Journal of Studies in Social Sciences and Humanities
http://www.jssshonline.com/
Volume 9, No. 4, 2023, 351-361
ISSN: 2413-9270

On the Protection of Children's Online Privacy from the Phenomenon of Sharenting

Rongrong Guo*
China University of Political Science and Law, China
Email: 2302030186@cupl.edu.cn

Corresponding author

Abstract
With the rise of social networks, parents are increasingly showing off their children, which is called Sharenting. On the one hand, parents lack awareness of prevention; on the other hand, Sharenting has become the currency of interpersonal transactions, and parents have a serious mentality of following the herd. In this context, children's rights are ignored and their voices are not listened to. This study takes the phenomenon of Sharenting as an entry point to discover the current difficulties in technical, social self-awareness, and legal to protect in children's right to online privacy. This paper combines the United Nations' protective measure of children's rights with national practices to explore multiple paths to improving the protection of children's online privacy. In this way, the legitimate rights of children can be safeguarded form families and schools, internet industry self-regulation, legal policy, and government propaganda, and it can also prevent illegal infringement caused by privacy leak.

Key words: Social media, Sharenting, Protection of children's rights and interests, Online Privacy, Children's right to online privacy

Introduction

If the 80s and 90s have just stepped into the new era of social networking, children have long been forced to be surrounded by big data and digital due to behaviors such as Sharenting. The term sharenting was first coined by Wall Street Journal writer Steven Leckart, and has been given a more academic definition by Marasli et al. Sharenting is a combination of the concepts of "parental sharing on social media" and "parenting", that is, parents post photos and videos of different ages of children on social media to express their feeling about their children (Marasli et al., 2016). The special feature of Sharenting is over - sharing.

Parents have never asked their children whether they agree to be judged on social networks, in other words, children do not know which photos they take or in which form they send. When Sharenting on social networks, there are hundreds eyes behind the screen looking at and evaluating the content posted by parents. Although most parents post children's photos for entertainment or to make people laugh, it is undeniable that some parents post interesting stories or information about children to gain people's attention, such as Like and comments. In fact, preliminary analysis indicated that adolescents generally disapprove of Sharenting, and they mostly think it is embarrassing and useless (Verswijvel et al., 2019). Blum-Ross and Livingstone (2017) found that bloggers face a profound moral dilemma because representing their status as parents inevitably publicizes their children's lives and, paradoxically, introduces risks that they have a responsibility to guard against. Some parents think that their children naturally have the right to possess them, and there is nothing wrong with showing off. Others believe that children are independent individuals and they have inherent rights to privacy. If parents show off their children (Sharenting) on social networks without restraint, they will not only shows off excessively and is offensive, but also violate the online privacy rights of children. Although some behaviors are not inappropriate in the eyes of information sharers, they implicitly violate the online privacy rights of children, and may give criminals the opportunity to obtain private information and commit crimes.

In conclusion, social media is the hardest hit area for leaks of sensitive information, but parents have vague concepts of online security and online privacy. Young children have no right to make independent choices about their environment and the things they face. However, parents who are supposed to be guardians have unconsciously turned into disseminators of information, infringing on children's online privacy, even if they are not aware of the seriousness of the problem.When parents press the button of send, they hardly consider that children also have basic human rights. Children are the future of a country, but they are a relatively weak group within the scope of human rights. Because of this, their own rights and interests are often ignored.

Starting from the phenomenon of Sharenting, this article focuses on the protection of children's online privacy rights, analyzes the attributes of children's online privacy rights, discovers the existing legal protection problems, and looks for solutions. The purpose of this paper is to safeguard the legitimate rights of children, and to speak for children while also preventing illegal infringement due to privacy leaks.

What is Online Privacy Protection for Children ?

Definition of Children's Online Privacy

When talking about children's online privacy rights, the three concepts of privacy, online privacy and children need to be involved.

Privacy The right to privacy comes from human dignity and freedom. Based on Westin's thinking, Steeves (2007) thought that privacy is no longer a characteristic of social isolation, but rather constructed by real social actors through inter subject communication. Due to the fact that communication is a process of self emergence and establishing relationships with others, privacy is placed at the center of human identity and social interaction. As a passive personality right, the object of privacy is mainly the private information of an individual, which covers a wide range, including personal physical condition, family income, interpersonal relationships, and other parts that individuals are unwilling to disclose and do not involve public interests.

Online Privacy With the advent of the big data era, more and more people are gradually exposing their privacy on social networks voluntarily or involuntarily. Some of them come from personal sharing, and they appropriately expose certain parts of their lives; Some are being monitored or even violated by illegal means and forced to be exposed to the public. Thus, the concept of online privacy emerged. The formation of online privacy rights is closely related to the highly developed new media and the rise of social networks. Chinese scholar Zhao (2002) pointed out that online privacy is mainly the right of natural persons to enjoy the peace of private life and private information on the Internet. Similar to traditional privacy rights, in the field of cyberspace, it is also prohibited to disclose personal-related photos, information that others are unwilling to publish, sensitive events, etc. In this environment, the privacy of rights holders is naturally protected in accordance with the law and will not be infringed upon by others through illegal methods such as knowing, collecting, copying, and disclosing. In essence, compared with the concepts of traditional privacy and online privacy, due to the flow and dissemination of personal information in the networks has become easier, so online privacy only has a limited space scope, which further emphasizes the importance of this right.

Children First of all, a child is the legal definition of age, usually a minor. In China, children generally refer to people under the age of 18. And this is also recognized in *the United Nations Convention on the Rights of the Child* (UNCRC). Secondly, children are intellectually underdeveloped, have not yet established correct cognition, and their self-prevention and risk-resisting abilities are still very weak. So they should be a key target of protection for all sectors of society. However, children, as a vulnerable group, their right to online privacy is often ignored by adults such as guardians.

To summarize, the concept of children's right to online privacy is understood from all above aspects, that is, children's right to privacy on the Internet, which not only refers to children's right to privacy in the Internet environment, but also includes the part of children's right to privacy in the dissemination of information on the Internet in the real society. Children, like adults, enjoy the right not to be disturbed in their private lives and not to have their private information disclosed on the Internet. But children are special because of the relatively weak position of the subject of their rights in society.

Special Features of children's Online Privacy

They often find it difficult to speak for themselves in society, and their online privacy have special manifestations in four aspects:

Firstly, the subject of children's online privacy is inherently vulnerable. Compared with adults, young people do not have the right to make independent choices about their environment and the things they face. There are emerging concerns as children are also at risk of emotional and behavioral harm, cyber bullying, identity theft, manipulation, labeling, and restriction, which may affect their current and future opportunities (Johnson,2020). Children are more susceptible to influence from the outside world and may disclose their privacy without knowing it, causing indelible security risks to individuals and even their families, while they themselves cannot take responsibility for this.

Secondly, there are various ways in which children's online privacy are violated. According to Minkus, Liu and Ross (2015), they described four threats to a child whose information is posted on Facebook: stranger danger, overexposure to acquaintances, data brokers, and surveillance. In the digital information age, with just a click of a mouse button, a minor's image, age, name, school and other information will be shared around the world through the Internet and will exist forever. Generally speaking, there are two main ways in which children's online privacy are infringed: first, children's own poor self-prevention ability leads to the leakage of information during the process of surfing the Internet; second, adults, including guardians, expose children's information on the Internet, such as Sharenting.

Thirdly, the protection of children's right to online privacy has multi-layered. The vulnerable status of this group determines that the protection and relief of their online privacy rights cannot be accomplished by themselves. In addition, from the perspective of civil law, most children are still under the protection of their guardians and do not have full capacity for civil conduct. When their online privacy is violated, guardians are naturally duty-bound, and school teachers, network operators, the government even community of nations also play an important roles.

Finally, the path to protecting children's online privacy rights is challenging. As mentioned above, with the continuous development of digital technology, the flow and dissemination of personal information on the Internet has become easier, and the discussion on the topic of online privacy has become particularly heated. In addition to parents unconsciously revealing too much information about their children through Sharenting, children themselves share their privacy with others without parental supervision in the Internet, and these behaviors increase the risk that they will be violated in cyberspace. Moreover, the law cannot restrict technical problems, and technical problems cannot be solved if they exist objectively. Furthermore, parents have a low level of importance and respect for children's online privacy rights, which adds an invisible threshold to the protection of this right.

To sum up, the online privacy of children is included in the personal information of children, and the application is stricter than the general protection of personal information.

Methods

This study is dedicated to analyzing the challenges faced by the protection of children's online privacy and seeking effective strategies to improve the relevant protection measures. In order to achieve this goal, the study adopts a qualitative analysis method to identify the problems and deficiencies in the current situation of children's online privacy protection in practice, and then proposes targeted optimization strategies.

In addition, this study investigates and analyzes the protection of children's online privacy in practice. Various types of data are collected and organized through the 'Library Research Method', including research reports, typical cases, court decisions and research papers about Sharenting. At the same time, the 'Content Analysis Method' is used to obtain a wealth of secondary data, such as books, articles, journals, and newspapers. These data come from different countries and regions, and cover different age groups and backgrounds of children with online privacy protection related situations arising from Sharenting.

The study also compares and analyzes the experience and inspiration of the United Nations in the protection of children's right to online privacy from an international comparative perspective, and interprets them in depth in the light of legal theories.

Findings: The Dilemma of Protecting Children's Online Privacy

In today's world, data abuse has become the potential risks for children. In the online privacy of children, they are mainly infringed upon by their portrait rights and reputation rights. The reason for such a serious situation is not only the uncontrolled exposure of children's information on social platforms by parents, but also the various difficulties faced in protecting online privacy.

Difficulties in Technical

Technical difficulties are mainly reflected in the process of use or technical vulnerabilities, which are often objective and difficult to overcome.

Although some platforms provide parental monitoring functions and privacy settings, due to the openness and anonymity of the Internet, it is impossible to accurately identify who is behind the manipulation. In less than 10 years, mobile phones have become the most commonly used and most desired device among teenagers. Its physical characteristics and the psychological processes involved in its use explain both the grace it elicits and the abuse or dependence it can come to provoke or encourage in adolescents (Chóliz, 2012). In order to solve this problem, in China, youth mode is stetted in APPs of mobile phone. Youth mode means an anti-addiction system for teenagers. This system regulates the online behavior of children in terms of functions, usage time and browsing content. After entering the teenager mode, the children can not use it for more than a limited amount of time each time. If they exceed the imitation and want to continue to use it, a password is required. Through time settings, parents can effectively control when and how long their children spend online. So some people think that setting youth mode in APPs of mobile phone can isolate many hidden dangers, but the reality is not satisfactory. When we open an APP, a page pops up prompting people whether to choose "youth mode". Whether you are an adult or a minor, you can choose whether or not you are a teenager. And such pop-up warning is neither useful nor helpful. Obviously, most applications do not strictly abide by the relevant regulations of children's privacy protection, and they lack corresponding technical guarantee measures.

Moreover, with the rapid development of network technology, hackers' computer skills have also increased. It is difficult to determine the identity of keyboard operators and the network space itself has unlimited characteristics, which adds an invisible threshold to overcome the dilemma for the protection of children's online privacy. In order to protect children's online privacy, Bélanger et al. (2013) designed an automated tool called POCKET. It provides an easy-to-use interface for parents to configure their child's privacy choices and then automatically enforces those policies. But design members also pointed out that, to date, business practices and the technological approaches used have failed to effectively protect children's online privacy, and the POCKET, like other scientific studies is that continued use could not be evaluated.

Difficulties in Social self-Awareness

Self-consciousness is often closely related to social. From a general perspective, the Internet world is not only a technological leap, but also requires netizens to be cautious in terms of ethics and morality. However, in recent years, people's thinking patterns, moral concepts, and outlook on life have gradually fundamental changes. People abuse others wantonly on social platforms, cyber manhunt and publicly leak other people's personal information. The online privacy rights of children who are in a vulnerable position in social groups cannot be respected and protected. From a small perspective, most of the people who infringe on children's right to online privacy are their parents. The majority of parents of all ages report that they post/share photos, videos, or information about their children online, with nearly 90% of them sharing this information on their social media accounts. And most parents admit that online privacy doesn't exist or don't know if it ever has (Manotipya & Ghazinour, 2019). Although most parents just record their children's daily growth, there are still some parents who want to follow suit. Amon et al. (2022) suggested that not only do parents generally not worry that their children will someday be embarrassed by the photos they post online, they are even more likely to expect that friends and family will share or repost photos of their children. Sharenting is not seen as a uniquely risky behavior. When this mentality becomes common, they unknowingly infringe on the rights of others, and the infringement of children's online privacy rights is the first to bear the brunt.

Social self-awareness also includes the self-regulatory mechanism of the Internet industry. Livingstone and Nandagir (2019) distinguish between online privacy: interpersonal privacy, institutional privacy, and commercial privacy that is collected and used for business and marketing purposes. At the same time, they pointed that intrusive tactics are used by marketers to collect children's personal information and it has raised concerns about data privacy and security. While the commercial use of children's data is at the forefront of current privacy debates, empirical evidence related to children's experiences, awareness, and competence with respect to online privacy has lagged behind. So the entire Internet industry self-regulatory system needs to implement specific protection measures for online privacy rights. However, the content of the Internet industry self-discipline is not only rough, but also the penalties are not very operational, which makes it difficult to truly protect children's right to online privacy. Judging from the individual website, the main problems focus on the following two points: first, it is like a fake website privacy statement; second, the privacy statement has become a tool for the industry to protect the website itself rather than protecting netizens. The value of setting up a website's privacy statement should first be considered to protect netizens, and secondly to avoid risks on the website. However, the reality is unsatisfactory. By carefully exploring the contents of the terms and conditions, it turns out that the website is suspected of excessively illegally collecting, using and disseminating the personal information of netizens to make profits. The website uses its status as a rule maker to limit the rights and interests of website users. If you want to enter its website, you must agree to the overbearing terms inside. The scary thing called hidden rules has combined to become a tacit and open secret within the Internet industry.

Difficulties in Legal

Legal problems include three levels: the current legal, the judicial and the law enforcement.

In the field of legislation, in terms of legislative model selection, the United States adopts a hybrid legislative mode, which combines elements of both industry self-regulation and government regulation. Among them, *the appearance of the Children's Online Privacy Protection Act* (COPPA) is a milestone in the history of protecting the right to Children's Online Privacy under the age of 13 in cyberspace. But to this day, there are still some scholars who express dissatisfaction with COPPA. Hargittai et al. (2011) found that cast serious doubt on the effectiveness of COPPA. The data also point to unintended consequences of the COPPA regulatory model based on web services. For example, Haber (2020) has pointed out that even if the current regulatory framework is re-calibrated in COPPA, it is not suitable for proper protection of children's privacy. Policy makers must consider other regulatory mechanisms to better protect children's privacy in the end, and they must abandon the method of privacy of the department. However, throughout the current legislation of many countries, there are separate provisions on the "right to privacy", but there are no specialized provisions for the protection of children's online privacy. Most countries, like China, have not established complete laws regarding the online privacy rights of children. After January 1, 2024, China will implement *regulations to protect minors in cyberspace*, but the content of the regulations is mostly encouraging and guiding, which plays a minimal role in daily life. Special legal protection for online privacy of children is in a gray area. We found that there are three main existing legal problems: Firstly, the legal subject and method are unclear, and the scope of protection is too broad. Compared with traditional privacy rights, children's online privacy rights need to be more detailed and specific. Secondly, the legal concept is still vague. Each country defines "children" differently, and whether it can be equated with "children" is controversial. More specifically, the COPPA protects people who is under the age of 13, while *the United Nations Convention* refers to people up to the age of 18. Lastly, some countries have low-level legal regulations regarding children's online privacy rights, so the role it plays is extremely limited. Thus, if there are no laws and regulations, relying solely on the awareness of network operators, it is difficult to require them to correctly guide children to protect their privacy during the online process.

In the field of justice, while sympathetic to children's privacy rights, courts are more respectful of parents' rights to accompany their children and their control over their own children's privacy. Previous cases reflect a strong tradition that based on a strong tradition of parental rights, parents have exclusive control over the disclosure of their children's information, and courts have provided limited guidance on Sharenting and on the protection of children's online privacy rights. Under such a legal framework, courts have rarely held that parents have behaviors in Sharenting on social media oversharing or that parents are a potential source of harmful disclosures (Steinberg, 2017).

And cases involving Internet infringement is generally a large number of people. Most of the people registered on social platforms have anonymous identities, and their IPs are often scattered. It is difficult to determine the direct infringers or joint tort-feasors, so the prosecute and jurisdiction remain major problems. In addition, electronic evidence has complex characteristics such as being easily forged, tampered with and not easily extracted, and it involves a wide range of technical fields, including computer science, network security and data mining. Although the judicial organs of some countries and regions have begun to take measures to regulate and safeguard the acquisition and identification of electronic evidence, even some judicial organs have also strengthened cooperation with relevant technical departments to establish electronic evidence appraisal agencies to improve the probative power and credibility of electronic evidence, the professional requirements for judges and technical experts are high. These features have created difficulties for both parties in obtaining evidence and increased the difficulty for judges in hearing cases.

In the field of law enforcement, the infringement of online privacy involves both the infringer and the infringed. When an infringer violates another person's right to online privacy, the infringed person files a lawsuit in court and displays his or her scars to the public. It is a secondary injury in a certain sense, whether it is mental or material. If the infringed's lawsuit is successful, people's attention will be attracted to the incident itself during the enforcement process, and this will lead to a new round of "cyber manhunt" to the infringer. Moreover, civil law has always advocated the principle of "no trial without complaint". It is so difficult for adults to protect their own online privacy, not to mention the protection of children's online privacy. If the infringer is the minor's parents, the lawsuit is simply impossible. Parents usually believe that they have the right to manage their children's personal information, while children believe that they should have the right to their own privacy. In such cases, law enforcement agencies often choose not to intervene because they are unable to determine who is right and who is wrong, resulting in a lack of protection for children's online privacy. Finally, because of the cross-border nature of the Internet, some violations of children's right to online privacy may involve multiple countries and regions, and thus obstacles to cross-border law enforcement cooperation, including issues such as differences in judicial procedures and the collection and retrieval of evidence, pose certain difficulties for law enforcement agencies.

Ways to Protect Children's Online Privacy

The United Nations Protection of Children's Online Privacy

The protection of children's right to online privacy by the United Nations is an important and necessary endeavour. In today's digital age, children's use of the internet has become the norm, and Sharenting has made them passively involved in the social network world, facing various potential risks and threats from the cyberspace. Therefore, the protection of children's right to online privacy is not only related to personal information security, but also to their future physical and mental health, social adaptability, social skills and many other aspects.

The United Nations has played an active role in this regard and is committed to ensuring that every child enjoys equal rights and dignity. Firstly, the United Nations has adopted a series of international legal documents on the rights of the child, providing a legal framework for the protection of children's rights. The most important of these is UNCRC. UNCRC establishes the basic principles of children's rights and sets out the obligations that governments should undertake in protecting children's rights. The Convention stipulates that children are entitled to special protection, including the protection of the privacy in the field of information and communication technologies. According to this Convention, States should take the necessary legislative and administrative measures to ensure that children's privacy is adequately protected in the online environment. These legal documents not only provide action guidelines for governments, but also encourage all sectors of society to participate in the protection of children's rights. In other words, as UNCRC is relevant to the online, mobile and new media environment, it can serve as a new policy framework for the protection of the right to privacy (Brown & Pecora, 2014). Secondly, the United Nations Children's Fund (UNICEF) is committed to safeguarding children's rights worldwide, including the protection of rights in the digital field. UNICEF promotes countries to strengthen the protection of children's online privacy rights through research, advocacy, and policy development. UNICEF collaborates with governments to regularly monitor and evaluate the implementation of children's rights. By collecting and analyzing data, UNICEF is able to identify areas where children's rights are adequately safeguarded and where improvements are needed. Thirdly, the UN Sustainable Development Goals (SDGs) includes goals on digital inclusiveness and digital rights, including safeguarding children's privacy rights on the internet. This reflects the importance and commitment of the United Nations to promoting children's right to privacy on the Internet globally. Fourth, the United Nations Educational, Scientific and Cultural Organization (UNESCO) also plays an important role in promoting the protection of children's privacy online. By promoting digital literacy education, it improves children's understanding of and protection of online privacy. In addition, the United Nations recognizes the importance of education and advocacy in the protection of children's rights. It promotes children's rights through various media platforms to raise global public awareness, and it has been encouraging governments to incorporate children's rights education into school curricula and to carry out publicity campaigns to raise public awareness of children's rights.

In short, the United Nations has played a key role in the protection of children's rights. Through a variety of means, including its agencies and international conventions, the United Nations has been actively promoting and advocating the protection of children's online privacy on a global scale. These efforts have not only provided guidance and norms at the legal level, but also promoted practical actions and policy formulation in protecting children's online privacy in various countries by various projects and advocacy activities.

Therefore, in order to further optimize the relevant mechanisms, strengthen publicity, and reform legal. States can address the challenges through the development of legal frameworks, monitoring and evaluation, education and awareness-raising measures. Only in these ways can we safeguard the healthy development of every child and provide solid guarantees for the creation of a safe and trustworthy cyberspace, and every child can explore the infinite possibilities of the digital world in peace.

Suggestions for improving the protection of children's online privacy

Civic Responsibility: Strengthening Parents' and Schools' Awareness

Sorensen (2016) argued that even though parents and their children are viewed as a fiduciary legal relationship, it is difficult for the law to hold the view that parents are penalized for disclosing information about their children. Therefore, an awareness-raising resolution is more appropriate than Therefore, an awareness-raising resolution is more appropriate than a decree with coercive powers. It is not difficult to obtain information about children's names, ages, home addresses, and schools attended from parents' sharing on social media platforms, and such information is often memorized, downloaded, and even processed and misused by unscrupulous individuals. Parents' awareness of self-prevention is the first level that can protect children's online privacy, and schools are the second level. *For parents*, they must recognize that the current rules and restrictions on the amount of time and the number of times per day that they can access the Internet are not sufficient to ensure the safety of their children online. Children must be informed of the dangers of disclosing sensitive information (Lwin et al., 2008). First of all, parents should communicate with their children and tell them what is private information and how to protect their privacy. At the same time, parents should set a good example. When parents want to post photos or interesting facts about their children on social media platforms, they should ask their children for their opinions first and tell them which social media platforms to post their photos on, so that they can participate in the process and let their children supervise the content of their parents' postings as well. If parents post something that the child is uncomfortable with, the parents should patiently listen to the child's wishes and delete the content. Second, children's behaviors on the Internet should be monitored to prevent them from being exposed to undesirable information or interacting with strangers. *For schools*, they should organize relevant courses or activities, and provide some resources and guidance materials to help students understand the online privacy. Schools can also organize lectures, seminars, and other events to popularize knowledge, enhance awareness, and cultivate the correct use of internet skills for children. They can invite professionals to explain the common sense and techniques of network security and personal privacy protection to students. Children's immature mind determines that they naturally lack the ability to recognize information and protect their privacy when faced with such a huge information system on the Internet. Even with strategies in place to help children protect their personal information, children's true understanding of the risks in online interactions remains a problem (Andrews et al., 2023). So that is why parents and schools must work together to provide children with appropriate guidance and education on Internet safety.

Industry Responsibility: Standardization of the Internet Industry

The rapid development of Internet technology has led to an inevitable lag in legislation. In order to change this situation, industry self-regulation has become one of the most important means to solve the problem. While possessing a large amount of information about children on the Internet, Internet service providers in the Internet industry should also carry a line of defense to prevent the leakage of children's privacy on the Internet. Network service providers should materialize the principle of informed consent and abide by professional ethics, and strictly prohibit providing children's personal information directly or indirectly to third party, and selling it to unscrupulous elements. The Internet industry can establish convention guidelines or industry associations among themselves, as well as establish management grading systems, sign protection agreements, and post self-regulatory logos, among others. In view of the relative weakness of the current technical standards and regulatory system for children's online privacy, many apps and social platforms should actively explore corresponding technical safeguards on the basis of strict compliance with the relevant laws and regulations on children's privacy protection. For example, they can develop and design technologies and products that meet the requirements of children's privacy protection, adopt product design concepts in which privacy protection is the primary consideration, and strengthen data privacy protection technologies, including encryption, anonymization and data rights management, so as to ensure the privacy and security of children when using various applications and services.

State Responsibility: Improving Policies, Regulation and Legal System

The lagging nature of the law is difficult to overcome, but the government should still strengthen the formulation and improvement of laws and regulations for the protection of children's online privacy. Considering that children do not have sufficient cognitive ability, control ability and self-protection ability, their rights and interests are more likely to be infringed upon (Zhang, 2015). Therefore, in terms of personal information protection and utilization, special protection should be provided for children. It is reasonable to include children's personal information into the scope of sensitive information protection. By developing a comprehensive legal framework, children will enjoy the same or even a higher level of real-life privacy rights protection. Although recent regulatory developments, for example the General Data Protection Regulation (GDPR) and proposals for child-friendly design, have recognized the need for better design for children, children have only occasionally been consulted in these efforts. Designers and policymakers should recognize the interests of children and the need to involve children in design and policymaking (Zhao et al., 2019).

We are able to detect possible abuses in the collection, processing and transmission of data that may exist, as well as penalties for violations of children's right to online privacy. In addition, appropriate penalties must be established and enforced for any violation of children's online privacy, and to protect and care for children's online safety rights and interests at the legal level. Steeves and Webster (2008) suggested that parental supervision is not sufficient to reduce privacy risk behaviors. In turn, children's willingness to comply with the types of privacy-protective behaviors promoted by adults is also related to their desire to interact socially with peers and to use the Internet to play social roles with different identities. Thus, policymakers should revisit the current policy paradigm - which focuses on the central role of parents in reducing privacy risk behaviors - and examine how to expand online privacy protections for children. Governments can also actively promote public participation and monitoring of children's online privacy, and encourage social organizations, the media and citizens to supervise privacy protection issues, so as to promote the implementation and enforcement of relevant policies. Given the difficulty at the technical level, national governments should work to push Internet companies and service providers to take effective measures to enhance the protection of children's privacy. For example, companies are called upon to introduce encryption technology and anonymization in user registration, data storage and exchange to minimize the risk of unauthorized access or leakage of personal information. In fact, the industry does have the responsibility and obligation to protect the privacy of Internet users from being infringed upon, but it is unrealistic to expect to rely entirely on the industry itself. The most important thing that the government should do to strengthen regulation is to set up a self-regulatory mechanism for the Internet industry, establish more stringent laws and regulations on children's privacy protection and technical standards, and strengthen the supervision of relevant enterprises and platforms. The mechanism should mainly regulate and supervise social media, Internet companies and other related organizations to ensure that they comply with the relevant privacy protection laws and regulations, and that they do not collect and misuse children's personal information.

Cooperation to Achieve Win-Win Situation

Due to the borderless nature of the Internet, with the development of the Internet, children's personal information may be exchanged and stored across national borders. However, there are differences in the legislative standards and principles of personal information protection laws across countries and regions, and the complexity of cross-border data flow brings challenges to the protection of children's online privacy. Therefore, it has become particularly important to collaborate across national borders, which is the main reason why the United Nations has been calling on governments, international organizations and NGOs to strengthen their cooperation and work together to protect children's right to online privacy through cross-border cooperation and joint efforts. Governments can work together to develop and implement policies and measures to protect childre's online privacy through cross-sectoral cooperation, including education, communications and child welfare. Enhanced cooperation can improve the comprehensive governance capacity of governments in this area. At the same time, different countries have strengthened communication and coordination to jointly develop binding and highly enforceable global standards to ensure that all children can benefit from a unified and solid online privacy framework. The international technology industry, government departments and social organizations also need to strengthen cooperation and work together to solve the technical protection problems of children's online privacy. To summarize, countries need to make joint efforts in legislation, education, regulation, technical support and public participation to build an all-encompassing, multi-level protection system to make sure that children can grow up safely and healthily in the online environment.

Conclusion and Implications

Children's online privacy is a basic right of children and an important guarantee for their healthy growth. However, in reality, children's online privacy rights are often violated, including Sharenting, which may cause great harm to children's physical and mental health.

The core value of this study is to highlight the urgency of the protection of children's online privacy and reveal the shortcomings of the current practice in the protection of children's online privacy. At the same time, it draws on the practice of the United Nations and relevant documents to provide theoretical support for the improvement of relevant laws and regulations.

In order to protect children's online privacy, we need the joint efforts of the whole society. In the digital age, we need to continuously explore and improve laws, regulations and technical means to adapt to the development trend of the Internet, strengthen the supervision of Internet data, and increase the public's awareness and attention to children's online privacy. Joint efforts are necessary for children to grow up in a healthy online environment, and governments, schools, families, businesses and other parties need to work together to create a safe and healthy online environment. Only in this way can we pave a safer, healthier and more just path for children's future.

Limitations

The limitations of this paper are that the reality is evolving and may be even more challenging than analyzed in this paper. In addition, due to the limited scope of the study, we are unable to comprehensively explore the measures and approaches taken by various countries in protecting children's privacy. Taking COPPA as an example, although this paper points out the shortcomings of the act in protecting children's online privacy, COPPA has been improving and advancing since its implementation. This suggests that legal measures for the protection of children's online privacy need to be cognizant not only of the problems that exist, but also of the measures that have been taken by the relevant parties to remedy them.

What's more, from an international perspective, measures to protect children's online privacy vary from country to country. Future research could explore specific countries or regions to gain a more comprehensive understanding of children's online privacy protection. This will help us better understand the strengths and weaknesses of each country in protecting this right, thus providing useful reference and inspiration for the protection of children's privacy on the Internet globally.

References

Amon, M. J., Kartvelishvili, N., Bertenthal, B. I., Hugenberg, K., & Kapadia, A. (2022). Sharenting and children's privacy in the united states: Parenting style, practices, and perspectives on sharing young children‘s photos on social media. *Proceedings of the ACM on Human-Computer Interaction, 6*(CSCW1), 1-30.

Andrews, J. C., Walker, K. L., Netemeyer, R. G., & Kees, J. (2023). Helping Youth Navigate Privacy Protection: Developing and Testing the Children's Online Privacy Scale. *Journal of Public Policy & Marketing*, 07439156231165250.

Bélanger, F., Crossler, R. E., Hiller, J. S., Park, J. M., & Hsiao, M. S. (2013). POCKET: A tool for protecting children's privacy online. *Decision Support Systems*, 54(2), 1161-1173.

Blum-Ross, A., & Livingstone, S. (2017). "Sharenting," parent blogging, and the boundaries of the digital self. *Popular communication*, 15(2), 110-125.

Brown, D. H., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. *Journal of Children and Media*, 8(2), 201-207.

Chóliz, M. (2012). Mobile-phone addiction in adolescence: the test of mobile phone dependence (TMD). *Progress in health sciences*, 2(1), 33-44.

Eldar. (2020). The Internet of Children: Protecting Children's Privacy in A Hyper-Connected World (November 21, 2020). *UNIVERSITY OF ILLINOIS LAW REVIEW*, 2020, 1209-1248.

Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. Retrieved from https://firstmonday.org/ojs/index.php/fm/article/download/3850/3075#p6. [Accesed: 11/13/23].

Johnson, A. F. (2020). 13 Going on 30: An Exploration of Expanding COPPA's Privacy Protections to Everyone. *Seton Hall Legis. J.*, 44, 419.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: growing up in a digital age: an evidence review. Retrieved from http://eprints.lse.ac.uk/id/eprint/101283. [Accesed: 11/13/23].

Lwin, M. O., Stanaland, A. J., & Miyazaki, A. D. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of retailing*, 84(2), 205-217.

Manotipya, P., & Ghazinour, K. (2020). Children's online privacy from parents' perspective. *Procedia Computer Science*, 177, 178-185.

Marasli, M., Suhendan, E., Yilmazturk, N. H., & Cok, F. (2016). Parents' shares on social networking sites about their children: Sharenting. *The Anthropologist*, 24(2), 399-406.

Minkus, T., Liu, K., & Ross, K. W. (2015). Children seen but not heard: When parents compromise children's online privacy. *In Proceedings of the 24th international conference on World Wide Web*, 776-786.

Sorensen, S. (2016). Protecting children's right to privacy in the digital age: Parents as trustees of children's rights. Child. *Legal Rts. J.*, 36, 156.

Steeves, V. (2006). It's not child's play: The online invasion of children's privacy. *U. Ottawa L. & Tech. J.*, 3, 169.

Steeves, V., & Webster, C. (2008). Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society*, 28(1), 4-19.

Steinberg, S. B. (2017). Sharenting: Children's privacy in the age of social media. *Emory Law Journal*, 66, 839.

Verswijvel, K., Walrave, M., Hardies, K., & Heirman, W. (2019). Sharenting, is it a good or a bad thing? Understanding how adolescents think and feel about sharenting on social network sites. *Children and Youth Services Review*, 104, 104401.

Zhang, H. M. (2002). On the legal protection of network privacy. *Journal of Peking University (Philosophy and Social Sciences)*, S1, 165-171.

Zhang, X. B. (2015). From privacy to personal information: Theory for remeasuring interests and institutional arrangements. *China Legal Science*, 2015(03), 38-59.

Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., & Shadbolt, N. (2019). I make up a silly name': Understanding children's perception of privacy risks online. Retrieved from https://doi.org/10.1145/3290605.3300336. [Accesed: 11/13/23].