6-18-2024

Protecting Child Online Data Privacy in the Age of AI: A COPPA Theoretical and Policy Analysis

John Wilkerson
Augusta University, jowilkerson@augusta.edu

Marcia Dailey
Clark Atlanta University, mdaley@cau.edu

Protecting Child Online Data Privacy in the Age of AI: A COPPA Theoretical and Policy Analysis

John Wilkerson
Augusta University
jowilkerson@augusta.edu

Marcia Daley
Clark Atlanta University
mdaley@cau.edu

ABSTRACT

The role of child data privacy and artificial intelligence-generated data copyright is an important topic in today's Smart communities. Policymakers, information security scholars, and parents must balance a child's Right to Privacy and growth with potential future artificial intelligence data copyright infringements across the internet. The purpose of this paper is to raise awareness of potential future artificial intelligence-generated child data privacy copyright infringements. Through the examination of information flow, privacy, and activity theories, this study identifies child data privacy protection sources as well as potential artificial intelligence child data copyright infringement opportunities. Furthermore, this research benchmarked 76 public privacy policies to contrast the child data privacy literature with real-world policy trends. This study expands the Information Security AI data copyright body of knowledge by identifying gaps in child data privacy and introducing a COPPA activity model to help explain one potential AI inference.

Keywords

Artificial Intelligence, Data Copyright Infringement, COPPA, PII, Activity Theory, Theory of Information Flow, Theory of Being Left Alone

INTRODUCTION

The internet is fundamental to today's child (Brown & Venkatesh, 2005). Many scholars argue that internet-enabled hardware, software, and next-generated artificial intelligence technologies are changing child online behavior at an extraordinary rate (Wang & Vella-Brodrick, 2018). Future extensive dependence on Internet technologies and next-generation artificial intelligence technologies open the door to countless challenges to the Child Online Data Privacy Protection Act (COPPA). The purpose of this paper is to raise awareness of artificial intelligence (AI)-generated child data privacy copyright infringements among state and city policymakers, information security (InfoSec) scholars, and parents. This study builds on the foundation of the Investigating Protected Healthcare Information Privacy: Smart City Policymaker Challenges paper (Wilkerson et al., 2023). This baseline InfoSec AI child, data copyright research, investigated user online behavior theories and established a data privacy policy framework for analyzing government and privacy security privacy policies. This paper explores Smart Community child online behavior and benchmarks 76 state and city government child privacy policies across three COPPA data privacy variables.

The study's methodology is detailed in section two, while section three describes the existing children's data privacy legal framework. Section four discusses closely related works, and section five analyzes random Smart Government privacy policies. Lastly, section six presents the findings of this study and highlights opportunities for further research. This paper asserts that some policymakers, InfoSec scholars, and parents may need to be made aware of potential AI-generated data copyright threats. Hence, this study answers the question: What are potential gaps in child online data privacy protection during an unsettled AI-generated data copyright governance era?

METHODOLOGY

This research paper analyzed the InfoSec body of knowledge gathered from conferences and databases from 2002 to 2023. One hundred and four journal articles and privacy policies from top libraries such as AIS, MIS Quarterly, and Management Science were reviewed. Initially, the study focused on research terms such as "children online protection," "children online privacy protection," and "human-centered behavior." The papers methodologies, theories, and findings were analyzed thoroughly. Therefore, new research topics were explored, specifically "artificial intelligence," "copyright data infringement," and "online user behavior." The paper also examined various federal, state, and local smart government law enforcement sources to define reasonable data privacy standards for children. This paper's study groups were segmented by state government and city government. Thirty-eight smart state governments and 38 smart cities' privacy policies were meticulously reviewed and either accepted or rejected based on the inclusion and exclusion criteria in the paper.

SMART COMMUNITY CHILDREN'S DATA PRIVACY LEGAL FRAMEWORK

The United States does not have a comprehensive data privacy law (Balaban, 2009). The 4th Amendment protects one's Right to Privacy (Henning, 2017). The Privacy Rights Act (PRA) of 1974 describes personally identifying information standards (McCallister et al. 2010). The Federal Trade Commission (FTC) and other legal partners are tasked with enforcing the Children's Online Privacy Protection Act (COPPA).

COPPA provides child data privacy security standards such as defining a child (aged 13 years or younger), setting an online contact standard, and describing what action online platforms should take before collecting, using, and disclosing children's personally identifiable information (PII) (FTC, 2013). However, some scholars argue that online content (child data) is free speech (open copyright) and is protected by the 1st Amendment (Post & Rothman, 2020). This child data privacy legal framework, child behaviors, as well as next-generate AI are likely threats to child data privacy in tomorrow's Smart communities.

CLOSELY RELATED THEORETICAL WORK

This study's theoretical groundwork was built by an introductory data privacy study published by the Midwest Association of Information Systems in August 2023. The initial research investigated InfoSec concepts such as the Theory of Information Flow and Theory of the Theory of Being Left Alone. This paper will briefly reintroduce these theories and dive deeper into the Activity Theory's relationships and AI-generated data privacy root causes (table 1.).

Theory of Information Flow

Consistent with the foundational study (Wilkerson et al. 2023), the internet is often categorized by open access and availability (Mousavi Baygi et al. 2021). The authors and First Amendment theorists Post and Rothman (2020) imply that online children's artifacts are one of many ordinary slices of the information flow of the internet. Internet artifacts such as cookies are key technologies that authenticate users and track user (child) online behaviors.

In contrast, Reyes et al. (2018) tested 5,855 online software apps for COPPA compliance (November 2016-March 2018). One hundred fifty-one apps transmitted child data to 3rd parties without consent (COPPA violation). One hundred fifty-six apps collected persistent cookies without consent (COPPA violation). Two hundred fifty-four apps collected child physical locations and other PII without (COPPA violation). The evidence is clear: COPPA violations can lead to future child AI data copyright challenges.

Theory of Being Left Alone

Corresponding with the introductory literature (Wilkerson et al., 2023), the Theory of Being Left Alone is focused on online users' data loss responses and users (parent and child) limited regard to share PII across education, entertainment, social media, and other online platforms. Theory of left-alone privacy theorists Culnan and Armstrong (1999) and Norberg and Horne (2007) infer that users' (parent and child) muted response to data privacy violations has become normalized, irrespective of potential AI-generated copyright data infringement threats.

Nevertheless, policymakers, InfoSec scholars, and parents must balance children's online data safety with education and entertainment technologies. For example, "Smart TVs" software platforms are standard tools to access countless internet streaming apps. Macioce (2018) points out that certain "Smart TVs" internet stream apps and data brokers utilize online identifiers to recognize the user's physical zip code, date of birth, and gender. The author also suggests that 18% of the population was identified online in 2014 with an unsupported computer operating system (OS). In sum, parent and child Theory of Being Left Alone followers are subject to education, entertainment, as well as OS email and other online software platforms.

Activity Theory

Allen et al. (2013) describes activity theory as linking a user's (child) feelings to their activity. Activity design theorists Barki et. al. (2007) reduces this theory's complexity by describing the relationship between three opposing forces: the community (people), child behaviors (process), technology (instrument), and outcomes (AI data copyright infringements) (Figure 1).

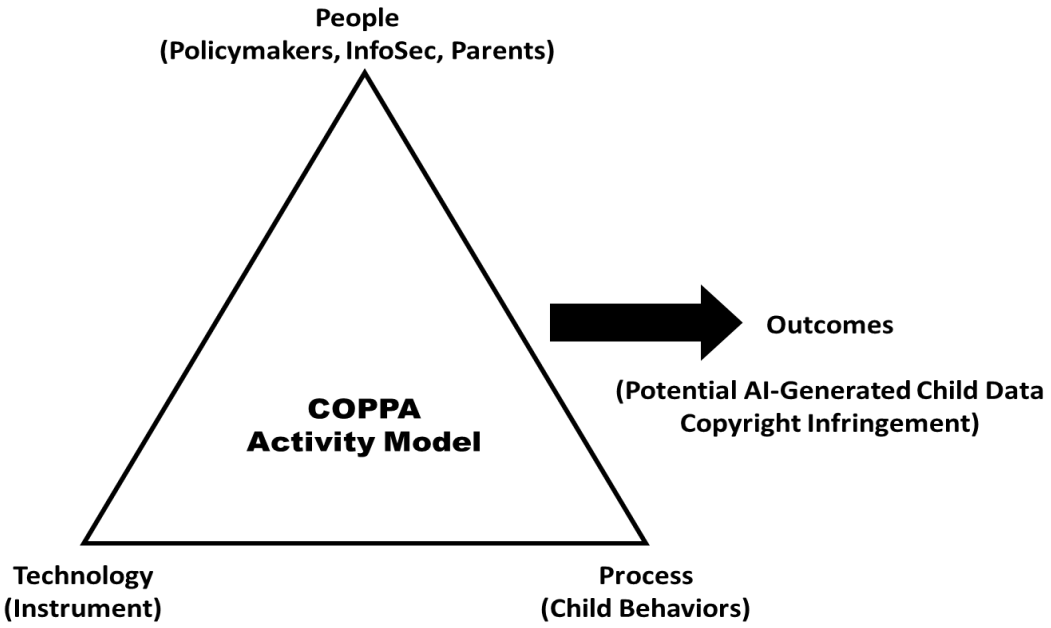

Figure 1. **COPPA Activity Model (Adapted from Engestrom's Activity System Model, 2000)**

The InfoSec literature infers that a larger societal framework shapes a child's motivation Minick (1989). With a multidisciplinary perspective, one could argue that the current behaviors of children and future outcomes are influenced by interventionist marketing and software-designed disciplines. Mehta et al. (2012) deduce that misleading food packaging could lead to unhealthy nutrition choices. Clearly, product design could lead to questionable child behaviors and long-term AI child data privacy infringements.

Future child, AI data copyright infringement, is also based on the premise that child-limited supervised internet use influences a kid's behavior and future outcomes. Radesky (2020) studied the behaviors of 346 children and parents with tablets and smartphones, children aged 3 to 5. This study concluded that all children were online for 115 minutes/day. This research determined that children with their devices averaged 240 minutes/day. Thirty-five percent of the unsupervised children's parents earned high incomes, obtained higher education, and were likely married. Kids visited child education, adult and child entertainment, and other online search platforms. It is reasonable to assume that many 3 to 5-year-old children have limited capacity to consent to child data privacy policies. This COPPA gap may trigger future AI-generated data copyright infringements debate.

Policymakers, InfoSec, and parents are operating in a conflicting and burdensome internet environment. Mulligan and King (2011) imply that policymakers must bridge the gap between social media websites, email /messaging platforms, and other online software apps. The authors argue that AI and other technologies have changed internet data privacy infrastructure. For example, social media news feeds track each user's click. Over time, each article clicked degrades a child's privacy. Bulgurcu et al. (2010) imply that the InfoSec community must first define and strengthen the information security gaps. This study reveals that limited online kid direction, partial child consent capacity (some demographics), and technological constraints such as cookies, email, and browsers could lead to potential COPPA violations.

The InfoSec Body of knowledge suggests that users (parents) must address two critical child data privacy decisions: understanding self-help and voluntarily controlling opportunities Cockcroft (2002). The author asserts that parents are accountable for their child's online consent, online access restrictions, and online data security awareness. The author could infer that understanding the relationship between child behaviors, COPPA violation sources, and technology is a crucial step toward a holistic child data privacy strategy (avoiding future data copyright violations).

InfoSec Data Privacy Theory	COPPA Violation Source	COPPA Technology	AI-Generated Child Data Privacy Copyright Infringement Root Cause	Reference
Theory of Information Flow	• Physical Location • Persistent Cookies • No 3rd Party Consent	Mobile Phone/Tablet 3rd Party Apps	• Product Design • Parent Consent	Reyes et al. (2018)
Theory of Being Left Alone	• Physical Location, Date of Birth, Gender Revealed	Smart TV (Online Identifiers) Data Brokers 3rd Party Apps	• Product Design • Parent Consent	Macioce (2018)
Activity Theory	• Cookies • Email/Messaging	Mobile Phone/Tablet Messaging / Email Apps	• Product Design • Parent Consent	Radesky (2020) Cockcroft (2002)

Table 1. Child Data Privacy Theory – AI Copyright Relationship Summary

SMART CITY CHILD PRIVACY POLICY ANALYSIS

This section examines four Smart Community data privacy variables described in this study's foundation paper. The Department of Justice and the Federal Trade Commission sets the data privacy policy standard for US entities (Wilkerson et al., 2023).

Smart Community Child Privacy Policy Analysis Results

1. The results of the analysis of the Child Privacy, Email Privacy, Persistent Cookies Privacy and 3rd Party Consent Privacy Policies for 38 states and 38 cities are shown in Table 2 and will now be discussed:
2. Child privacy policies reveal two trends. One, 56% of the randomly selected States comply with the federal child privacy policy standards. Two, 21% of the arbitrarily selected Smart Cities child privacy policies met the federal privacy policy standard. Information security policy is the first step toward developing a comprehensive data privacy strategy (Soomro, 2016) and reducing potential future child AI-generated data copyright infringement.
3. Email privacy policies also describe two tendencies. One, 95% of selected States comply with the federal email privacy policy standards. Two, 50% of selected Smart Cities' child email policies met the federal privacy policy standard. Email software and similar messaging platforms. Kids data privacy threat and a possible child AI-generated data copyright threat.
4. Persistent cookie privacy policies define another smart community gap. One, 82% of selected States conform with the federal persistent cookie privacy policy standards. Two, 50% of the arbitrarily selected Smart Cities' persistent cookies privacy policies achieved the federal persistent cookies privacy policy target. Website persistent cookies collect user data to enhance a child's online experience, yet this software is a root cause of potential AI-generated copyright infringement.
5. 3rd party consent privacy policies also disclose another smart community data privacy gap. One, 67% of selected states follow 3rd party consent privacy policies standards. Two, 55.26% of selected smart cities reached the federal 3rd party consent privacy policy benchmark. This gap is significant to AI-generated copyright infringement because of the volume of 3rd party institutions throughout the smart community.

Child Privacy Policies	**N**	**Federal Compliance**
State	38	56.00%
City	38	21.05%
N	76	
Email Privacy Policies	**N**	**Federal Compliance**
State	38	95.00%
City	38	50.00%
N	76	
Persistent Privacy Cookies Policies	**N**	**Federal Compliance**
State	38	82.00%
City	38	50.00%
N	76	
3rd Party Privacy Consent Policies	**N**	**Federal Compliance**
State	38	67.00%
City	38	55.26%
N	76	

Table 2. Smart Community Child Privacy Policy Summary

DISCUSSION

This research answers the question: What are potential gaps in child online data privacy protection during an unsettled AI-generated data copyright governance era? This paper suggested four significant privacy gaps, when coupled with AI's learning potential, could create an unsettled data governance future. First, this paper explored the smart community children's data privacy legal framework. This study argues that 1st and 4th Amendment precedents could have a profound impact on today's child data privacy and copyright enforcement. Second, this research explores three concepts to help expand child and parent behavior: Theory of Information Flow, Theory of Being Left Alone, and Activity Theory. This paper proposes that mobile phones/tablets, social media, Smart TVs, and other software platforms are designed with inadequate child consent in mind. Third, the study argues that parents must overcome the technology instrument product design gap. Parents may develop strategies to address persistent cookies, email/messaging physical location disclosure, and other data privacy PII leaks. Lastly, this study identified children's online data privacy protection gaps across 76 randomly selected smart communities. The data points out that child online data privacy protection may be a low priority for numerous state and smart city communities. This study contributes to the InfoSec body of knowledge by introducing a COPPA activity model and identifying child data privacy gaps that could impact today's kids and tomorrow's adults for numerous decades. Future studies may include a for-profit child data privacy analysis.

REFERENCES

1. Agranoff, M. (1991). Controlling the Threat to Personal Privacy, Corporate Policies Must Be Created. *Information System Management*, 8(3), 18-52.
2. Allen, D., Brown, A., Karanasios, S., & Norman, A. (2013). How Should Technology-Mediated. Organizational Change be Explained? A Comparison of The Contributions of Critical Realism and Activity Theory. *MIS Quarterly*, 37 (3).
3. Balaban, T. (2009). Comprehensive Data Privacy Legislation: Why Now Is the Time. *Case Western Reserve Journal of Law. 1*, (1).
4. Barki, H., Titah, R., & Boffo, C. (2007). Information system use-related activity: An expanded behavioral conceptualization of individual-level information system use. *Information Systems Research*, 18(2), 173-192.
5. Brown, S. & Venkatesh, V. (2005). Model of Adoption Of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle. *MIS Quarterly*, 29(3).
6. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 523-548.

7. Cockcroft, S. (2003). Gaps Between Policy and Practice in the Protection of Data Privacy. JITTA, 4, 1-III .
8. Mulligan, D. & King, J. (2012) Bridging the Gap Between Privacy and Design, 14 *University of Pennsylvania Law*. 989.
9. Engestrom, Y. (2000). Activity Theory as a Framework for Analyzing and Redesigning Work. Ergonomics, 43(7), 960-976.
10. Henning, K. (2017). The Reasonable Black Child: Race, Adolescence, and the Fourth Amendment. *American Law Review.*, 67, 1513.
11. Macioce Jr, D. L. (2018). PII in Context: Video Privacy and A Factor-Based Test for Assessing Personal Information. *Pepperdine Law Review. 45*, 331.
12. McCallister, E., Grance, T., & Scarfone, K. A. (2010). Sp 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).
13. Mehta, K., Phillips, C., Ward, P., Coveney, J., Handsley, E., & Carter, P. (2012). Marketing Foods to Children Through Product Packaging: Prolific, Unhealthy, and Misleading. *Public Health Nutrition*, 15(9), 1763-1770.
14. Minick, N. (1989). Mind and Activity in Vygotsky's Work: An Expanded Frame of Reference. *Cultural Dynamics*., 2(2), 162-187.
15. Mousavi Baygi, R. Introna, L. and Hultin, L. (2021). "Everything Flows: Studying Continuous Socio-Technological Transformation in a Fluid and Dynamic Digital World," *MIS Quarterly*, (45: 1) pp.423-452.
16. Post, R. & Rothman, J. (2020). The First Amendment and the Right (s) of Publicity. *Yale Law Review, 130*, 86.
17. Radesky, J., Weeks, H., Ball, R., Schaller, A., Yeo, S., Durnez, J., & Barr, R. (2020). Young Children's Use of Smartphones and Tablets. *Pediatrics*, 146(1).
18. Reyes, I., Wijesekera, P., Reardon, J., Elazari Bar On, A., Razaghpanah, A., Vallina-Rodriguez, N., and Egelman, S. (2018). "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. In The 18th Privacy Enhancing Technologies Symposium.
19. Soomro, Z., Shah, M., & Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2), 215-225.
20. Wang, T. and Vella-Brodrick, D. (2018) Examining Screen Time, Screen Use Experiences, and Well-Being in Adults. *Social Networking*, **7**, 32-44.
21. Wilkerson, J., Daley, M., and Brown, P. (2023) "Investigating Protected Health Information Privacy: Smart City Policymaker Challenges" *MWAIS 2023 Proceedings*. 10. https://aisel.aisnet.org/mwais2023/10.