

<https://doi.org/10.5281/zenodo.18368343>

Children's Digital Privacy in Pakistan: Legal Gaps and Policy Recommendations



Mehran Khan	LLM Research Scholar Department of Law, Abdul Wali Khan University Mardan. Mehran.global2016@gmail.com
Dr Syed Raza shah Gillani	Associate Professor at Department of Law Abdul Wali Khan University Mardan. sgilani@awkum.edu.pk

Abstract: *The rapid development of digital technologies has significantly transformed how children engage with the world, offering them opportunities for learning, socialization, and entertainment. However, this digital revolution has also exposed children to substantial privacy risks, including data exploitation, cyberbullying, identity theft, and surveillance. Despite the growing recognition of the right to privacy in international human rights law, a notable gap exists in the legal protection of children's digital privacy, particularly in developing countries like Pakistan. While international frameworks such as the Children's Online Privacy Protection Act (COPPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union offer some degree of protection, they remain insufficient in addressing emerging threats associated with new technologies, such as artificial intelligence and data tracking. This article critically examines the legal frameworks governing children's digital privacy, focusing on Pakistan's Prevention of Electronic Crimes Act (PECA) and comparing it with international standards. It highlights the gaps in Pakistan's legal system, proposes targeted reforms, and provides policy recommendations aimed at enhancing the protection of children's privacy in the digital world. The study advocates for a more robust legal framework that ensures children's digital privacy is safeguarded, aligning Pakistan's laws with international best practices and promoting greater public awareness and education.*

Keywords: Cyberbullying, Identity theft, Surveillance, Right to privacy, International human rights law, Children's digital privacy, Legal protection

1. Introduction

Context of the Issue:

Digital technology has fundamentally altered the way children interact with the world, creating opportunities for learning, communication, and entertainment. Today, children are engaged with digital platforms such as social media, online games, and educational apps (Livingstone et al., 2018). While these platforms offer numerous benefits, they also expose children to significant privacy risks. For instance, personal data

collected by these platforms can be exploited for commercial purposes, and children may become targets for cyberbullying, identity theft, and online surveillance (Kieron et al., 2020). These privacy concerns are compounded by the rapid pace of technological advancement, which outstrips the development of legal protections for children's digital rights.

Legal Protection Gap:

Despite growing awareness of the importance of children's privacy in the digital world, there

remains a significant legal protection gap, particularly in developing countries such as Pakistan. While international frameworks such as the Children's Online Privacy Protection Act (COPPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union provide some level of protection, many national legal systems, including Pakistan's, fail to address the unique challenges posed by the digital era (Zeng, 2021). Pakistan's current legal framework, including the Prevention of Electronic Crimes Act (PECA) of 2016, has made strides in regulating cybercrimes but falls short in offering comprehensive protection for children's digital privacy (Mohan, 2020).

Purpose of the Study:

This study aims to explore the gaps in legal frameworks protecting children's digital privacy, focusing specifically on Pakistan. By identifying the inadequacies in the existing legal system and comparing it to international standards, the study seeks to propose practical solutions and policy recommendations to enhance legal protections for children in the digital world. The study also aims to contribute to the ongoing global conversation about the need for stronger laws and policies to safeguard children's privacy in the digital age.

Research Questions and Objectives:

The primary research questions that guide this study are:

1. What are the key privacy risks children face in the digital world?
2. How do current legal frameworks, both in Pakistan and internationally, address these risks?
3. What gaps exist in Pakistan's legal system regarding children's digital privacy, and how can they be addressed?

The objectives of this study are:

- To analyze the legal protections available to children in Pakistan in terms of their digital privacy.
- To compare Pakistan's legal framework with international laws such as COPPA and

GDPR.

- To propose policy recommendations for improving the protection of children's digital privacy in Pakistan.

Significance:

Protecting children's privacy in the digital world is crucial for their safety, mental health, and overall well-being. As children increasingly engage with digital platforms, their personal information becomes vulnerable to exploitation and misuse (Parker et al., 2019). By strengthening legal protections for children's digital privacy, this study aims to contribute to creating a safer online environment for children in Pakistan and other developing countries. Moreover, the findings of this study can serve as a valuable resource for policymakers, legal experts, and educators striving to enhance the digital privacy rights of children globally.

2. Literature Review

Children's Digital Engagement:

Children's interaction with digital platforms has increased dramatically in recent years. The digital world offers children new ways to learn, socialize, and engage with their peers through social media, educational apps, online games, and more (Livingstone & Haddon, 2009). Social media platforms such as Facebook, Instagram, and TikTok provide opportunities for creative expression, while apps like Duolingo and Khan Academy enhance learning (Boyd, 2014). Online gaming platforms such as Fortnite and Minecraft allow children to engage with friends in a virtual environment. However, the vast amount of personal data shared and collected through these platforms raises serious privacy concerns, as children often lack the maturity to understand the implications of their online behaviors and the data they share (Avery & Ruggiero, 2020).

Children's growing digital engagement has led to the creation of a "digital footprint" that includes sensitive personal information, such as location data, preferences, online behavior, and even images and videos. Many children are unaware of the long-term implications of this digital presence, which can have both positive

and negative effects on their safety and privacy (Livingstone et al., 2018).

Privacy Risks and Legal Shortcomings:

The increasing use of digital platforms exposes children to several privacy risks. One of the most prominent concerns is the exploitation of children's personal data. Companies often collect extensive data for advertising and marketing purposes without adequate transparency or consent from the children or their guardians (Cohen, 2017). Furthermore, children are vulnerable to **cyberbullying**, where malicious behavior, harassment, or threats are carried out online. This has detrimental effects on children's mental health and well-being (Kowalski et al., 2014).

Another significant risk is **identity theft**, where children's personal information is stolen and used fraudulently for financial gain (Jones & Glover, 2015). In addition, surveillance practices are becoming increasingly common, where children's online activities are monitored and tracked by both private corporations and governments (Solove, 2011). These practices are often implemented without clear consent, leaving children vulnerable to privacy breaches.

Despite these risks, there are notable shortcomings in the legal frameworks that are supposed to protect children's online privacy. Many countries have outdated or ineffective laws that fail to address the rapid evolution of digital technology and the complex privacy concerns it raises (Lievens, 2020). This gap in legal protections has prompted calls for stronger, more comprehensive laws that ensure children's digital privacy is adequately safeguarded.

Comparative Legal Analysis:

In response to the growing concern over children's privacy, several countries have enacted laws aimed at protecting children's digital rights. One of the most notable examples is the **Children's Online Privacy Protection Act (COPPA)** in the United States, which was enacted to restrict the collection of personal data from children under the age of 13 (Lambrecht, 2020). COPPA mandates that websites and

online services directed at children must obtain parental consent before collecting personal information. While COPPA has made significant strides in safeguarding children's online privacy, it has been criticized for being too narrowly focused on website operators and not addressing emerging technologies such as mobile apps and social media platforms (Hernández, 2021).

Similarly, the **General Data Protection Regulation (GDPR)** in the European Union introduced stronger protections for children's data by requiring parental consent for children under the age of 16 to access online services (EU GDPR, 2018). It also mandates that data controllers ensure that children are informed in an age-appropriate manner about the collection and use of their personal data. Although GDPR represents a significant advancement in data protection law, its implementation has been inconsistent across member states, and it has been difficult to enforce in cases involving cross-border data flows (Zeng, 2021).

While COPPA and GDPR have been positive steps in protecting children's privacy, both frameworks face challenges in keeping up with rapid technological changes and ensuring effective enforcement, particularly when it comes to platforms that operate across borders.

Pakistan's Current Legal Framework:

In Pakistan, the **Prevention of Electronic Crimes Act (PECA)**, enacted in 2016, serves as the primary law addressing cybercrimes, including offenses related to children's privacy. While PECA includes provisions for data protection and privacy in the digital environment, it primarily focuses on combating cybercrimes such as hacking, online fraud, and the sharing of offensive content (Mohan, 2020). However, the Act lacks comprehensive provisions specifically targeting the protection of children's digital privacy, leaving gaps in safeguarding children from online risks such as data exploitation and cyberbullying.

Furthermore, the **National Commission of Child Rights Act (2022)** aims to protect the rights of children in Pakistan, but it does not explicitly address the unique challenges posed

by the digital environment (Bano, 2022). This Act lacks a clear focus on digital privacy and fails to provide a robust legal framework for regulating online platforms that collect and exploit children's data. There is also a lack of public awareness regarding digital privacy rights, which further weakens the enforcement of existing laws (Qureshi, 2021).

Thus, Pakistan's legal framework is still in its infancy when it comes to safeguarding children's digital privacy. While the government has made some efforts to address the issue through PECA and the Child Rights Commission, the existing laws are insufficient to address the complex and evolving nature of digital privacy threats faced by children.

3. Theoretical and Conceptual Framework

Digital Privacy Rights of Children:

The concept of digital privacy for children can be understood through both ethical and legal lenses. Ethically, children are considered to be particularly vulnerable in the digital realm due to their developmental stage. Children may not fully comprehend the risks involved in sharing personal data or participating in online activities, which makes them susceptible to exploitation and harm (Cohen, 2017). From a legal perspective, digital privacy rights are rooted in the broader concept of the right to privacy, which is recognized as a fundamental human right in international law (Article 12 of the Universal Declaration of Human Rights, 1948). However, children's right to privacy requires specific attention due to their unique vulnerabilities, such as limited capacity to provide informed consent and increased exposure to risks like cyberbullying, data exploitation, and surveillance.

The ethical dimensions of children's digital privacy emphasize that children should be treated as autonomous beings with rights to protect their personal information online (Binns, 2020). Digital platforms often exploit children's personal data for targeted advertising, making it crucial to ensure that privacy protections are in place to safeguard their interests. Ethical theories such as **utilitarianism** and **deontological**

ethics advocate for the protection of children from harm while respecting their autonomy. **Utilitarianism** emphasizes the greatest good for the greatest number, urging legal reforms that prioritize children's welfare in the digital space (Beauchamp & Childress, 2019). On the other hand, **deontological ethics** stresses the importance of respecting children's rights to privacy as a duty, irrespective of the potential benefits for others, such as companies profiting from children's data (Kant, 1785).

Moreover, the **vulnerability theory** suggests that because children are not yet fully capable of understanding the long-term consequences of their online actions, they require special protection under both ethical and legal standards (Archard, 2010). This theory argues that children's interests should take precedence over the interests of businesses or governments in cases where privacy is at stake. Thus, ensuring that children's digital privacy is protected is not only a legal obligation but also an ethical imperative to avoid harm and exploitation.

International Standards:

The global community has recognized children's digital privacy as an urgent issue, and various international frameworks have emerged to protect children's rights in the digital space. The **United Nations Convention on the Rights of the Child (UNCRC)**, adopted in 1989, serves as the cornerstone of children's rights internationally. Article 16 of the UNCRC protects children from arbitrary interference with their privacy, family, home, or correspondence, and it asserts that children should be protected from information and materials that may harm their well-being (UNCRC, 1989). The UNCRC recognizes the vulnerability of children in the digital space and calls for the protection of their privacy in the context of new technologies (UN, 2013).

Furthermore, the **General Comment No. 25 on Children's Rights in the Digital Environment**, issued by the UN Committee on the Rights of the Child in 2021, outlines the specific obligations of states to ensure that children's rights are protected online. It

emphasizes that children have the right to privacy, including protection of their personal data, and calls on governments to establish legal frameworks that address online risks such as cyberbullying, online grooming, and data exploitation (UNCRC, 2021). The Comment stresses the need for governments to ensure that children are informed about their rights and have access to avenues for redress in cases of privacy violations.

In addition to the UNCRC, the **Children's Online Privacy Protection Act (COPPA)** in the United States and the **General Data Protection Regulation (GDPR)** in the European Union also set important international precedents. COPPA specifically addresses the collection of personal information from children under the age of 13 and mandates that companies obtain verifiable parental consent before collecting data (FTC, 1998). Similarly, GDPR has strengthened children's privacy protections by requiring parental consent for children under 16 to use online services and by enhancing transparency around the processing of children's data (EU GDPR, 2018). These legal frameworks reflect a growing recognition of the need for comprehensive protections against the misuse of children's personal information online.

Despite these efforts, challenges remain in ensuring the uniform implementation of these standards across different jurisdictions, especially in developing countries like Pakistan, where legal frameworks may not be fully aligned with international norms. There is a pressing need for countries to integrate these global frameworks into their national laws to provide children with the digital privacy protections they deserve.

In conclusion, the theoretical and conceptual framework surrounding children's digital privacy emphasizes the ethical obligation to protect children's data while balancing it with legal measures such as the UNCRC and the GDPR, which aim to provide comprehensive safeguards for children's privacy in the digital era.

4. Discussion

Legal Gaps in Pakistan:

Pakistan's legal framework addressing children's digital privacy is still in the early stages, and significant gaps exist in providing comprehensive protections for children in the digital space. The **Prevention of Electronic Crimes Act (PECA) 2016**, while a step forward in regulating cybercrimes, does not sufficiently address the specific privacy needs of children (Mohan, 2020). PECA primarily focuses on issues such as cybercrimes, hacking, and online defamation but lacks clear provisions on the collection, use, and protection of children's personal data. This legal gap has left children particularly vulnerable to data exploitation, online bullying, and other privacy violations. Additionally, the enforcement of PECA has been inconsistent, with limited mechanisms for holding offenders accountable for breaches of children's privacy, especially in the context of online platforms that collect data from children (Qureshi, 2021).

One of the most significant issues with Pakistan's legal approach to children's privacy is the lack of a **dedicated children's privacy law**. While there are laws aimed at protecting children's rights in general, such as the **National Commission of Child Rights Act 2022**, they do not specifically address the nuances of digital privacy. This lack of specificity and a dedicated legal framework leaves children exposed to risks like cyberbullying, identity theft, and the misuse of their data on digital platforms (Bano, 2022). The absence of a robust legal structure to govern children's digital rights means that children's privacy is often overlooked in favor of broader cybercrime legislation.

Moreover, Pakistan's **enforcement mechanisms** are underdeveloped. While laws like PECA exist, they lack a clear and efficient framework for enforcement, and there is limited public awareness regarding children's rights to digital privacy. This creates an environment in which violations go unnoticed, unreported, or unresolved. For instance, online platforms based in Pakistan are not required to adhere to any privacy standards specific to children's data, and there is little government intervention to monitor or regulate these platforms.

International Comparisons:

In comparison to Pakistan's legal framework, international laws such as **COPPA** (Children's Online Privacy Protection Act) in the United States and **GDPR** (General Data Protection Regulation) in the European Union offer more comprehensive and enforceable protections for children's digital privacy.

COPPA, enacted in 1998, was one of the first laws to specifically address the issue of children's online privacy. It imposes stringent requirements on online services directed at children under the age of 13, including obtaining verifiable parental consent before collecting personal data from children. This law also mandates that websites provide clear privacy policies, restrict the use of children's data for marketing purposes, and give parents the right to access and delete their children's information. However, COPPA has faced criticism for its limited scope, especially in the context of mobile apps and evolving technologies, yet it remains one of the few laws in the world offering dedicated child privacy protections (Lambrecht, 2020).

GDPR, introduced in 2018, provides broader protections for children in the digital space, particularly for those under the age of 16. It requires parental consent before children can access most online services and places additional transparency requirements on data controllers, ensuring that children are informed about how their data will be used in an age-appropriate manner. GDPR's provisions for children's privacy are more stringent than those found in COPPA, as it also requires businesses to implement mechanisms to protect children's data and to respond to violations in a timely manner. Despite its strength, the enforcement of GDPR has been uneven, with concerns about its application in cross-border contexts and its ability to hold tech companies accountable across jurisdictions (Zeng, 2021).

In contrast, Pakistan's legal framework lacks these detailed, child-specific provisions, leaving children more vulnerable to privacy breaches. While PECA addresses some aspects of cybercrime, it does not have clear regulations for protecting children's data. The absence of a dedicated child privacy law or a regulatory body

focused on children's online rights means that Pakistan's legal system is far behind countries like the United States and members of the European Union when it comes to protecting children's privacy.

Policy Recommendations:

To improve children's digital privacy protections in Pakistan, the following policy recommendations are proposed:

1. Enactment of a Dedicated Children's Privacy Law:

Pakistan should enact a comprehensive law specifically designed to protect children's digital privacy, similar to COPPA and GDPR. This law should require parental consent for data collection, set clear guidelines for the types of data that can be collected from children, and mandate that digital platforms provide transparency about how children's data will be used. Such a law should also include provisions for safeguarding children from risks such as cyberbullying and online harassment.

2. Parental Consent and Digital Literacy Programs:

Along with legal reforms, it is crucial to implement **digital literacy programs** aimed at both children and parents. These programs would educate children about the risks they face online and empower parents to understand the implications of their children's digital engagement. Parental consent should be reinforced through programs that educate parents about their rights to control their children's data and monitor their digital activities.

3. Strengthening Enforcement and Accountability Mechanisms:

To ensure the effectiveness of children's privacy laws, Pakistan must strengthen its **enforcement mechanisms**. This includes the establishment of a dedicated body to oversee and enforce children's privacy laws and monitor the compliance of online platforms. Penalties for non-compliance should be increased, and platforms that violate children's privacy

should be held accountable. Public awareness campaigns can help raise awareness about children's digital rights and encourage reporting of violations.

4. **Collaboration with International Bodies to Adhere to Global Privacy Standards:**

Pakistan should collaborate with international organizations such as the **UNICEF** and the **International Telecommunication Union (ITU)** to align its legal frameworks with global standards on children's privacy. By working with international bodies, Pakistan can ensure that its laws are consistent with global best practices, which will help improve cross-border enforcement and cooperation. Additionally, this collaboration can foster a more robust regulatory environment and help Pakistan stay updated with emerging technological trends that may impact children's privacy.

In conclusion, by enacting a dedicated children's privacy law, improving digital literacy, strengthening enforcement mechanisms, and collaborating with international organizations, Pakistan can significantly enhance the protection of children's privacy in the digital age.

5. **Conclusion**

This study has analyzed the current state of children's digital privacy rights in Pakistan, identifying significant gaps in the existing legal framework. Pakistan's **Prevention of Electronic Crimes Act (PECA) 2016**, while addressing general cybercrimes, lacks comprehensive provisions specifically protecting children's personal data in the digital space. Furthermore, **Pakistan's National Commission of Child Rights Act 2022** does not explicitly address the nuances of digital privacy, leaving children vulnerable to risks such as data exploitation, cyberbullying, and online surveillance.

The analysis also revealed that while international frameworks such as **COPPA** in the United States and **GDPR** in the European Union offer more robust protections, Pakistan's legal structure lags behind. The country does not have

a dedicated **children's privacy law** and lacks effective enforcement mechanisms to ensure that children's privacy rights are upheld. The absence of clear guidelines and regulatory oversight exacerbates the situation, making children's data especially vulnerable to misuse in the digital environment.

In summary, Pakistan's current legal framework falls short of providing adequate protection for children's digital privacy, and substantial reforms are urgently needed to bridge this gap.

Final Recommendations:

Based on the findings, the following specific actions are recommended for Pakistan to better protect children's privacy in the digital realm:

1. **Enact a Dedicated Children's Privacy Law:** Pakistan should establish a law specifically aimed at protecting children's digital privacy. This law should include provisions for parental consent, data protection, and transparency for digital platforms collecting children's data. It should also address risks such as cyberbullying, identity theft, and online harassment.
2. **Implement Digital Literacy Programs:** To empower both children and parents, Pakistan should launch digital literacy programs. These programs should educate children about the risks of sharing personal information online and teach parents how to safeguard their children's digital presence. Parental consent should be emphasized, ensuring that parents are well-informed about their children's online activities and data protection rights.
3. **Strengthen Enforcement and Accountability:** The government must establish stronger enforcement mechanisms to ensure compliance with children's privacy laws. A dedicated regulatory body should be created to oversee the implementation of privacy protections for children and ensure that violators are held accountable. This body should be empowered to take action against non-compliant platforms and impose penalties

for violations.

4. **Collaborate with International Bodies:** Pakistan should align its legal framework with international best practices by collaborating with organizations such as UNICEF and the International Telecommunication Union (ITU). By working with these bodies, Pakistan can ensure that its laws are compatible with global standards, facilitating cross-border cooperation and enhancing the protection of children's privacy worldwide.

Future Directions:

There are several avenues for future research that can further the understanding and protection of children's digital privacy:

1. **Impact of Emerging Technologies on Children's Privacy:** Future research could explore how emerging technologies like artificial intelligence, blockchain, and virtual reality impact children's digital privacy. Understanding how these technologies collect, process, and store children's data will help shape future regulatory frameworks.
2. **Cross-Cultural and Comparative Studies:** It would be beneficial to conduct cross-cultural studies comparing how different countries protect children's digital privacy. This research could identify best practices and lessons that can be applied in Pakistan and other developing countries.
3. **The Role of Technology Companies in Protecting Children's Privacy:** Further research could also explore the role of technology companies in safeguarding children's privacy. This includes examining the effectiveness of self-regulation by these companies and their responsibility in ensuring compliance with privacy laws.
4. **Public Awareness and Advocacy:** Future studies should investigate the effectiveness of public awareness campaigns regarding children's digital rights. This research could help design more effective campaigns that educate both parents and children about the risks and responsibilities associated with

digital engagement.

In conclusion, while this study has highlighted critical gaps in Pakistan's legal framework regarding children's digital privacy, it also underscores the need for comprehensive legal reforms and a concerted effort from the government, technology companies, and international bodies to create a safer online environment for children. Through the recommended reforms, Pakistan can significantly enhance the protection of children's privacy in the digital realm, ensuring that their rights are respected in an increasingly connected world.

References:

- Archard, D. (2010). *Children, autonomy, and the vulnerability principle*. Routledge.
- Avery, M., & Ruggiero, L. (2020). The evolution of children's digital footprints: Data, privacy, and protection. *Children's Digital Safety Journal*, 7(2), 125-140.
- Beauchamp, T. L., & Childress, J. F. (2019). *Principles of biomedical ethics* (8th ed.). Oxford University Press.
- Bano, S. (2022). Protecting children's rights in the digital age: A critical analysis of Pakistan's National Commission of Child Rights Act. *Asian Journal of Law and Policy*, 14(3), 205-220.
- Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
- Cohen, J. (2017). Privacy in the digital age: Challenges in protecting children's data. *Journal of Digital Privacy Law*, 11(1), 33-47.
- EU GDPR. (2018). General Data Protection Regulation. *European Union Official Journal*, 61(9), 48-74.
- Hernández, R. (2021). COPPA at 25: Evolution, challenges, and opportunities. *International Journal of Internet Law*, 28(3), 101-118.
- Jones, M., & Glover, J. (2015). Identity theft and

- children: The unseen risk. *Journal of Digital Security*, 5(2), 75-89.
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Cyberbullying among college students: Evidence from multiple domains. *Computers in Human Behavior*, 36(3), 317-323.
- Lambrecht, L. (2020). COPPA and its limitations: Protecting children in an age of mobile apps and social media. *Children's Privacy Journal*, 5(1), 1-14.
- Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final Report*. EU Kids Online.
- Livingstone, S., et al. (2018). Risks and safety for children online: The UK report. *EU Kids Online*.
- Lievens, E. (2020). The legal protection of children's digital privacy: A global perspective. *International Journal of Child Protection*, 18(2), 89-104.
- Mohan, S. (2020). Pakistan's Prevention of Electronic Crimes Act and children's online privacy: An evaluation. *International Journal of Cyber Law*, 4(2), 45-60.
- Parker, D., Lee, R., & Brown, C. (2019). Protecting children's digital rights: Lessons from the GDPR and COPPA. *Cybersecurity Law Review*, 15(1), 32-48.
- Qureshi, Z. (2021). Legal framework for children's online privacy: Gaps and challenges in Pakistan. *Journal of Cyber Policy*, 22(3), 30-41.