaker Companies Attempt to Address Privacy Concerns

Smart speaker companies attempted to respond to these privacy concerns but had limited success. As Huang et al. (2020), Lau et al. (2018), and others had suggested, Amazon Alexa added privacy controls to build trust with consumers via two new features. Users could now view voice recordings through the mobile app and delete them either through the app or through their smart speaker by uttering phrases like "Alexa, delete what I just said" or "Alexa, delete everything I said today." A recent study found, however, that these features did not improve trustworthiness among consumers (Cho et al., 2020, p. 9). While the additional privacy controls did increase regular users' trust as hypothesized, it decreased trust in power users likely due to the "control paradox": where having more information about all the ways to control their data causes users to feel more vulnerable and hopeless to control it (Cho et al., 2020, p. 2, 9). Given that consumers' overall trust did not increase after Amazon's reasonable attempt to address privacy concerns, we should not expect smart speaker companies to build sufficient trust on their own either.

Considering Government Regulation

Instead of smart speakers trying to build trust with consumers themselves, they could instead be validated by trusted third-party, such as the government. Unlike the private sector, the government has legislative and executive powers that allow it to incentivize behavior that the free market would not otherwise. In history, we have seen where the lack of regulation has led to unsafe practices that have cost lives, such as the Triangle Shirtwaist Factory fire. In 1991, a rag caught on fire (likely by a discarded cigarette) on the 8th floor of a sweatshop in New York City (Britannica, 2021). The fire extinguisher was rusted dysfunctional, the stairwells were locked to prevent theft, and the fire truck ladders only reached the 6th floor. The workers were unable to escape, and 146 workers died. Sweatshops' cost-cutting practices and the absence of accountability meant that sweatshops, including the Triangle Shirtwaist Factory, were vulnerable to fires and did not commit to making changes afterward. Citizens protested the government to enact legislation for labor reforms and building code inspections. Thanks to the passed regulations, this disaster has not been repeated since.

In the case of the Triangle Shirtwaist Factory and many others, government intervention has forced companies to protect citizens' interests when the free market could not incentivize them to do so. Perhaps the government could help in the case of smart speaker data privacy as well. Politicians, older ones especially, have struggled to understand new technologies, but they can be instrumental in bringing real, enduring change. How can policymakers and other relevant actors better understand how to identify, explore, and solve smart speaker data privacy?

Methods: Applying Schwarz-Plaschg's Method of Analogies to Produce Actionable Insight on Smart Speakers

In "The Power of Analogies for Imagining and Governing Emerging Technologies" (2018), Schwarz-Plaschg argues how analogies, a fundamental cognitive skill, are critical to our understanding of novel, complex issues. She describes how analogical imagination and analogical sensibility enable exploration, anticipation, framing, and persuasion. Policymakers, citizens, and others alike can utilize them together to understand the significance of new technologies. I apply Schwarz-Plaschg's rhetorical lens of analogies to conceptualize possible governmental actions and outcomes concerning smart speaker data privacy.

Schwarz-Plaschg's Method of Drawing Analogies

Schwarz-Plaschg explains how to use analogies to explore and anticipate technological development, which she labels as analogical imagination. She first defines imagination as Paul Recour did – "as the power of the possible that can assist in teasing out the potentialities of reality" (p. 3). Schwarz-Plaschg demonstrates how analogies can enable such imagination by correlating new technologies with older ones, allowing us to "come to know something about that object case over and above its existence as an allegedly isolated occurrence" (Smith, 2002, p. 246). In other words, analogies can be drawn to new technologies by relating them to a specific historical and sociotechnical context of previous ones, in turn revealing probable future realities.

For example, the National Nanotechnology Initiative (NNI) of the USA compare the effects of nanotechnology on the "health, wealth, and lives of people" to those of microelectronics, medical imaging, computer-aided engineering, and man-made polymers combined; at the same time, others have compared it to asbestos suggesting that "nanoparticles

could turn out equally harmful in the future" (Schwarz-Plaschg, 2018, p. 7). Note that a single analogy is unlikely to capture all the relevant dimensions of the problem, so multiple analogies will be used to obtain a broader coverage.

Another important aspect of analogical imagination that separates it from science fiction is the power of retrospective prospection. What prevents analogical imagination from drifting into extreme speculation is that analogies are rooted in history. The participant must think back to previous sociotechnical systems and consider how society responded, the lessons learned, and what issues may reemerge (as in the examples above). Although it is important to consider the novel aspects of the new technology, grounding the problem to the past can prevent unrealistic predictions.

Analogical sensibility, the second aspect of Schwarz-Plaschg's method, focuses on problem framing and constructing persuasive versions of the world. Schwarz-Plaschg states framing is used to communicate the situation via a meaningful narrative: "analogies are crucial resources for underpinning expectations and promises, as different social groups make use of different analogies to mobilise for their preferred version of the future" (p. 6). Actors can use different analogies to persuade others to support different views. Consider the above examples once again. Framing nanotechnology akin to computing technologies helped the NNI persuade the US government to increase their funding; policymakers framing it to asbestos and GMO's, however, prompted a public backlash in the US and Europe. Analogical sensibility has helped actors achieve initiatives in the past through framing and persuasion. Similarly, this study will use analogical sensibility to suggest the best course of action for the US government to promote smart speaker data privacy.

Why Analogies Are Powerful for Investigating Smart Speaker Governance

Schwarz-Plaschg states, "When human beings encounter something new, they often seek to grasp its meaning and relevance by identifying similarities with better known phenomena" (p. 1). She begins by describing the evolutionary benefit of understanding analogies has had in humans' lives with an example of a poisonous berry. If one berry resembles the berry that killed someone, we reason by analogy that this berry might kill me as well and we should therefore not eat it. Hence, analogies have played a critical part in our survival. Analogies are not so simple, however, when it comes to today's highly complex issues within sociotechnical systems. There are various actors, motivations, biases, and relationships to consider, forming a webbed network. Still, analogies can be a resourceful tool for helping us understand these issues in the manner we know best. Schwarz-Plaschg writes, "While these processes have become more and more sophisticated, the involved actors—regardless of whether they are scientists, policy makers or 'lay' citizens—are still very much analogical animals in the sense that they rely on analogies when thinking and debating about emerging technological developments" (p. 2).

Besides our engrained ability to reason by them, analogies are persuasive also because they are limited in scope and build upon shared experiences. Analogies are limited because they are not an absolute form of proof. There is no reason that because one technology unfolded in a particular way that another should follow the same. Returning to the berry example, let us consider the situation where the berries are both red. Their visual similarity is insufficient evidence to conclude that the berry is poisonous unless one knew there are no other types of berries that are red. Similarly, conclusions about future technological developments cannot be made based on a few similarities without knowing what all the relevant attributes are (which is

impossible). Thus, Schwarz-Plaschg argues that analogies' persuasiveness, contrary to the scientific method, "does neither rely on logical validity nor upon empirical or scientific evidence" (p.10). Instead, analogies rely on the shared commonplaces (e.g. knowledge, experiences, culture, values) of those engaging with the analogy. Schwarz-Plaschg claims that "by conjuring up such shared interpretations of previous experiences, analogies can influence how people attach meaning to a new scientific or technological field…evoking shared interpretations or framings" (p. 10). One may believe that analogies' persuasive power is determined by the degree of parallelism between the two subjects, it does not explain why some analogies are accepted while others are not.

Finally, analogies should be used to understand new technologies like smart speakers because more rigid, scientific study is impractical. Pure science cannot be applied when studying the dependent variable of future technological developments while also lacking a stable experimental setting, controllable independent variables, and sufficient sample size. Analogies indeed lack the definite proof that traditional scientific experimentation has, but they do leverage what we can to produce insight into the future unknown, making them a powerful and practical tool for imagining and governing new sociotechnical systems. For the same reasons, Schwarz-Plaschg's model of analogies is suitable for investigating the governance of smart speakers.

I will follow Schwarz-Plaschg's method of analogies by looking back in history for actors in sociotechnical systems that share common traits with the problems that have arisen in smart speakers. These candidates will be used to draw analogies to smart speakers' current situation. Doing so will reveal potential future outcomes for smart speakers and what role the government can play in these scenarios.

Results: Recommendations for U.S. Smart Speaker Regulation

The analogies chosen to explore are smart speakers with smartphones and the General Data Protection Regulation (GDPR). The first analogy with smartphones relies on analogical sensibility. Smartphones are like smart speakers in that they both grew rapidly and were/are integrating deeply into our lives, storing very sensitive data while treading unknown waters. Consumers' perception of smart speakers is similar to when the smartphone was in its early days. The GDPR is the first regulation written to tackle modern data privacy issues including smartphone data and many others. Analogical imagination is used to consider what lessons can be taken from the GDPR to regulate smart speaker data privacy in the US. The findings from these analogies demonstrate that analogical imagination and sensibility are viable tools for moving towards better smart speaker legislation.

Comparing Smart Speakers to Smartphones

Smartphones have a plethora of similarities with smart speakers, many of which are relevant. The iPhone, released in 2007, was the first iteration of the smartphone we know today – a mobile phone integrated with a computer featuring internet connectivity, a touchscreen, and an app store. Now, they are an integral part of our lives; in 2019, 81% of Americans owned a smartphone, and 47% said they could not live without one (Metev, 2020, n.p.). People use smartphones to check email, message others, check social media, shop online, do banking, track health, take and store photos, and much more. They are a vault of our personal data, much more so in quantity and sensitivity than smart speakers today but could be in the future. Smart speakers are in their early days but are on target to becoming deeply integrated into human life.

As smartphones became more integrated into our lives, new ethical gray areas in data privacy emerged as with smart speakers, some of which have been addressed, while others

remain unresolved. Edward Snowden's NSA leaks revealed that the NSA and FBI had backdoors to Apple, Google, Facebook, and Microsoft data (Seifert, 2013, n.p.). The leaks led the companies to annually publish the number of data requests from the government, something they resisted doing for years, to dispute claims that they were feeding data into the NSA's PRISM surveillance program (Seifert, 2013, n.p.). Court cases have further clarified data boundaries. The Supreme Court unanimously ruled in Riley v. California (2014) that the search and seizure of information on cell phones are unconstitutional. In 2018, they ruled Carpenter v. United States that the government needs a warrant to access a person's cell phone location history. The court case rulings set concrete limitations on how the government can access data, and the public disclosure of data requests has allowed the people to hold the government and tech companies accountable.

Policies regarding data privacy in other contexts, however, remain undefined and continues to be exploited. For instance, mobile apps can request user permission to access location for additional functionality, such as giving location-based recommendations. Once granted access, apps can engage in the lucrative side business of selling location data to third parties. While data is often "anonymized" in the sense that there are no names or emails attached, it is still sensitive information because it can be reverse-engineered easily (Thompson & Warzel, 2019, n.p.). Figure 2 visualizes how playing Connect the Dots, simply drawing lines between consecutive location pings, can reveal a lucid picture of a person's life. Anonymous sources gave the New York Times location data for a few months in 2016 and 2017 in select cities. Although the data was "anonymized," they were able to map an individual who frequently worked at the

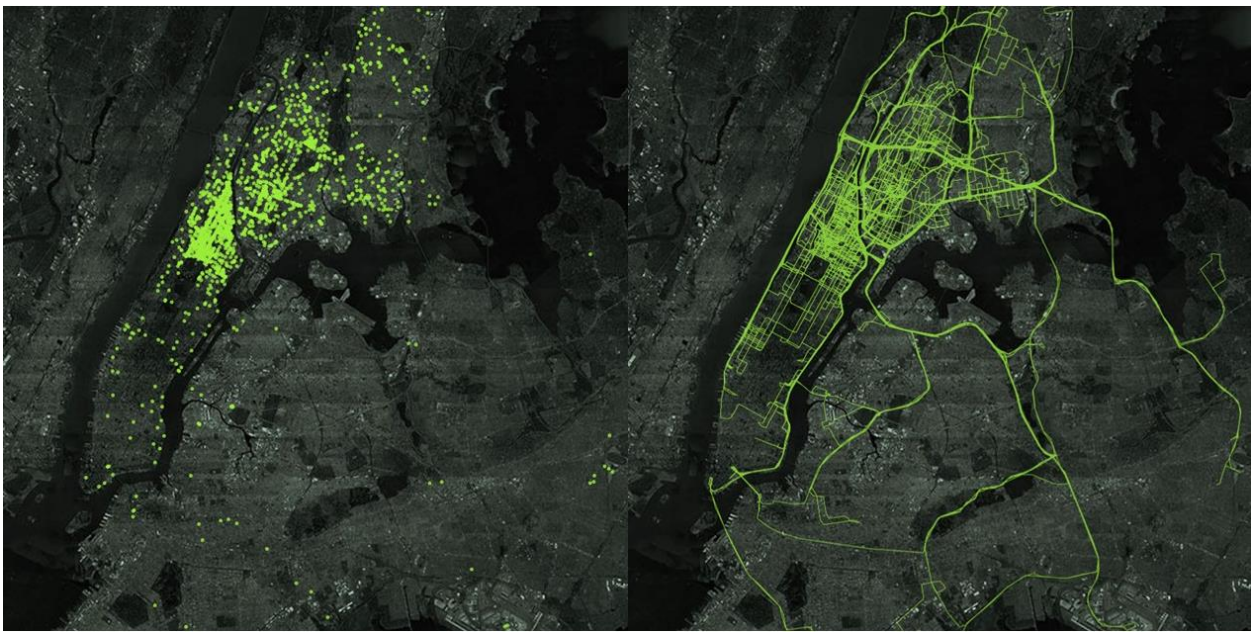

Figure 2. Anonymized Location Data Is Hardly Anonymous. A smartphone's location pings (left) can be connected to creates a diary of a person's life (right). With some research, a phone's anonymized data can be connected back to its owner (Thompson & Warzel, 2019, n.p.).

Microsoft headquarters, visited Amazon one day, and began working there a month later. In a few minutes, they identified the individual as Ben Broili, a manager for Amazon Prime Air. The ability to reattribute anonymous location data to its owner is highly alarming because anyone with the data could be spying.

Smart speaker data must be treated with the same level of severity as smartphone location data is. Consider the number of data points collected (as mentioned before in the problem frame section): times at home, purchases, searches, exercise patterns, etc. It is almost beyond doubt that smart speaker data collectively is personally identifiable as location data is. Policymakers should consider how to limit data exposure with smart speakers as with smartphones.

Comparing Smart Speaker Data Regulation to the General Data Protection Regulation (GDPR)

One regulation that attempted to regulate smartphone location and most other types of data privacy is the GDPR. (Smart speaker data is not covered in this legislation, which is explained later.) The GDPR website self-proclaims to be "the toughest privacy and security law

in the world," and it may be right (Wolford, 2018, n.p.). It is a broad regulation for data protection and data privacy that applies to all companies collecting data related to people residing in the EU, even including companies residing in the US, China, or any other country. The GDPR was passed in 2016 giving a 2-year grace period for companies to adjust before taking effect on May 25, 2018. The GDPR replaced the Data Protection Directive (DPD) of 1995, which was ill-equipped to protect its citizens from today's pervasive data collection.

Among the many revisions from the DPD, several notable improvements added to the GDPR are: redefining data and responsible actors, guaranteeing individual rights, eliminating country-specific standards, and effective enforcement (Beaumont, 2018, n.p.). The GDPR expanded the DPD's definition of data to include any information that could be used on its own or in conjunction with other data to identify an individual (this adds IP addresses, mobile identifiers, location data, biometric data). The GDPR also significantly expanded its scope by mandating compliance by all organizations that serve the EU. It distinguishes between "data controllers" and "data processors" and enhanced compliance guidelines for each. The GDPR also created a single, unified law with one compliance office. Under the DPD, each EU country was free to adopt its own standards and had its own compliance offices, increasing administrative costs for both companies and governments.

The ability for the GDPR to cause dramatic changes in tech may be thanks to its language and enforcement. While the GDPR is detailed, it is also intentionally vague (Greengard, 2018, p. 2). Language such as "reasonable expectations" and "implementing appropriate technical and organizational measures" leaves regulators room for interpretation to accommodate novel individual rights and technological advances. Furthermore, the penalties are very severe for companies in violation. The EU has demonstrated they are unafraid to levy their power even

against the likes of Google and Amazon (Lomas, 2020, n.p.). Vague legislation and the threat of harsh penalties placed tech companies at the EU's mercy and has forced them to change.

Unfortunately, the same subjective interpretation used to defend consumers can be used against them when it comes to smart speaker data. “Recital 18” (also known as “household exemption clause”) of the GDPR declares:

> This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

As expected, the language suggests that smart speaker companies would be treated as controllers and processors and accordingly held responsible; however, consumers may be placed in the same boat as well. Recent court rulings have expanded the scope of “joint collaborators,” which in this case could extend responsibility in the event of a breach to both smart speaker companies and consumers (Chen et al., 2020, p. 285). Chen et al. argue, “Keeping smart homeowners in the expanding circle of joint controllers may in individual cases offer some extra protection to data subjects, but this may at the same time create some widespread effects on the adoption of these technologies” (2020, p. 285). The unclear precedent on which party is responsible for the data explains why the smart speaker data privacy issues remain rampant and why smart speaker legislation is still necessary.

A couple of US states have identified flaws in the GDPR and have begun implementing their own data regulations. The California Consumer Privacy Act (CCPA) includes household data and individual data in the GDPR and went into effect on January 1, 2020. Virginia will begin enforcing the Consumer Data Protection Act (CDPA) in 2023, which is similar to the CCPA but has variations in security requirements, assessments, and appeals processes. Similar bills are also being reviewed in New York, Washington, Florida, and Minnesota.

Findings from Analogies with Smartphones and GDPR

Government intervention is a double-edged sword. They are the authority chosen by the people to act in their best interest. The government can use that trust to give smart speaker companies a metaphorical (or literal) stamp of approval. On the other hand, the government has acted paradoxically, violating their own citizens' privacy by spying on them as per Snowden's leaks. The drawing of analogies with smartphones and GDPR suggests two broad claims: the federal government must enact regulation on smart speaker data privacy, and they should imitate the vague language and strict enforcement of GDPR.

Firstly, the analogy with smartphones revealed that although the government has at times run contrary to the public good, it had been able to counterbalance itself through the system of checks and balances. Snowden's leaks uncovered the NSA's program for spying on its citizens through various channels. The government corrected course to a certain extend when the judicial system ruled against these practices. Court rulings clarified what executive powers could be exercised and others that violated constitutional rights. This demonstrates that the government is self-correcting and able to serve the common good in the aggregate.

The first reason the government needs to intervene is that smart speaker companies are unlikely to exhibit the same self-correcting behavior, as mentioned in the introduction and re-

emphasized in the smartphone analogy. Mobile carriers, mobile app companies, and others collecting location data are well-positioned to sell data to third parties and have done so. Many of the Big Tech companies that were passing data to the government are the market leaders in the smart speaker market. It follows that the same profit-oriented behavior should be expected with voice data. Smart speaker companies might be susceptible to selling third-party data, like their counterparts in the smartphone market, but unlike that market, there are not so many actors in the smart speaker game. It may be in companies' best interest to keep proprietary to themselves, but it does not mean the data could not be misused by them. Companies were able to build rapport after the NSA leaks by publishing data, but they only did so after a fire was lit under them. The government could provide the needed encouragement, which will be discussed later.

The second reason is that the risk of disjointed regulation is increasing rapidly. A lesson learned from the DPD was that allowing member states to tailor and enforce standards individually was that it was highly bureaucratic. Companies spent an excessive amount of time and money trying to comply with all the variations of legislation. One of the key improvements of the GDPR was that it consolidated data privacy regulation across all the EU. With only one law and one compliance office, companies can focus less on clashing standards and more on their business. The data regulation for smart speakers in the US, however, is trending in the opposite direction. California and Virginia have already passed data regulations, and several states are soon to follow. With each state that passes its own regulation, the US is at greater risk of repeating the mistakes of the DPD. Further fragmentation of privacy regulation could overburden companies, increase administrative costs, and reduce compliance rates. The federal government must intervene immediately to provide a nationwide regulation and enforcement agency.

The second finding is that the US government should use the GDPR as a model. The GDPR is still young, so its long-term fortitude is to be determined, but the most modern data regulation there is today has some guiding principles that the US government can take away. The first principle is the use of broad language to focus policies on goals rather than means. Consider the phrase "implementing appropriate technical and organizational measures." It does not dictate what technical approaches to use, but only that it uses the best practices. This phrasing is flexible to innovations, as long as the overarching goal of data protection is satisfied.

The second principle is taking a firm stance against misbehavior. The EU gave a two-year heads-up before fully enforcing the GDPR, and since then, no companies have been exempted nor given preferential treatment. The EU has fined Google, Amazon, Facebook, and Microsoft on multiple occasions, and the GDPR has been a continuation of their strict governance. The regulation has been so strict that an estimated 50% of companies that the GDPR applies to are non-compliant (Shastri et al., 2021). Shastri et al. cite the reason being that anti-patterns in the GDPR, while ideal, are difficult for modern systems to comply with (2021). This contrasts with US politicians who appease large tech firms by offering tax breaks and subsidies. The US government needs to take a firm stance against data misuse when writing and imposing its new legislation.

Conclusion

This paper demonstrates how analogies are a viable tool for understanding and governing smart speakers. Applying Schwarz-Plaschg's method of analogies revealed that the government must introduce regulation to ensure that smart speaker companies honor consumers' privacy, increase consumers' trust, and prevent inconsistency between states. This legislation should utilize vague, goal-oriented wording and levy harsh penalties to hold smart speaker companies

accountable. The smartphone and GDPR analogies, however, only scratch the surface. I encourage policymakers, citizens, and others involved in the legislative process to learn from these analogies, but more importantly, to construct analogies of their own. By using analogies to understand smart speakers and data privacy, we can move towards not just smart, but safe, homes.

Bibliography

Britannica. (2021, March 8). Triangle shirtwaist factory fire. Encyclopedia Britannica. https://www.britannica.com/event/Triangle-shirtwaist-factory-fire

Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. International Data Privacy Law, 10(4), 279–293. https://doi.org/10.1093/idpl/ipaa011

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12, 1. https://doi.org/10.1145/2335356.2335358

Cho, E., Sundar, S. S., Abdullah, S., & Motalebi, N. (2020). Will Deleting History Make Alexa More Trustworthy?: Effects of Privacy and Content Customization on User Experience of Smart Speakers. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–13. https://doi.org/10.1145/3313831.3376551

Gao, C., Chandrasekaran, V., Fawaz, K., & Banerjee, S. (2018). Traversing the Quagmire that is Privacy in your Smart Home. *Proceedings of the 2018 Workshop on IoT Security and Privacy*, 22–28. https://doi.org/10.1145/3229565.3229573

General Data Protection Regulation (GDPR) – Official Legal Text. (n.d.). General Data Protection Regulation (GDPR). Retrieved March 23, 2021, from https://gdpr-info.eu/

Greengard, S. (2018). Weighing the impact of GDPR. Communications of the ACM, 61(11), 16–18. https://doi.org/10.1145/3276744

Huang, Y., Obada-Obieh, B., & Beznosov, K. (Kosta). (2020). Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3313831.3376529

Kinsella, B. (2019, June 18). *Loup Ventures Says 75% of U.S. Households Will Have Smart Speakers by 2025, Google to Surpass Amazon in Market Share*. Voicebot.Ai. https://voicebot.ai/2019/06/18/loup-ventures-says-75-of-u-s-households-will-have-smart-speakers-by-2025-google-to-surpass-amazon-in-market-share/

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 102:1–102:31. https://doi.org/10.1145/3274371

Lomas, N. (n.d.). France fines Google $120M and Amazon $42M for dropping tracking cookies without consent. TechCrunch. Retrieved March 22, 2021, from

https://social.techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent/

Metev, D. (2020, November 17). 39+ Smartphone Statistics You Should Know in 2020. Review42. https://review42.com/resources/smartphone-statistics/

National Public Radio, & Edison Research. (2019, June 25). The Smart Audio Report. National Public Media. https://www.nationalpublicmedia.com/insights/reports/smart-audio-report/

Recital 18—Not Applicable to Personal or Household Activities. (n.d.). General Data Protection Regulation (GDPR). Retrieved March 25, 2021, from https://gdpr-info.eu/recitals/no-18/

Rottermanner, C., Kieseberg, P., Huber, M., Schmiedecker, M., & Schrittwieser, S. (2015). Privacy and data protection in smartphone messengers. Proceedings of the 17th International Conference on Information Integration and Web-Based Applications & Services, 1–10. https://doi.org/10.1145/2837185.2837202

Schwarz-Plaschg, C. (2018). The Power of Analogies for Imagining and Governing Emerging Technologies. NanoEthics, 12(2), 139–153. https://doi.org/10.1007/s11569-018-0315-z

Seifert, D. (2013, June 6). Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data. The Verge. https://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism

Smith, B. (2002). Analogy in Moral Deliberation: The Role of Imagination and Theory in Ethics. Journal of Medical Ethics, 28(4), 244–248. https://doi.org/10.1136/jme.28.4.244

Thompson, S. A., & Warzel, C. (2019, December 19). Opinion | Twelve Million Phones, One Dataset, Zero Privacy. The New York Times. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Zaeem, R. N., & Barber, K. S. (2021). The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. ACM Transactions on Management Information Systems, 12(1), 1–20. https://doi.org/10.1145/3389685