CHILD'S PLAY: EXPLORING AWARENESS OF THE INTERNET OF TOYS: A LITERATURE REVIEW

by

MICHELLE WILLIAMS

B.S., Purdue Global University, 2001

M.S., Stevenson University, 2008

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2024

Child's play: exploring awareness of the Internet of toys: a literature review

Michelle Williams, *Middle Georgia State University, michelle.williams3@mga.edu*

Abstract

The Internet of Toys (IoToys) is becoming more prevalent in households as parents buy them for their children. Do parents understand the dangers of IoToys and take precautions to safeguard their children's privacy? When a parent consents to the IoToy or associated application, the company collects and owns the data. The ability to gather data and the potential for data misuse make IoToys a privacy risk for kids. IoToy vulnerabilities can potentially result in the hacking or compromise of toys. The article will discuss COPPA regulations that are in place to safeguard children's privacy and will show that they are not enough. This article also addresses the privacy concerns that parents should consider. Parental responsibilities and controls are also discussed. IoToys are mainly for child's play, but parents must be concerned about bringing a connected toy into their household.

Keywords: Internet of Things; Internet of Toys; IoT; IoToys; smart toys; connected toy; privacy (children); COPPA; data protection

Introduction

The Internet of Things (IoT) has opened other markets for internet-connected devices, including the Internet of Toys (IoToys). An IoToy is a toy mainly targeted at children, is software-based, and represents 1. Connectivity, 2. Interaction, and 3. Programmability (Brito *et al.*, 2018). Security and privacy are issues with anything connected to the Internet. Do parents have a role in securing an IoToy for their child? Traditional toys differ from IoToys because they cannot transmit or learn data; they do not provide the same privacy concerns (Allana, 2023). Allana also writes that IoToys have various built-in sensors, voice recognition, location tracking, data storage, peer and cloud communication, and other capabilities. IoToys have become digital playgrounds for children aged 3 to 12 who are excluded from many social media platforms because of their age (Allana, 2023).

Regulatory acts such as COPPA help mandate how toys should comply with children under 13, and device manufacturers are not taking privacy and security seriously over ease of use of the device (Haber, 2019). While parents are concerned about children playing with internet-connected toys and the educational, social, and psychological concerns that can arise from exposure to the Internet, are they also aware of what data transmits from IoToys? Parents have privacy implications about IoToys, but are they reading the fine print of the user agreements? IoToys pose several risks to children's privacy, including the ability to collect data and the possibility of data misuse. Vulnerabilities in IoToys can also lead to toys being hacked or compromised. The current state of regulations regarding IoToys only partially protects the child's security and privacy.

IoToys is an emerging market integrating Internet of Things (IoT) technology with toys, creating interactive and connected play experiences (Allana, 2023). The rapid increase of IoToys raises significant concerns regarding privacy implications and security; what role do parents have in facilitating the challenges and potential risks? Misuse of children's data collection should be a primary concern when dealing with IoToys

(Haber, 2019). Parents are the first line of defense against these concerns. Therefore, it is essential to study the significance of parents' privacy and security concerns, if any.

This study aimed to explore existing literature and gather information about parents' perceptions of IoToys. There are implications of IoToys, including potential risks and challenges in integrating Internet of Things (IoT) technology with toys (Allana, 2023). By investigating parents' role in shaping children's perceptions and interactions with IoToys, we can also explore if parents are aware of the data that can be transmitted or if parents are monitoring their child's IoToys. A thorough analysis enhances the understanding of parents' privacy and security concerns related to IoToys and provides insights to various stakeholders, including policymakers, manufacturers, and parents.

This review will highlight gaps in the current research and suggest avenues for future studies in this area. Consistent with the study's purpose, this research will answer the following questions:

What does the current literature say about the perceptions of security and privacy of IoToys among parents, and how do these perceptions influence the data collected?

Review of the Literature

Defining IoToys

Before discussing parents' awareness of the digital content collected from their children's toys, it is necessary to define IoT and IoToy. "The Internet of Things (IoT) is a network of physical items called "things" that have implanted sensors, software, and other technologies to communicate and exchange data with other devices and systems through the Internet" (Colin & Perry, 2019, p. 11). Most devices connected to the Internet until 2000 were computers of various sizes, and the first sector to connect devices to the Internet was geared toward consumers (Colin & Perry, 2019). Children's toys with internet connectivity are a subset of IoT, coined the Internet of Toys (IoToys), like other IoT devices (Chu *et al.,* 2018). For this review, IoToys, internet-connected toys, and smart toys will be synonymous, or any toy that connects to the Internet to share data to control the toy's communication. (Collingwood, 2021).

Current Regulations

The current regulations that oversee IoToys are limited. Policymakers were concerned about "the potential datafication and misuse of children's data long before" IoToys were developed (Haber, 2019, p. 402). Haber (2019) pointed out that the environment when COPPA was enacted in 1998 differed from today's internet environment. Congress could not have predicted the technological advancements that led to IoToys, but the COPPA framework still applies. In 2017, the FTC updated its guidance to include toys, and the "new direction highlighted that COPPA does not apply only to websites and mobile applications but also to the growing list of connected devices that make up the Internet of Things" (Seth, 2021, p. 12). Under the COPPA framework, online service providers and device manufacturers have specific legal obligations and must meet requirements to comply with the FTC regulations. Parents cannot verify if the IoToy follows COPPA guidelines (Chu *et al.,* 2018). Unsurprisingly, the FTC recently announced that it would review the COPPA regulations (Collingwood, 2021).

No standardized or widely recognized rating system is dedicated to IoToys (Allana, 2023). Children rely on parents for their privacy, and current parental controls are insufficient and lack compliance from toy makers (Allana, 2023). Parental controls can help parents choose the privacy level for the IoToy's data. Available IoToys parental control tools provide limited features without concern for privacy and data collection or security (Albuquerque *et al*., 2022). There are no parental control standards for the IoToy maker industry to follow or guidelines that they can use to help parents select the level of privacy for their children.

Privacy Concerns

Holloway and Milosevic (2019) suggest connected toys can pose privacy threats and new vulnerabilities as issues while a child plays with IoToys. The article states that IoToys introduce a new level of play for children; advanced toys are connected to the Internet, can interact with children, and can be coded by the user. IoToys offer new personalized space and learning opportunities and raise new concerns and issues (Mascheroni & Holloway, 2017). How IoToys uses, shares and stores children's personal information should be a significant concern for parents. You can own the physical toy, but the children and their parents have no control or ownership over the personal data that the toy producer or service provider collects (Holloway & Milosevic, 2019). Who is responsible for the personal data collected via connected toys? Holloway and Milosevic (2019) state that "(w)hen parents or older children log on and sign up to internet services that support the toy (in order to access the full play experience), little choice is given regarding data usage" (p. 30). Parents *allow* their children's data to be collected. According to the conditions of use for the device, the toy manufacturers control the data that has been collected, and they seem to have the ability to share it (Collingwood, 2021).

Parental Responsibility and Controls

The market for smart toys is expanding and profitable for toy manufacturers. "It is estimated that the size of the global toy market is more than 87 billion U.S. dollars annually, of which about one quarter can be attributed to the North American market" (Collingwood, 2021, p. 76). The IoToys market will grow by 200% from 2018 (Solera-Cotanilla *et al*., 2022). Parents are buying children's toys that connect to the Internet, but are they aware of what they will share? Collingwood (2021) explains that allowing children to play with an IoToy connected to the Internet falls on the parent or caregiver, as they set the privacy and data sharing parameters with the toy manufacturers. If parents are concerned about privacy, are they reading the end-user-license agreement when they sign their children up to access the IoToy? Parents are often worried about privacy but are often unaware of the privacy concerns that could arise from playing with internet-connected toys and do not realize that data is being recorded (McReynolds *et al*., 2017)

McReynolds *et al*. (2017) explore the idea of parental controls. Out of every parent surveyed about Hello Barbie, they all expressed that the toy should have parental control. "In contrast, no parent commented on the email they received during the Hello Barbie setup process, which asked them to agree to allow their child to play with the toy" (McReynolds *et al*., 2017, p. 5203). The authors concluded that most parents quickly clicked through the screens requesting permission without commenting or slowing down to read. Parents also had a big orange button that reads "I Give Permission," which permitted the app associated with Hello Barbie to audio record their child's play. When one parent tried to "Revoke Permission" after accepting, within a minute, Hello Barbie stopped working (McReynolds *et al*., 2017, p. 5203).

Methodology

A literature search was conducted on the GALILEO, a virtual library portal through the University System of Georgia and Google Scholar databases until December 2023. A search strategy was performed with the following terms: Internet of Toys, IoT, IoToys, IoToys privacy, IoToys security—inclusion criteria where the abstract text includes relevant content, as judged by this researcher. The stages of a systematic review approach include establishing a protocol and starting the search for peer-reviewed research articles, books, and literature-reviewed research (Page, 2021).

The inclusion of literature for this review was based on articles published in English with full-text available and containing a keyword identified for the search criteria. The primary sources of literature were identified as research articles and journals. Additional articles were identified based on significant articles' citations. Articles were subjected to date range restrictions and were chosen from the last ten years, 2013-2023. This review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to help ensure transparency and consistency in the methodology and reporting (Page, 2021). As part of the review process, published studies and research were analyzed based on parents' perspectives on the security and privacy of IoToys. Exclusion criteria included nonempirical reviews, neither published in English nor between 2013-2023.

The PRISMA flow diagram in Figure 1 displays the number of articles included and excluded throughout the selection process following the PRISMA statement and study eligibility criteria.

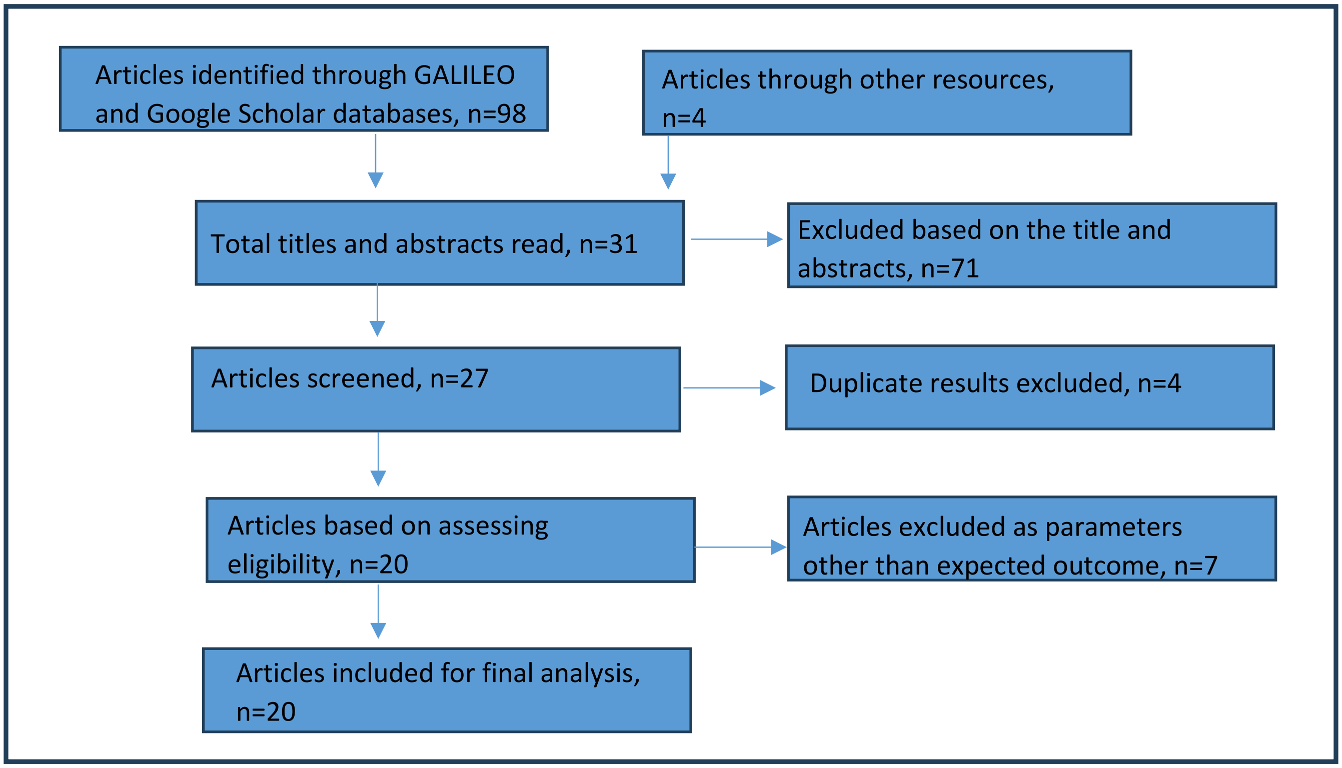
Articles identified through GALILEO and Google Scholar databases, n=98
Articles through other resources, n=4
Total titles and abstracts read, n=31
Excluded based on the title and abstracts, n=71
Articles screened, n=27
Duplicate results excluded, n=4
Articles based on assessing eligibility, n=20
Articles excluded as parameters other than expected outcome, n=7
Articles included for final analysis, n=20

Figure 1: Chart Diagram for Article Inclusion and Exclusion

Results

The PRISMA guidelines were followed to guide the analysis of this review but omitted the sections relating to meta-analysis (Page, 2021). A total of 20 articles were selected out of the 102 collected based on search criteria for this review (Figure 1). They were included in the systematic review after screening titles, abstracts, and full-text articles against predefined inclusion and exclusion criteria. After a search on GALILEO and Google Scholar databases, 102 records were identified. After screening the titles and abstracts, 71 articles were eliminated, leaving 31. Four duplicate records were identified and eliminated. After full-text screening, seven articles were removed, leaving 20 articles included in the final analysis.
Table 1 presents the articles that were included in the final review. Statements relating to privacy concerns, security concerns, data collection, parents' perceptions, and regulations were sorted by themes related to each topic. Several themes appeared in more than one of the categories.

The current literature's insights regarding parents' perceptions of the security and privacy implications of IoToys emphasize concerns regarding the potential risks associated with IoToy devices. Parents are worried about IoToys collecting, storing, and using their children's data. They share fears of unauthorized access, data breaches, and exploitation of sensitive information. IoToy device manufacturers' lack of transparency in data collection leaves parents uncertain about how and where the data is going.

Table 1: Included Articles

Author	Year	Title	Theme(s) Identified	Article Summary
Albuquerque *et al.*	2022	Recommendations for a smart toy parental control tool	Data Collection Privacy Concerns Security Concerns	Discusses current parental control tools environment and how implementation would help safeguard what data is collected.
Allana, S.	2023	Improving the scalability of a rating system for assessing safety of Internet of Toys.	Data Collection Privacy Concerns Security Concerns	A rating system for parents should be implemented to educate parents on data collection and concerns.
Brito *et al.*	2018	Young children, digital media and smart toys: How perceptions shape adoption and domestication.	Parents' Perception Security Concerns	Discusses children and their IoToys practices and the adoption into families.
Chu *et al.*	2018	Security and Privacy Analyses of Internet of Things Children's Toys.	Privacy Concerns Regulations Security Concerns	Investigated IoToys privacy and security and how they violate COPPA regulations.
Collingwood, L.	2021	Villain or guardian? "The smart toy is watching you now ...."	Data Collection Privacy Concerns Security Concerns	How IoToys are used, and what is collected from them. Safety regulations need to be evaluated.
Fosch-Villaronga *et al.*	2023	Toy story or children story? Putting children and their rights at the forefront of the artificial intelligence revolution.	Regulations Security Concerns	The impact IoToys have on children and the need for policymakers to understand the security concerns.
Gaeta, M.C.	2020	Smart Toys and Minors' Protection in the Context of the Internet of Everything.	Data Collection Regulations Security Concerns	Need to consider the ethical implications of IoToys and keeping the laws up to date as the technology.
Haber, E.	2020	The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World.	Privacy Concerns Regulations	IoToys should not compromise children's privacy, and safeguards should be implemented and required by policymakers.
Haber, E.	2019	Toying with Privacy: Regulating the Internet of Toys.	Parent's Perception Privacy Concerns Regulations	Children have the right to privacy, and regulations should help to protect children's data.
Holloway *et al.*	2016	The Internet of toys.	Data Collection Privacy Concerns Security Concerns	Data from IoToys are collected and disbursed without the concern for privacy and security.
Hughes *et al.*	2019	Making Future-Ready Students with Design and the Internet of Things.	Privacy Concerns	A small group of children brainstormed and designed IoT devices based on a set of instructed guidelines.
Kirtley *et al.*	2018	Too Smart for Its Own Good: Addressing the Privacy and Security Challenges of the Internet of Things.	Privacy Concerns Security Concerns Regulations	The Federal Government has introduced regulatory acts to help address privacy and security concerns with IoT devices.

Table 1 (continued): Included Articles

Author	Year	Title	Theme(s) Identified	Article Summary
Lopez *et al.*	2021	Protecting Minors in Relation to Interactive Software.	Regulations	More regulation should be considered for video games and interactive software for children.
Mascheroni *et al.*	2017	The Internet of Toys: A report on media and social discourses around young children and IoToys.	Parent's Perception Security Concerns	Small study to introduce IoToys to children and the risks associated with them.
Mascheroni, G.	2020	Datafied childhoods: Contextualising datafication in everyday life.	Data Collection Privacy Concerns	Introduces an overview of dataficiation and dataveillance of children.
McReynolds *et al.*	2017	Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys.	Parents Perceptions Privacy Concerns Security Concerns	A study on IoToys, observations, and interviews was conducted on nine families.
Nikolopoulou, K.	2021	Internet of Toys for Young Children: Educational Value or Threat?	Data Collection Privacy Concerns Security Concerns	Discusses the potential benefits and risks associated with IoToys and children. Do the potential risks outweigh the benefits of the device?
Seth, M. K.	2021	Protecting Children's Privacy in the Age of Smart Toys.	Privacy Concerns Regulations	Discusses COPPA and FTC best practices and how they relate to toy manufacturers.
Solera-Cotanilla *et al.*	2022	Security and Privacy Analysis of Youth-Oriented Connected Devices	Privacy Concerns Security Concerns	Study between 13-17 year olds and their relationship with IoT devices.
Turner, S.	2020	Connected Toys: What Device Documentation Explains about Privacy and Security.	Privacy Concerns Security Concerns	Discusses documentation and how it relates to the privacy and security of IoToys.

Discussion

The growing market of IoToys combines IoT with traditional toys, offering interactive and connected play opportunities (Allana, 2023). The quick expansion of IoToys brought concerns regarding privacy and security implications. Parents have a responsibility to navigate these challenges and mitigate potential risks. Parents play a pivotal role as the primary guardians against such concerns, so understanding the extent of apprehensions regarding privacy and security is necessary.

Data Collection

IoToys, which integrate Internet of Things (IoT) technology with traditional toys, often involve general data collection processes. Many IoToys have similar attributes and are alike in that they require activating an account in which the toy sends data to a remote location (Haber, 2019). The data at the remote site can then be datamined and analyzed by whomever the manufacturer has designated (Haber, 2019). Some IoToys constantly collect data from the device as children perform and interact with the toy. This continuous monitoring leads to data collection of personal and sensitive information. Data collected may include, but is not limited to, audio recordings, video footage, GPS location data, usage patterns, and performance metrics of the device (Albuquerque, 2022).

The main concern for data collection is who owns the data once created. Children and their parents may not have complete control over the data collected by the devices, mainly if it includes an app owned or operated by third-party companies (Albuquerque, 2022). It is unclear how data is gathered, used, and shared, as well as the potential risks associated with data manipulation (Albuquerque, 2022). "These opt-in-opt-out choices allow toy companies and their service providers to enter into long-term contractual agreements that transfer legal responsibility for the collection, analysis, and distribution of children's data to parents, and this effectively gives commercial entities the authority to continue and conceivably expand upon data-collecting and sharing procedures" (Holloway & Green, 2016, p. 7). Parents are normalized to data collection and surveillance of their children (Mascheroni, 2020). The processes that allow the IoToys to operate are unclear to parents, which makes them unaware of what data can and will be collected (Allana, 2023).

Data collection purposes in IoToys vary, ranging from improving product functionality and personalizing user experiences to provide valuable insights for product development and marketing strategies (Chu *et al)*. Parents need the ability to safeguard data that is collected from the possibility of data misuse. Misused data can be used in various ways, including targeted advertising, surveillance, and profiling (Collingwood, 2021). "The functionality of these toys enables data exchange between multiple stakeholders," which should be a significant concern. (Collingwood, 2021, p. 76). Without proper safety measures, the data collected could be exploited for unethical or harmful practices (Haber, 2019). If the manufacturers own the collected data, they can also sell it for commercial purposes to whomever is interested (Haber, 2019). It would not be easy to assess the data collected and who currently has access to it (Haber, 2019).

Manufacturers need to inform stakeholders of what data is collected and who will have access. "If third-party analytics companies receive data from numerous smart toys, they could similarly construct detailed profiles of individual children's behaviors, as well as large-scale datasets about smart toy users of value to manufacturers and distributors" (Chu *et al.,* 2018, p. 6*).* However, concerns develop regarding data collection's privacy and security implications, particularly concerning the sensitive nature of children's personal information and the potential risks of unauthorized access or misuse. Manufacturers are not taking accountability for the privacy and security concerns and failures of IoToys (Holloway & Green, 2016).

Privacy Concerns

Data privacy was a significant theme of concern among parents regarding IoToys. Anything connected to the Internet can be a target for hackers. Some concerns included the potential sub-themes of privacy concerns, highlighted unauthorized access to data, and a lack of transparency regarding what data is collected. Parents entrust the manufacturer to protect the data that is being collected, not to be hackable or released. When the Mattel toy Hello Barbie was hacked in 2015, data such as the Wi-Fi networks and identifiable account details could be collected (Holloway & Green, 2016). The security level of the Hello Barbie relied on the paternal choice when the toy was set up; if the parents chose the option of storing audio files, the files were then stored in the cloud and could be accessed from the Internet (Holloway & Green, 2016).

Children who play with IoToys may enjoy the functionality of the games and even the educational value they receive. However, they are unaware of how the device communicates and collects their activity (Gaeta, 2020). Parents are ultimately responsible for safeguarding their children from misuse and keeping them safe from the outside world. "The safety and security of children's data requires companies to go beyond the 'opt-in-opt-out' paradigm of data privacy" (Holloway & Green, 2016, p. 2). Children are often not equipped to understand privacy policies and how their data is collected using IoToys (Turner, 2020). Parental consent is the method for managing children's use of IoToys, and parents do not usually read the privacy policies for their children's devices (Turner, 2020).

Data collection is an option that parents should be able to choose if they want to participate to protect their children's data privacy. Although some data may be needed to help improve features of the IoToys device, manufacturers might not need to store the data (McReynolds *et al.,* 2017). Reducing what is collected from the device or limiting the time data is saved can help decrease the risk of data exposure (McReynolds *et al.,* 2017).

Security Concerns

Security concerns were a theme identified through the literature reviewed. Security concerns have become increasingly prevalent as the Internet of Things (IoT) continues to increase into various aspects of daily life, including children's toys. The sub-themes identified in the literature with security concerns were the perceived vulnerability of IoToys' networks and the potential for data breaches. Parents frequently voiced concerns about cybersecurity risks associated with IoToys. Worries centered around connected toys' susceptibility to hacking and malicious attacks, which could compromise children's safety. The lack of visible security techniques in toy design frequently leaves parents unprepared and unskilled to tackle dangers that originate from them (Allana, 2023). IoToys, encompassing a wide range of connected devices such as smart dolls, interactive learning devices, gaming systems, and remote-controlled gadgets, present unique vulnerabilities that require attention.

"IoToys are the newest data-driven media platform to collect information about children's activities, interactions, preferences, and behaviors" (Holloway & Green, 2016, p. 6). There are security risks that parents may be unaware of when using IoT technology, mainly because the devices are connected to the Internet; they are a threat to the other IoT or IoToy devices (Kirtley *et al., 2018*). Parents must consider the security of all the interconnected IoT devices in their household (Hughes *et al*., 2019). "Many people interact daily with smart devices with little appreciation for the inner workings of IoT or its security and privacy considerations" (Lopez *et al.*, 2021, p. 1).

One of the primary security concerns with IoToys is the risk of unauthorized access to data breaches (McReynolds *et al.*, 2017). IoToys can collect and transmit sensitive information, such as voices, images, and patterns, and send data to remote servers. If these communication channels are not properly secured, hackers could intercept the data, leading to privacy violations, identity theft, and physical harm if the information gets into the wrong hands. Another concern is the potential for manipulation and exploitation of children through IoToys (Brito *et al., 2018)*. The child may own the IoToys device, but the child does not own the data it produces and, therefore, is out of the parent's control to maintain (Nikolopoulou, 2021). Data security standards should be introduced and regulated to help combat the security concerns of IoT (Solera-Contanilla *et al.,* 2022).

Parent's Perception

Parents need to learn about their children's activities on the Internet. The Internet has become increasingly widespread, self-regulated, and autonomous (Brito *et al.,* 2018*)*. The Internet shapes parents' perceptions of online risks, opportunities, and technologies and is also influenced by the media; therefore, parents have varied perceptions about IoToy technology (Mascheroni & Holloway, 2017). IoToys have prompted concerns among parents, legislators, and the public about how children's personal information is saved, processed, and distributed. (Mascheroni & Holloway, 2017). Many parents expressed a need for greater control over the data collected by IoToys. They emphasized the importance of transparent consent mechanisms and robust parental control features to manage data-sharing settings and restrict access to sensitive information (Brito *et al.,* 2018*.)*. However, studies highlighted varying levels of awareness and utilization of these control functionalities among parents.

With varied views of IoToys, both positive and negative perceptions emerge. Research suggests that parents with positive attitudes toward digital media are likelier to use participating and instructional styles to help their children develop digital skills (Chu *et al*., 2018). Parental education levels, socioeconomic status, and prior experiences with the Internet and technology help shape perceived perspectives. Additionally, the age and maturity of the child are essential factors. Parents with higher education, money, and experience with digital media are more likely to have positive attitudes about their children's usage of digital technologies (Brito *et al.,* 2018). A positive perception is that IoToys introduce children to technology early, helping them become familiar with digitalization (Brito *et al.,* 2018*).* Another positive impact is the entertainment value they can bring a child through interactive play and watching movies and videos (Brito *et al., 2018).*

Conversely, parents with negative perceptions are likelier to monitor and limit their children's digital practices (Chu *et al*., 2018). Potential datafication and misuse of children's data are both negative perceptions. "IoToys devices sound almost like every child's dream. But while many benefits might accrue, they may quickly become nightmares" (Haber, 2019, p. 401).

Conclusion

This systematic review surrounding IoToys reveals an environment embodied by enthusiasm for innovation and growing apprehensions regarding privacy and security concerns. The review of IoToys articles provided an overview of the findings, including identified themes related to perceptions of security and privacy among parents and their influence on children's use of these toys. The research shows that as the market for IoToys continues to proliferate, parents must navigate the challenges and potential risks while technology advances (Brito *et al*., 2018). Parents need to understand their role as primary guardians against privacy and security concerns; recognizing the scope of these concerns is critical for the collected data to be safeguarded (Chu *et al., 2018).* Research also suggests parental attitudes toward IoToys vary greatly, and they are impacted by digital literacy, socioeconomic position, and prior experiences with technology (Brito *et al.,* 2018). While some parents see IoToys as valuable tools for early technology exposure and interactive play, others are concerned about data privacy, security weaknesses, and the possible misuse of children's personal information (Haber, 2019). IoToy data collection raises significant questions about ownership, control, and transparency in data-gathering practices (Gaeta, 2020).

Research shows that data collection is a significant source of concern because of issues ranging from confusing permission methods to the possibility of third-party data misuse (Collingwood, 2021). Parents must weigh the advantages of individualized experiences and product development insights against intrusive surveillance and data exploitation risks (Fosch-Villaronga *et al.,* 2021). Security and privacy concerns highlight vulnerabilities in IoToys to unauthorized access and data breaches.

As a whole, parents need to be more accountable and better educated on the privacy and security concerns of IoToys. Once a better understanding is made, parents can be better prepared to demand improved protection. Parents need to urge manufacturers to adopt more transparent and better security practices to protect their children's right to privacy (Haber, 2020). As IoToys become more prevalent in children's daily lives, collaborative efforts between all stakeholders must come together for regulatory oversight to be updated and enforced (Gaeta, 2020). Therefore, robust privacy protections, transparent data practices, and compliance with relevant regulations must address these concerns and maintain trust among parents and users. Future studies should further investigate if IoToys manufacturers are adhering to safeguarding privacy and how they are implementing safeguards to protect the data.

This study is limited to a doctoral project's time constraints and space requirements. This is not an exhaustive study of the topic of security and privacy perceptions of IoToys among parents and their influenced perceptions.

While there is growing awareness of the security and privacy implications of IoToys among parents, more research is needed to understand the full extent of their concerns and how they influence data collection practices by toy manufacturers. Additionally, ongoing developments in technology and regulation may continue to shape parents' perceptions and the practices of toy manufacturers in this area.

References

Albuquerque, O., Fantinato, M., Hung, P. C. K., Peres, S. M., Iqbal, F., Rehman, U., & Shah, M. U. (2022). Recommendations for a smart toy parental control tool. *Journal of Supercomputing*, *78*(8), 11156–11194. https://doi.org/10.1007/s11227-022-04319-4

Allana, S. (2023). Improving the scalability of a rating system for assessing safety of Internet of Toys. *Computer Standards & Interfaces*, *83*, 103645. https://doi.org/10.1016/j.csi.2022.103645

Brito, R., Dias, P., & Oliveira, G. (2018). Young children, digital media and smart toys: How perceptions shape adoption and domestication. *British Journal of Educational Technology*, *49*(5), 807–820. https://doi.org/10.1111/bjet.12655

Chu, G., Apthorpe, N., & Feamster, N. (2018). *Security and Privacy Analyses of Internet of Things Children's Toys*. https://doi.org/10.1109/JIOT.2018.2866423

Colin, D., & Perry, L. (2019). *Mastering IOT: Build Modern IoT Solutions That Secure and Monitor Your IoT Infrastructure*. Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=nlebk&AN=2106795&site=eds-live&scope=site&custid=ns235467

Collingwood, L. (2021). Villain or guardian? "The smart toy is watching you now ...." *Information & Communications Technology Law*, *30*(1), 75–86. https://doi.org/10.1080/13600834.2020.1807118

Fosch-Villaronga, E., van der Hof, S., Lutz., C., & Tamò-Larrieux, A. (2021) Toy story or children story? Putting children and their rights at the forefront of the artificial intelligence revolution. AI Soc. 2023;38(1):133–152. doi: 10.1007/s00146-021-01295-w. Epub 2021 Oct 6. PMID: 34642550; PMCID: PMC8494166.

Gaeta, M. C. (2020). Smart Toys and Minors' Protection in the Context of the Internet of Everything. Eur. J. Privacy L. & Tech., p. 118.

Haber, E. (2020). The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World. *U. Ill. L. Rev.*, 1209.

Haber, E. (2019). Toying with Privacy: Regulating the Internet of Toys. *OHIO STATE LAW JOURNAL*, pp. *80*, 56.

Holloway, D., & Green, L. (2016). The Internet of toys. *Communication Research and Practice*, *2*(4), 506-519

Hughes, J., Robb, A., & Lam, M. (2019). Making Future-Ready Students with Design and the Internet of Things. *EAI Endorsed Transactions on Creative Technologies*, *6*(21), 1–9. https://doi.org/10.4108/eai.13-

Kirtley, J., & Memmel, S. (2018). Too Smart for Its Own Good: Addressing the Privacy and Security Challenges of the Internet of Things. *Journal of Internet Law*, *22*(4), 1–33.

López Jiménez, D., Carlos Dittmar, E., & Vargas Portillo, J. P. (2021). Protecting Minors in Relation to Interactive Software. *Law, State & Telecommunications Review / Revista de Direito, Estado e Telecomunicações*, *13*(1), 20–39. https://doi.org/10.26512/lstr.v13i1.29743

Mascheroni, G., & Holloway, D. (2017). The Internet of Toys: A report on media and social discourses around young children and IoToys. In *DigiLitEY* (No. June, pp. 3-52).

Mascheroni, G. (2020). Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology.*, *68*(6). https://doi.org/10.1177/0011392118807534

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 5197–5207. https://doi.org/10.1145/3025453.3025735

Nikolopoulou, K. (2021). Internet of Toys for Young Children: Educational Value or Threat? In *Handbook of research on using educational robotics to facilitate student learning* (pp. 424–439). IGI Global.

Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., & McKenzie, J. E. (2021). PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. International journal of surgery.

Seth, M. K. (2021). Protecting Children's Privacy in the Age of Smart Toys. *Landslide*, *13*(3), 10–61.

Solera-Cotanilla, S., Vega-Barbas, M., Pérez, J., López, G., Matanza, J., & Álvarez-Campana, M. (2022). Security and Privacy Analysis of Youth-Oriented Connected Devices. *Sensors*, *22*(3967), 3967–3967. https://doi.org/10.3390/s22113967

Turner, S. (2020). Connected Toys: What Device Documentation Explains about Privacy and Security.