Impacts of Security Policy on the Decline of Connected Toys

Emily Caragay, Raveen Nzilani, Sarah Vu

May 20, 2021

Abstract

Internet of Things (IoT) toys grew in popularity from the early to mid-2010s, but almost completely disappeared by the end of the decade. However, IoT devices for adults and online platforms for children like YouTube Kids have only grown in popularity. We focus on the United States and explore the downfall of IoT toys by synthesizing research on public opinion of IoT devices and placing enacted legislation in the timeline of these toys' rise and fall. The results of our analysis suggest that public policy had the most impact on the failure of these toys, and we have found that there are many implications from this case study that can be used to benefit future security and privacy legislation. In our discussion, we highlight the importance of the Federal Trade Commission (FTC) and analyze their methods of operation, scrutinize the informed consent model used in the US to protect privacy and security, and compare the impacts of privacy and security legislation on small and large businesses.

Introduction

Internet of Things (IoT) devices have begun appearing in every part of life: from connected home appliances, farming equipment, shipping container trackers to wearable health monitors [36, 27, 32, 31]. Many of these devices come with an abundance of security and privacy concerns [40, 39], but IoT toys directed at minors raise a whole new class of issues. IoT toys rose in popularity around 2015, with voice recording teddy bears and conversational dolls becoming popular in the market [30, 29].

The unique concerns that IoT toys raise vary: parents may have differing expectations of privacy for their children than they do for themselves, children may not understand what the toy is actually doing or be able to provide informed consent, and the United States law treats technology directed at minors as a separate category from other technology.

In this paper, we consider IoT toys independently from other IoT devices, evaluating how public opinion and legislation around children's security shaped the market. We found that in 2017-2018, many IoT toys were discontinued and few remain today, while at the same time, other IoT devices such as the Amazon Alexa rose in popularity [23]. We synthesize significant evidence that shows parents are willing to share their child's data with toy companies, finding these toys to be acceptable devices in many circumstances, and determine it is unlikely that public opinion itself was the cause of the decline. However, the implementation and enforcement of US law targeting technology directed at children was strengthened just prior to 2017, indicating that changes in regulation significantly impacted the industry. The newly enforced regulations made it much more difficult for companies without significant financial and technical resources to produce law-abiding toys.

By identifying the role of regulation in the decline of IoT toy popularity, we provide a lens through which policymakers should consider future privacy legislation. Despite IoT toys largely being absent from the market today, many other apps and websites targeted at children are on the rise. It is essential to understand how parents and children view their privacy, and the role and impact of legislation in protecting the privacy of minors.

Background

IoT toys are different from other IoT devices for a variety of reasons, the most prominent of which are differences in the user's ability to give consent and the user's knowledge base. With IoT Toys, informed consent is not expected from the primary users, children, and is instead requested from parents. Additionally, children do not understand basic online safety and cannot differentiate between public and private information. Because of these differences, regulations for children's privacy are stricter in most countries than regulations for adult privacy.

The hardware making up IoT toys also create concern among users. Most connected toys use microphones and cameras, which people consider to be technological sensors with the largest invasions of privacy [24]. These sensors and other components, such as bluetooth chips and wi-fi sensors, are also often inexpensively made. In the attempt to create affordable toys for the general population, IoT toy manufacturers have an incentive to cut corners on security measures.

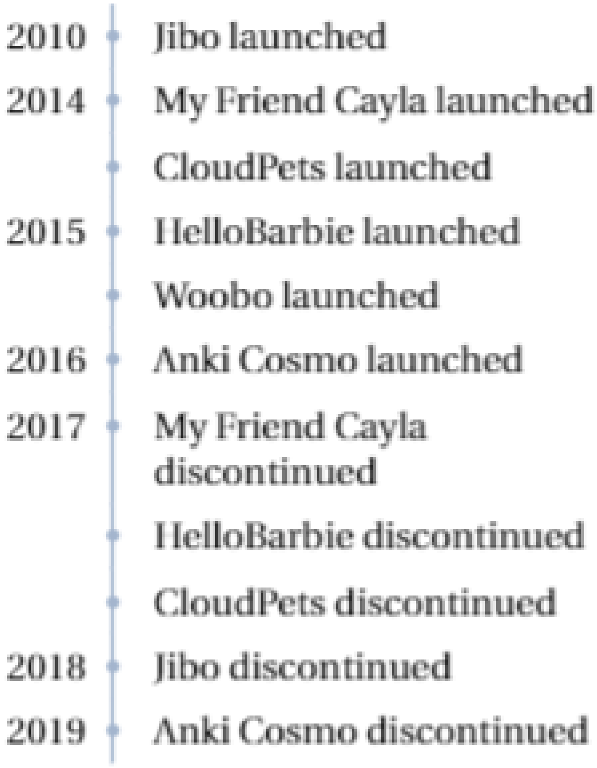

Figure 1: Toy Timeline

The rise and fall of IoT toys is described in Table 1. One of the first toys, Jibo the social robot, was launched in 2010 and was designed to be another "friend" in the home [12]. Kids could play games on Jibo, use its camera, and converse with it. More toys however, appeared between 2014 and 2015, which was the peak in popularity for these toys. However, in 2017, toys began to fail as My Friend Cayla, HelloBarbie, and CloudPets were discontinued [35, 5, 4]. All three companies had a lot of negative press in 2016 and 2017 [4, 3, 37], including official notices warning consumers about their security from organizations like the FBI, the Norwegian Consumer Council, and the FTC [28, 19, 21]. However, Jibo and Cozmo Anki did not receive any negative press about privacy and security and their manufacturers still discontinued the products in 2019 [12, 17].

Even though these toys failed, similar IoT devices like smart speakers with recording capabilities have only skyrocketed in popularity [23]. Technology targeting kids such as YouTube kids has also grown in popularity, and even Facebook is trying to market to kids with the creation of Instagram for Kids [41, 26]. This paper explores why IoT toys were unsuccessful while these other technologies with similar security and privacy concerns have seemed to thrive. We pose the question: How has the popularity of IoT toys changed over time, and what was the impact of public opinion and security and privacy policies?

We attempt to answer this question by synthesizing existing work that studies how the general population in the United States view IoT devices and placing enacted legislation in the timeline of toys we have created. We do this to explore in what ways both public opinion and policy have shaped the evolution of these devices and what we can learn from this phenomenon.

General Opinion on IoT Devices and Toys

We synthesized existing literature to understand how people viewed IoT devices for adults compared to IoT toys, which are aimed at children. We chose to include studies that focused on smart home assistants and speakers, because the main privacy concern of these devices is sound recordings, similar to IoT toys. Overall, we found that most adults in the United States are not overly concerned about their own privacy and explore little of the privacy controls given to them on their own devices. When it comes to children, adults express increased concerns about privacy and security, but are still willing to give their children's data to private companies in many circumstances. Children think of security and privacy even less frequently than adults do and have a very weak understanding of how to protect themselves.

IoT Devices Intended for Adults

Smart home assistants, whose primary users are intended to be adults, have only been growing in popularity since they were introduced in the early and mid-2010s. To discuss how the general population views these devices, we first have to note that there are two main categories: non-users and users.

Non-users of smart home assistants and speakers mostly fall into two distinct groups. The first group does not have any use for smart assistants, so they choose not to buy them. They are either unconcerned about security and privacy and do not even consider it before choosing not to purchase a device. The other group of non-users actively resists buying these devices because of security and privacy concerns. Their main issue is a general distrust of the companies that manufacture these devices (Google, Amazon). Users do not believe that the companies will abide by the Terms of Service (ToS), and they also worry that if the ToS are updated later on to further infringe on a user's privacy, the device is rendered useless if the user does not agree to them [7].

Users, on the other hand, overwhelmingly state that they trust smart home devices specifically because of the companies that produce them. They believe that large companies like Amazon and Google have the resources to correctly protect their customers' data, and they believe these companies will choose to do so in order to protect their best interests and remain competitive and profitable [7]. The initial barriers for purchasing these devices in the first generation of release were high costs, lack of heterogeneous integration, and security concerns [1]. We theorize that most users were not overly concerned about security, because once the other barriers of cost and utility were removed, the devices sold quickly. We wonder if these same barriers of cost and utility affected the IoT toys that never faced negative security press, since Jibo and Anki Cozmo were the most expensive of the IoT toys at hundreds of dollars a device.

Though users are not as preoccupied with security as resistant non-users, they are not completely unaware of the security and privacy risks of their devices. Most users knowingly trade privacy and security for convenience, but with varying levels of acceptance. Interview responses expressed mostly resignation - interviewees believed the security and privacy risks were unavoidable, that they already accepted those risks when they use Google, and that they simply did not care "as much as they used to" [7]. We believe that this could be a significant factor that makes toys different from smart speakers and home assistants. Adults already experience giving away their data to tech companies (Facebook, Google) and consenting to surveillance (work devices, cameras at work).

Users understand that they are trading off privacy and security for convenience, but few users fully understand the risks that are posed to them and exactly what they are consenting to. In one survey of 116 smart speaker owners, almost half didn't know speakers were keeping recordings permanently, only a quarter ever reviewed recordings (which users have access to), and few deleted any of them [11]. Some users even use their devices to spy on others by reviewing recordings. One owner interviewed in a study looked back at recordings to spy on their baby-sitter [7]. However, many more users express lack of concern for their own privacy but an increased sense of concern for the privacy of others that may use the device, specifically children and guests [11].

Overall, it seems that users are aware of the privacy and security risks of smart home assistants and speakers, but they do not fully understand how the devices work and what risks they pose. They accept the risks because they value the convenience and utility of these devices much higher. For IoT toys to be accepted in the way these devices have, parents would have to be able to trust the companies to keep the data safe and the value returned from the toys would have to outweigh the risks. What the returned value could be, whether it is joy for the child or safety and monitoring abilities for the parents, is unclear.

IoT Toys

Parents

When it comes to IoT toys, parents care about having parental controls, monitoring abilities, and access and control of their childrens' data. Education and income level do not affect parents' views on IoT toys, but if parents already own an IoT device such as a smart home assistant or speaker, they are more likely to accept IoT toys [10]. Parents mainly view these toys differently because they are not the primary users and cannot control access to them [6]. One can argue that access to smart speakers is also not controlled, but they are usually hidden away in adult rooms or in a central location where children can be monitored by their parents.

In one study, all of the parents explicitly desired parental controls, and most expressed appreciation when toys came with monitoring abilities [6]. Those who were not impressed with monitoring abilities expressed ideas along the lines of "too much data to sift through" and "nothing interesting to listen to" in response to saved recordings of their children from their toys.

When it comes to privacy and security concerns, they are most strongly concerned about external threats such as hackers [2]. However, parents' safety conversations with their children mostly just concern conversations about what kind of information is personally-sensitive and should not be shared [8]. The majority of rules that parents lay down for their children have nothing to do with privacy and security, but instead focus on tech addiction and inappropriate content [8]. This creates a gap in knowledge for children, and shows how parents prioritize different risks of technology use. Parents are either unaware of the privacy and security risks of internet-connected devices for children or give it lower priority than other risks.

Parents want access and control of their children's data, but they are willing to share the data with companies. In Apthorpe et. al, hundreds of parents were interviewed and given scenarios with different types of data, companies, and devices, and were asked to rate how "acceptable" it was to give a company a type of data collected from a specific device. The study found that parents were willing to share every single type of data the researchers specified in many of the contexts given, including the child's birthday, video of the child's face, their location, and their common routes [10]. These contexts were also not unreasonable - when consent is explicitly asked for often and easily revoked and when data could be reviewed, deleted, and is reasonably protected, parents were open to data collection. We were surprised by how much data parents were willing to share with toy manufacturers, because this suggests that the privacy of their children is not unnegotiable.

Children

When it comes to IoT toys, the design of it is essential. Privacy and security concerns aside, children were easily bored by early IoT toys because they looped and repeated conversation topics [6]. Children found Siri and Alexa much more interesting because of their wider array of responses. It's also important to note that children are consumers, not creators, when it comes to technology [2]. They prefer watching videos or playing games over creating their own content, which includes holding conversations with IoT toys that speak. This is a limiting factor for the success of IoT toys unrelated to privacy and security, and while there is no research to suggest that boredom led to the decline of the toys, we want to note its significance.

In terms of privacy and security, parents and the United States government are correct in assuming that their children cannot give fully informed consent. Children do not perceive external threats well if it all, and mostly fear direct family members such as siblings and parents when it comes to their privacy and security [2]. The IoT toys market is generally directed toward children younger than 13, and often even younger than ten, and at this age, children do not have strong safety practices. In one study, children were unable to tell if a toy had recording capabilities [6], and were unable to pinpoint when recording started on their toys. In another, young children ages 7-11 could not conceptualize private information and who they could and could not share it with [2].

It is reasonable for parents and government agencies to be concerned with children's privacy and security when it comes to technology they use and interact with, but children share little of the concerns adults do and show a weak understanding of security and privacy. Their main concern regarding IoT toys is entertainment.

Synthesis

Overall, it seems that parents and children do not find IoT toys completely unacceptable - their privacy and security concerns are less thorough and less important to them than we expected, and parents are willing to share their child's data with toy companies in reasonable contexts.

While the research suggests that security and privacy is more important to parents when it comes to their children rather than themselves as adults, it is still not always the most salient factor. Tech addiction and inappropriate content pop into their minds first. Additionally, parents often want to violate their children's privacy by asking for monitoring abilities, though they do not see themselves as privacy risks or consider themselves or a child's siblings as threats.

For an IoT toy to meet the specific safety expectations of parents, the toy must properly secure data and ask for consent explicitly and often. The toy also must give full control of the data to parents, allowing them to review their child's data and delete it when desired. Parents are willing to work with third party companies, but prefer if their child's data is only handled by the direct manufacturer and producer of the products. These attributes are already reflected in the smart speakers sold by Amazon and Google. There is trust established between the consumer and manufacturer, and the privacy and security tradeoffs are made knowingly and willingly by the primary owners even though the tradeoffs are not always fully understood.

In conclusion, we do not believe that parent protectiveness and concern over their children's privacy and security were enough to cause IoT toys to fail. Parents and children are open to these toys and we believe that some IoT toys, such as Jibo and Anki Cozmo, had already met these expectations before they were discontinued. However, Jibo and Anki were incredibly expensive and had little utility to offer, and we wonder if like early smart speakers, these were the main barriers to adoption.

Impacts of Policy and Enforcement

In addition to considering the effects of parental concern on the popularity of IoT toys, we consider the effects of policy and changes in the enforcement of that policy, with a focus on the United States. The primary law impacting technology targeted at children is the Children's Online Privacy Protection Act (COPPA). COPPA is enforced by the Federal Trade Commission (FTC). We found that in 2017 and early 2018, the FTC pivoted towards explicit enforcement of COPPA in the realm of IoT toys. As discussed in ¡Section¿, many IoT toys were discontinued in 2018. We conclude that the decline of these IoT toys was greatly impacted by changes in regulations and enforcement.

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) was enacted in 1998, and it required the FTC to issue and enforce regulations concerning the online privacy of children. The goal of the legislation is to protect children under the age of 13 and to place parents in control of the information being collected on their children. The expectations COPPA places on companies generally fall into the following categories: the contents of privacy policies, the process of obtaining parental consent, and the storage of collected data.

It is notable that COPPA expects the FTC to "issue and enforce regulations." By giving the FTC this power, COPPA is a flexible law, with the FTC changing what the regulations and enforcement look like over the years. To establish what a given law, such as COPPA, means, the FTC publishes "rules", which are explicit, industry-wide regulations based on a given law. In addition to rules, the FTC issues "guidance", which are interpretations of the rules, designed to provide additional clarity regarding legal requirements [22]. Companies look to rules and guidance to understand how a given law applies to their business. Noting changes to rules and guidances will be significant in our analysis of the impacts of policy on IoT toys.

Timeline

In 2000, the FTC published and began enforcing its first COPPA rule. In 2013, significant changes to the rule were made. The most notable change impacting IoT toys was the expansion of the definition of "personal information." Information such as audio files containing a child's voice and geolocation information were now considered personal information [25]. This rule change also strengthened the expectations of consent and privacy around companies sharing information with third parties.

In 2017, the FTC released a new guidance in their “Six Step Compliance Plan.” In this guidance, they clarified that “connected toys or other Internet of Things devices” are items covered by COPPA [20]. This guidance was the first time the FTC explicitly stated that connected toys are included under COPPA guidance. Prior to this guidance, it was not clear that COPPA applied, as the actual language of the law simply states that it applies to any “website or online service” that collects personal information from children. Before 2017, despite IoT toys having been on the rise for multiple years, no IoT device company had undergone FTC investigation. This stood in stark contrast to the many websites, games, and other purely online services that were fined, an indication that prior to 2017 the FTC was not looking closely at these devices.

This new guidance sent a signal to the connected toys industry that IoT devices would be a priority area for the FTC enforcement of COPPA moving forward. Around the same time as the FTC’s updated guidance was published, the Federal Bureau of Investigation (FBI) published a warning for parents, informing them that their internet-connected toys could be misusing their children’s data, and to use caution when considering purchasing these toys. In this consumer notice, the FBI cited COPPA and the new updated guidance targeting IoT toys [19]. Paired with the FTC guidance, it is clear that in 2017 the security of IoT toys became a significant area of concern for governmental agencies that dealt with children’s privacy.

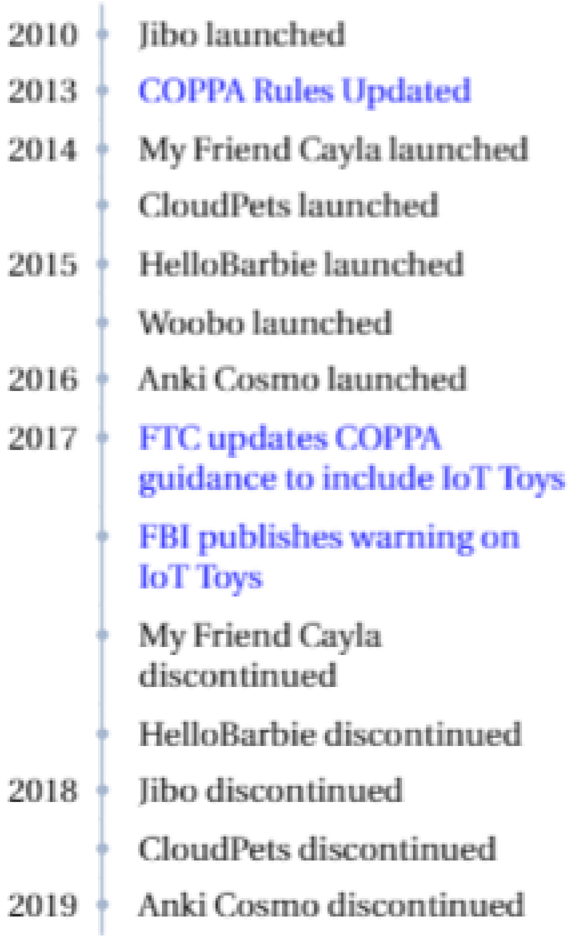

Figure 2: Policy and Toy Timeline

First Connected Toys Settlement

Just six months after signalling their intent to begin holding connected toys manufacturers accountable, the FTC announced the first settlement of a case involving an IoT toy violating COPPA. VTech was a manufacturer of educational toys that worked in conjunction with its “Kid Connect” app, that settled with the FTC for 650,000 USD over their violations of COPPA [21]. This landmark settlement was a concrete warning to other IoT toy manufacturers that the FTC would pursue legal action if they failed to comply.

The process of enforcement by the FTC is unique in that violations rarely go to court. Instead, the FTC receives complaints from the public about companies, then decides when to follow up by pursuing an investigation or issuing a formal FTC complaint with charges. The resolution of these charges is usually a consent agreement. A consent agreement is when the company agrees to settle, paying a fee and accepting other requirements such as future audits or trainings.

VTech was investigated for numerous violations of the COPPA rule, paired with deceptive practices. VTech's key violations [9] were failure to:

- Post a clear and complete privacy policy
- Obtain "verifiable parental consent"
- Establish "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children"

As part of the settlement, VTech paid $650,000 USD in addition to being required to implement a data security program that will be independently audited over the next 20 years [9].

The FTC took advantage of this settlement to explicitly draw attention to the importance of IoT toy security. The Acting Chairman of the FTC said, "As connected toys become increasingly popular, it's more important than ever that companies let parents know how their kids' data is collected and used and that they take reasonable steps to secure that data" [21]. A blog post was posted on the FTC website by one of the FTC's Senior Attorneys, with the headline "VTech settlement cautions companies to keep COPPA-covered data secure." It is clear that this case was meant as a warning bell to other connected toy companies. Many of these toy companies had recently experienced security scandals as discussed in ¡section¿. A study in 2018 showed that the majority of children's apps were likely in violation of COPPA, despite apps having been the target of FTC investigations for years [33]. This makes it likely that many more IoT toy companies were also in violation of COPPA, beyond those with public scandals.

Costs of COPPA Compliance

COPPA is a complex, many layered law, and the cost of compliance is high. In 2000, the House of Representatives' Committee on Commerce estimated a cost of $115,000 to $290,000 per year for a mid-sized children's website [15]. The challenges and costs of compliance can be so great that many companies choose to simply exclude children under the age of thirteen from their customer base. Companies ranging from Facebook [18] to Steam (an online game platform) [34] do not allow minors under the age of 13 to make accounts to avoid COPPA requirements, despite the loss of market opportunities caused by this. However, connected toys were often explicitly marketed at young children, with their monitoring capabilities marketed as a feature.

Prior to the FTC's guidance that connected toys must comply with COPPA, it is likely that many of these companies were not in compliance, as evidenced by the many data breaches that came to light. Following the guidance and subsequent settlement with VTech however, the risk of ignoring COPPA increased greatly. The complexities and costs of compliance that caused many companies to avoid children's technology all together now had to be borne by connected toy companies.

Discussion

Given that parents are not adverse to sharing their children's sensitive data with these companies, we propose that the decline of IoT toys was not driven by parental concerns. If any aspect of public opinion was the driving force of the decline, we believe it would have been the lack of utility of these toys for parents and children. Rather, we propose that the driving cause was regulatory; changes in enforcement in 2017 impacted the subsequent decline of connected toys. The increased severity of regulation and the financial cost of failing to comply made building connected toys a more complex, expensive, and risky process. The impacts of stricter enforcement on IoT toys is a key case study of the effect policy can have on mitigating privacy concerns.

While we believe policy was a driving factor, it is also evident that significant negative publicity can impact companies as well. For example the FTC had only begun investigations into the recently publicized security flaws of My Friend Cayla when the toy was taken off market [16]. This supports our claim that FTC investigations can have impacts on the market, but the rapidness of the toy being discontinued indicates that parental concern was also relevant. As discussed in ¡Section¿, parents find toys acceptable so long they believe basic privacy requirements are being met. When privacy flaws are prominent in the news this condition is violated, and parents may withdraw their support.

While many IoT toys are discontinued, there is much that can be learned from the rise and fall of these devices, and the impact policy had on their popularity. Children are a large share of the market that many large businesses are now looking to expand into. Facebook is working on Instagram for Kids, a social media site targeted at children [26]. Youtube has Youtube Kids, a contained way for children to explore Youtube and parents to monitor them [41]. We propose the following implications of our research that policymakers should consider when drafting policy that will regulate the technology that interacts with children.

1. The FTC's enforcement choices are powerful signals to industries. As discussed in this paper, the existence of laws and rules alone are not enough to promote security. It is often infeasible for the FTC to evaluate the security of every new product before the product goes to market, so the system relies on FTC complaints and investigations. If the FTC does not take sufficient enforcement action in some section of industry, many companies in that section may decide the risks of not complying to not outweigh the costs of compliance.

2. The timeline of the FTC drafting guidance that applies existing rules / laws to new technologies can have a significant impacting on security and market growth. Laws often struggle to keep up with changing technology. This is commonly said, and research has been done on designing a legal system that can "cope in a rapidly changing technological environment" [14]. As it stands today, the benefit of giving the FTC rulemaking and guidance power is it allows the Commission to adapt rules and guidance to new technology. The legislators who drafted COPPA likely never imagined connected toys existing, and yet that same legislation regulates connected toy manufacturers, due to FTC enforcement.

The responsibility lies on the FTC to constantly survey industry for emerging technologies that should be regulated under existing laws. Seven years passed between the emergence of Jibo, the earliest IoT Toy discussed in this paper, and the FTC guidance explicitly including IoT devices under COPPA. This lag in regulation can result in new technologies evolving without compliance in mind, as we saw with the lax security measures taken by IoT manufacturers. Therefore, it is essential that the FTC releases clear guidance about new technologies early and updates that guidance regularly.

3. Given the privacy / security views of parents, the parental informed consent model for protecting privacy should be reviewed for efficacy. The synthesization of existing research on parental views of their children's privacy and security make clear that parents are willing to share quite a bit of information about their children. In the United States, data collection is tied to consent. COPPA sets requirements for how the data of children is protected, but ultimately, as long as parents consent and data is properly stored and protected, manufacturers targeting children can collect any type of data. However, informed consent is not the only model for protecting children's privacy.

The European Union and the General Data Protection Regulation (GDPR) go beyond the informed consent model. For any type of data a company seeks to collect, they must explain why it is necessary to obtain that data. In this case, the burden of scrutinizing a company's data collection and the privacy and security of their toys lies with the government and companies, rather than with parents. Placing this burden on experts in the government and the field can provide better privacy and security protections for consumers. It has been shown that consumers rarely read the ToS of their products,adults and children both have poor understanding of IoT devices with recording capabilities, and they are often not informed enough to provide their full consent for using IoT devices, so

Another option is to revise the way informed consent is given, using Apple's recent IPhone privacy changes as a model. Periodically, iPhones send push notifications informing the user about the data that different apps are collecting and give them options to approve or deny the data collection, all in clear, user-friendly terms. Users are frequently reminded of what data they are giving to different companies and they can control their privacy settings piece by piece without the burden of reading through an entire Terms of Service for each app [38].

These solutions are two of many, but as technology changes faster and becomes more complex, it becomes harder for consumers to fully understand the devices they purchase;Informed consent will become less and less reliable. There is room for improvement, and the FTC should take inspiration from other countries or within the industry itself.

4. Strict security legislation may have outsized impacts on small businesses while having smaller impacts on large companies. As COPPA stands today, it is challenging for a small business to be confident they are in full compliance. There are many layers of rules, expectations, and details that can significantly raise the cost of producing compliant technology. If a small business is found to be non-compliant, the fees levied by the FTC can be devastating.

In contrast, large companies have significant, existing legal teams devoted to teasing out the nuances of how security legislation applies to their product. When they are found in violation, the fees are often paltry compared to the profits and size of the business. In 2019, Google paid a $170 million fine in a settlement of COPPA violations on Youtube. Many claimed that in contrast to Alphabet's 30 billion dollar yearly revenue, this fine was meaningless [13].

When developing future security legislation, it is essential to consider the different impacts that occur on small vs large businesses. There is significant risk that new regulations can fail to significantly increase consumer security, but levy high costs and create barriers to entry for small companies. Legislation should consider both the efficacy of security requirements and the affordability of investing in compliant security and privacy standards.

Conclusion

There are many lessons to be learned from the decline of IoT toys and the role of public policy. Even though parents and children were still open to these types of devices, it is likely that FTC enforcement of COPPA forced companies to choose between shutting down or meeting compliance, which is incredibly expensive and difficult for smaller businesses. This phenomenon shows that policy is a feasible route to better security and privacy, but in writing legislation, it is important to consider the implications we highlighted in the discussion. As the reach of technology expands with the use of speech recognition devices and other invasive technologies like facial recognition, it is important to have robust, thoughtful policies addressing the new technology.

References

[1] Home automation in the wild: challenges and opportunities. *CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011. URL https://dl.acm.org/doi/10.1145/1978942.1979249.

[2] From nosy little brothers to stranger-danger:children and parents' perception of mobile threats. *IDC*, 2016. URL https://dl.acm.org/doi/pdf/10.1145/2930674.2930716.

[3] German parents told to destroy cayla dolls over hacking fears, 2017. URL https://www.bbc.com/news/world-europe-39002142.

[4] Data from connected cloudpets teddy bears leaked and ransomed, exposing kids' voice messages, 2017. URL https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/.

[5] Hello barbie, 2017. URL http://hellobarbiefaq.mattel.com/.

[6] Toys that listen:a study of parents, children, and internet-connected toys. *CHI*, 2017. URL https://techpolicylab.uw.edu/wp-content/uploads/2017/10/Toys-That-Listen_CHI-2017.pdf.

[7] Alexa, are you listening? privacy perceptions, concerns, and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction (PACM HCI)*, 2018. URL https://dl.acm.org/doi/pdf/10.1145/3274371.

[8] Exploring parents' security and privacy concerns and practices. *Workshop on User Security (USEC)*, 2018. URL https://www.ndss-symposium.org/wp-content/uploads/2018/07/usec2018_04-3_Alqhatani_paper.pdf.

[9] Jan 2018. URL https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_stip_order_1-8-18.pdf.

[10] Evaluating the contextual integrity ofprivacy regulation: Parents' iot toy privacy norms versus coppa. *USENIX Security Symposium*, 2019. URL https://www.usenix.org/system/files/sec19-apthorpe.pdf.

[11] Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019. URL https://par.nsf.gov/servlets/purl/10109137.

[12] Jibo, 2021. URL https://jibo.com/.

[13] Barret. YouTube's Case Shows FTC Fines Alone Won't Slow Down Big Tech | WIRED, 2019. URL https://www.wired.com/story/youtube-ftc-fines-alone-arent-enough/.

[14] Lyria Bennett Moses. Recurring Dilemmas: The Law's Race to Keep Up With Technological Change. *SSRN Electronic Journal*, 2007. ISSN 1556-5068. doi: 10.2139/ssrn.979861. URL http://www.ssrn.com/abstract=979861.

[15] Anupam Chander, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park, and Isabel Yu. *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation.* Policy Research Working Papers. The World Bank, March 2021. doi: 10.1596/1813-9450-9594. URL http://elibrary.worldbank.org/doi/book/10.1596/1813-9450-9594.

[16] Gordon Chasseau. FTC Will Consider Spying Toy Privacy Concerns - Privacy - United States, 2017. URL https://www.mondaq.com/unitedstates/privacy-protection/569600/ftc-will-consider-spying-toy-privacy-concerns.

[17] S. Crowe. Anki addresses shutdown, ongoing support for robots, 2019. URL https://www.therobotreport.com/anki-addresses-shutdown-ongoing-support-for-robots/.

[18] Facebook. How do I report a child under the age of 13 on Facebook? | Facebook Help Center, 2021. URL https://www.facebook.com/help/157793540954833.

[19] FBI. Internet Crime Complaint Center (IC3) | Internet-Connected Toys Could Present Privacy and Contact Concerns for Children, 2017. URL https://www.ic3.gov/Media/Y2017/PSA170717.

[20] FTC. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, June 2013. URL https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[21] FTC. Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act, January 2018. URL https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

[22] FTC. Guidance Documents, 2021. URL https://www.ftc.gov/enforcement/guidance.

[23] Heater. The smart speaker market is expected to grow 21 percent next year, 2020. URL https://techcrunch.com/2020/10/22/the-smart-speaker-market-is-expected-grow-21-next-year.

[24] P. Davidsson J. Bugeja, A. Jacobsson. On privacy and security challenges in smart connected homes. *European Intelligence and Security Informatics Conference (EISIC)*, 2016. URL https://doi.org/10.1109/EISIC.2016.044.

[25] Hunton Andrews Kurth. Amended COPPA Rule Comes into Effect, July 2013. URL https://www.huntonprivacyblog.com/2013/07/01/amended-coppa-rule-comes-into-effect/.

[26] Kim Lyons. Facebook is working on a version of Instagram for kids under 13, March 2021. URL https://www.theverge.com/2021/3/18/22338911/facebook-instagram-kids-privacy-coppa.

[27] Meola. Smart farming in 2020: How iot sensors are creating a more efficient precision agriculture industry, 2021. URL https://www.businessinsider.com/smart-farming-iot-agriculture.

[28] F. Myrstad. Connected toys violate european consumer law, 2016. URL https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/.

[29] O'Neill. Insecurity by design: Today's iot device security problem. *Engineering*, 2016. URL https://core.ac.uk/download/pdf/82794567.pdf.

[30] Phaneuf. The security and privacy issues that come with the internet of things, 2021. URL https://www.businessinsider.com/iot-security-privacy.

[31] Phaneuf. Latest trends in medical monitoring devices and wearable health technology, 2021. URL https://www.businessinsider.com/wearable-technology-healthcare-medical-devices.

[32] Puri. Iot enabled shipping containers sail the high seas improving global supply chains, 2021. URL https://www.networkworld.com/article/3432170/iot-enabled-shipping-containers-sail-the-high-seas-improving-global-supply-chains.html.

[33] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies*, 2018(3):63–83, June 2018. ISSN 2299-0984. doi: 10.1515/popets-2018-0021. URL https://www.sciendo.com/article/10.1515/popets-2018-0021.

[34] Steam. Steam Subscriber Agreement, 2021. URL https://store.steampowered.com/subscriber_agreement/.

[35] Genesis Toys. My friend cayla, 2021. URL https://www.genesis-toys.com/my-friend-cayla.

[36] Tuohy. The best automation devices and how to use them, 2021. URL https://www.sciencefocus.com/future-technology/smart-home-the-best-automation-devices-and-how-to-use-them/.

[37] J. Vincent. This 'smart' barbie is raising concerns over children's privacy, 2015. URL https://www.theverge.com/2015/3/16/8223251/hello-barbie-speech-recognition-privacy.

[38] Wamsley. Apple Rolls Out Major New Privacy Protections For iPhones And iPads, 2021. URL https://www.npr.org/2021/04/26/990943261/apple-rolls-out-major-new-privacy-protections-for-iphones-and-ipads.

[39] Wired. The dolls have ears, 2017. URL https://blog.mozilla.org/internetcitizen/2017/08/21/iot-surveillance/.

[40] Wired. Security news this week: An iot teddy bear leaked millions of parent and child voice recordings, 2017. URL https://www.wired.com/2017/03/security-news-week-iot-teddy-bear-leaked-millions-parent-child-voice-recordings/.

[41] Youtube. YouTube Kids - An App Made Just For Kids, 2021. URL https://www.youtube.com/kids/.