JOPAG
JOURNAL OF POLITICS AND GOVERNANCE

Journal of Politics and Governance
14(3), September – December 2024

Protecting Children's Privacy: Legal Strategies to Limit Sharenting in Thailand

Wasin Yimyam [1]

[1] Faculty of law, Ramkhamhaeng University, Thailand
ORCID ID: https://orcid.org/0000-0001-9738-9195, Email: wasin.yi@ru.ac.th, © Authors

Article history:

Received: November 11, 2023

Revised: April 14, 2024

Accepted: April 19, 2024

Keywords:

Sharenting, PDPA,
Personal Data Protection,
Child Protection

Abstract

The rise of social media has led to the phenomenon of "sharenting" - parents sharing extensive personal information and pictures of their children online. While this practice is well-intentioned, it raises significant privacy concerns for children whose personal information is published without their consent. Thailand, where social media usage is very high, but data protection laws are still emerging, is an example of the challenges of protecting children's online privacy. This study analyzes the Thai legal framework for the protection of children's personal data, particularly about sharenting and the "right to be forgotten" under the Thai Data Protection Act (PDPA). Through a comparative analysis of data protection regimes in the United States and the European Union, gaps in Thai laws are highlighted. The study highlights the urgent need for Thailand to clarify the policies and procedures that allow children to request the deletion of their data shared online by their parents. It suggests possible changes to existing child protection and privacy laws to better define the boundaries for parental sharing of children's information. It also recommends raising parental awareness and creating mechanisms for children to exercise their privacy rights. In light of growing concerns about digital privacy, this study highlights the importance of continuously reviewing and strengthening legal protections for the most vulnerable members of society.

1. Introduction:

Social media has revolutionized how we interact online, and its impact on parenting is no exception. In today's digital age, many parents use social media to document their children's lives and share their experiences with others (Brosch 2016). However, the practice of "sharenting" has raised concerns about children's privacy and personal information being shared online without their consent (Steinberg 2017). This problem is particularly worrying in Thailand, where internet usage is rapidly growing, and children's rights to privacy are not always clearly defined.

The COVID—19 pandemic has only accelerated the trend of "sharenting," with many parents working from home and using social media to connect with others. As a result, there has been a surge in data exchange and storage, which has also increased threats to privacy rights (Amon et al., 2022). In Thailand, approximately 52.25 million

people, or 72.8% of the population, use social media, according to a report by Datareportal Digital. (Internet Usage in Asian Internet Users 2023; Datareportal Digital 2023) This widespread adoption of smartphones and increased internet usage has increased privacy violations, particularly against children (Livingstone & Smith 2014).

Despite the potential risks, Thailand's legal framework for protecting children's privacy on social media is still in its infancy. This study aims to analyze Thailand's current laws and regulations that protect children's personal information and privacy rights from being shared on social media. Specifically, we will explore the right to the erasure of personal data and the extent to which current laws address this right. This study will use qualitative and documentary research models to gather information from various sources, including constitutional provisions, textbooks, articles, dissertations, expert opinions, and critical analysis.

The significance of this study is to bring attention to the issue of "sharenting" and to explore the legal framework in Thailand that protects children's rights to privacy. Children are particularly vulnerable to privacy violations on social media, and their rights must be protected to ensure their safety and well—being. By analyzing current laws and regulations, we can provide guidelines for further legislation that better protects children's privacy rights on social media.

2. Materials and Methods:

This research examines the legal provisions that protect children's personal information and privacy rights in Thailand and other countries with strong privacy laws. By analyzing laws from Thailand and countries such as the United States and in Europe, this study aims to understand the measures in place to safeguard children's personal information and privacy.

The methodology for this research will involve a thorough review of relevant laws, regulations, and scholarly articles on children's privacy and the protection of personal information. This research will also examine the practical implications of these laws, exploring any challenges or gaps in protecting children's personal information and privacy rights.

The findings of this research will be significant in highlighting the strengths and weaknesses of the legal provisions in place to protect children's personal information and privacy rights in Thailand, as well as providing a comparative perspective with other countries. Furthermore, by drawing attention to areas needing improvement, this research will inform efforts to strengthen the protection of children's personal information and privacy rights in Thailand and beyond.

In conclusion, this research will comprehensively examine the legal provisions in place to protect children's personal information and privacy rights in Thailand and other countries. Furthermore, by analyzing the strengths and weaknesses of these provisions, this research will inform efforts to enhance the protection of children's personal information and privacy rights in the future.

3. The Concept of Protecting Personal Rights and Personal Data:

The contemporary legal frameworks of democratic nations across both international and domestic domains exhibit an almost universal acknowledgment and safeguarding of individual rights. This phenomenon arises from the conceptualization of personal rights as intrinsic human rights, inherent to all individuals from the moment of birth. Consequently, state authorities are expressly proscribed from undertaking any actions that would constitute an infringement or violation of these fundamental rights. The inviolability of such rights is regarded as an inviolable tenet, requiring the utmost adherence and reverence within the juridical sphere. Empirical research endeavors have yielded findings that

elucidate the congruent conceptualization of the "right to privacy" espoused by global and regional international organizations. This shared understanding can be encapsulated as follows: the inviolable personal prerogative and liberty of every human individual to self—determine their existence or modus vivendi by their intrinsic satisfaction or desire, unfettered by the obtrusive interference or interventions of external parties. This formulation posits the right to privacy as an inalienable human right, granting individuals the autonomy to chart the course of their lives without encroachment from extraneous entities or forces (Nimnoo 2019).

3.1 The Concept of Protecting Personal Rights

The concept of individual rights can be traced back to Christian religious teachings and the natural law schools of thought, evolving over an extended period. Throughout history, there have been periods where individual rights were abolished and others where they were more widely accepted.

In contemporary times, the most significant and widely recognized individual rights can be categorized as follows (Nimnoo 2019):

1.*Information Privacy* is a fundamental right concerning personal information, encompassing any data related to an individual that can be obtained directly or indirectly through identifiers such as national identification numbers (e.g., social security numbers) or unique personal elements (e.g., full name, date of birth, biometric data, fingerprints, DNA, etc.). This personal data is subject to regulations governing its collection and management, to safeguard individual privacy.

2.*Bodily Privacy* is a fundamental aspect of personal autonomy that safeguards an individual's physical integrity against invasive procedures or interventions that may violate their privacy rights without informed consent. This concept encompasses the protection of an individual's body from being subjected to operations or experiments that infringe upon their privacy rights, such as genetic experimentation, mandatory drug testing, and other forms of unauthorized bodily intrusion (Beauchamp & Childress 2001).

3.*Privacy of Communication* is a fundamental principle that safeguards the confidentiality and security of individuals' communications, regardless of the medium used. This principle aims to protect the sanctity of communications by letter, telephone, electronic mail, or any other means, ensuring that the content of such communications remains inaccessible to unauthorized parties (Solove 2008).

4.*Territorial Privacy* refers to the concept of establishing boundaries or limitations that prevent unauthorized individuals from encroaching upon or intruding on private premises (Altman 1975). This notion encompasses various aspects, including the installation of surveillance devices such as closed-circuit television (CCTV) cameras and the verification of individuals' identities through national identification documents (ID checks) before granting access to residential or private spaces.

The evolution of personal rights protection in Thailand's constitutional framework has undergone significant transformations over time. The Constitution of the Kingdom of Thailand, B.E. 2540 (1997), marked the first explicit recognition of personal rights in Section 34 (Constitution of the Kingdom of Thailand, 1997). Subsequently, the Constitution of the Kingdom of Thailand, B.E. 2550 (2007), in Section 35, further solidified the protection of personal rights and provided more comprehensive safeguards for personal data (Constitution of the Kingdom of Thailand, 2007). However, when the Constitution of the Kingdom of Thailand, B.E. 2560 (2017), came into effect, the wording in Section 32, which had previously protected personal rights in the 2007 Constitution, was revised to be more concise (Constitution of the Kingdom of Thailand, 2017). This constitutional evolution reflects Thailand's ongoing efforts to adapt its legal framework to address the evolving needs and challenges surrounding personal rights and data protection. The changes in wording and scope across the different constitutional iterations

highlight the dynamic nature of this area and the continuous refinement of legal provisions to keep pace with societal developments.

3.2 The concept of protecting Personal Data

The internet has revolutionized global connectivity and information sharing. While its creative utilization offers manifold benefits, misuse can lead to concerning consequences. Unauthorized access to personal data, illegal content dissemination violating intellectual property rights, cybercrime facilitation, and obfuscation of digital trails exemplify the potential dangers. Such activities infringe upon individual privacy and freedoms, necessitating regulatory measures to strike a balance. Initially, internet content regulation aimed to safeguard minors from harmful materials while preserving free expression and fostering open technological development. Regulatory frameworks must evolve to uphold user rights and safety in the digital sphere (Srihatai 2019).

The protection of personal information privacy on the Internet involves two main approaches: legal measures and self—regulation. Legal measures can be further divided into two (Nimnoo 2019):

1. Comprehensive legislation: This approach involves a single, overarching law that covers all privacy cases. It is commonly found in European countries, such as Sweden and Germany, as well as in countries with common law systems.

2. Case-specific legislation: In contrast, the United States has adopted a sectoral approach, enacting legislation to address specific privacy issues as they arise, such as privacy for medical information, loan information, and so forth.

The second approach is self—regulation, which is widely accepted in the United States. In this model, groups of entrepreneurs or individuals form organizations to create rules, etiquette, and ethical guidelines for self—monitoring (Bambauer 2013). These self-regulatory efforts do not rely on state—enforced legal authority but rather on shared missions and responsibilities. Consequently, self-regulation is generally considered more flexible and voluntary than law enforcement (Hirsch 2010).

The recognition of the significance of privacy and the exercise of individual rights and freedoms has led to the evolution of the protection of individual rights and personal data, both internationally and at the national level. This is reflected in the legal framework that guarantees and safeguards fundamental rights such as Information Privacy, Bodily Privacy, Privacy of Communication, and Territorial Privacy. In Thailand, the Constitution has witnessed continuous improvements in laws aimed at protecting personal rights and personal data, underscoring the importance of privacy and the exercise of individual rights and freedoms in the country's legal landscape.

4. Sharenting and the Protection of Children's Personal Data: A Comparative Analysis of the United States, the European Union, and Thailand

4.1 Protection of children's personal data in the United States

Social media use among young people in the United States is widespread, with 95% of 13-17-year-olds with access to social media and over 45% using it regularly. This technology makes it easier for parents to share photos and updates of their children, with approximately 75% of parents and guardians in the U.S. using social media for this purpose. However, when a parent publicly shares a child's personal information on social media, it creates potential risks, such as exploitation by fraudsters, and negative impacts on the child's well-being, such as bullying or difficulty at school or work (Anderson & Jingjing 2018).

Although the US has privacy and personal data protection laws, including the Fourth Amendment and sectoral laws, there is no centralized law on data protection, such as the European General Data Protection Regulation (Blum—Ross & Livingstone 2017; Keith & Steinberg 2017). This lack of a centralized law means that the US does not have a specific "right to be

forgotten" as provided for in the European Union Directive (Dowdell 2017). One of the reasons for this is that the right to be forgotten conflicts with the fundamental human right to free and open access to information, which is enshrined in the First Amendment of the United States Constitution.

In the U.S., the Restatement of Torts provides legal protection like the "right to be forgotten" and deals with the public disclosure of shameful private facts. Nevertheless, if the information is no longer relevant or has lost its significance, individuals do not have the authority to ask for its deletion (Gajda 2018).

While the Supreme Court has recognized the rights of parents to raise their children and the freedom of expression, these rights are limited and can be restricted if they affect the child's welfare. The court has also recognized the right to privacy in the Bill of Rights, as seen in the 1965 case of Griswold v. Connecticut (Fazlioglu 2021).

In the United States, the Communication Decency Act 1966 (CDA) protects third parties from the content on websites, ensuring that Internet companies can grow without fear of litigation from their activities. Section 230 of the CDA provides online intermediaries with immunity for their editorial decisions regarding screening and deletion from their network. However, the right to be forgotten is still difficult to define and protect in the United States, as it conflicts with the rights of free expression and access to information. It is also difficult to exercise this right in a world where information is usually saved on the internet all the time (Goldman 2007).

Overall, while the US has privacy and personal data protection laws, it does not have a central law for data protection or a specific right-to-be-forgotten law. The US does have legal forgiveness in the Restatement of Torts, which is like the right to be forgotten, but the right to be forgotten conflicts with the fundamental human right to free and open access to information, which is protected by the First Amendment of the United States Constitution (Dowdell 2017).

4.2 Protection of children's personal data in the European Union

Protecting children's personal data privacy is a global issue not limited to specific regions like the European Union (EU) or the United States (Schwartz & Solove 2014). The EU's General Data Protection Regulation (GDPR) provides a central law for personal data protection, but it still has gaps in protecting children's personal data. While the GDPR recognizes the need for specific protection for children's information, the exemption of personal and household activities from the GDPR's provisions creates a loophole that could violate children's rights through practices such as "Sharenting" (Donovan 2020).

Sharenting refers to parents sharing their children's photos and personal information on social media platforms without their children's consent (Barnes & Potter 2020). This phenomenon has become widespread, with some parents sharing information about their children's lives from birth through adulthood (Brosch 2018). However, it is essential to recognize that this practice can put children's privacy and security at risk. Moreover, children may not fully understand the potential risks and consequences of sharing their personal information online (Siibak & Traks 2019).

To protect children's personal data effectively, the GDPR must be refined to address the complexities of family life and household activities. The regulation must provide comprehensive and specific protection for children's privacy, given their vulnerability and the increasing internet use by younger generations. The GDPR recognizes the right to be forgotten, where individuals can request that their personal information be deleted when it is no longer needed or deemed incomplete or inaccurate. This law aims to ensure that data controllers who collect and manage private information respect the rights of data owners and protect their information from misuse (Haley 2020).

Recently, the EU proposed a new directive to address present issues and achieve the most significant benefit for individuals. On June 15, 2015, the Council agreed on the new General

Data Protection Regulation approach. In May 2016, the official texts of the Regulation were launched and enforced, intending to replace Directive 95/46/EC. Under the new directive, the right to be forgotten is provided under the title of "Right to Erasure" in Article 17. This law imposes strict conditions and only allows data controllers to retain personal information for legitimate purposes (Asensio 2020).

In conclusion, protecting children's personal data privacy needs to be addressed globally, and the GDPR needs to be refined to ensure comprehensive protection for children's privacy. While the GDPR recognizes the right to be forgotten, it must address the complexities of family life and household activities to ensure that children's rights are not violated through practices such as sharenting. The new directive proposed by the EU is a step in the right direction towards achieving the most benefit for individuals while addressing present issues.

4.3 Protection of children's personal data in Thailand

Thailand has established a legal framework to protect personal data through the PDPA. The PDPA safeguards personal data and regulates its collection, use, and disclosure by data controllers. The law requires data controllers to obtain consent from data subjects, provide information on the purpose of data collection, and implement measures to secure the data (Greenleaf & Suriyawongkul 2019).

However, the PDPA does not explicitly address protecting children's personal data or provide for their protection. This gap is concerning, as children increasingly use social media and may be at risk of having their personal data shared online. Moreover, there is a lack of awareness among parents and children about the risks of sharing personal data online. Therefore, there is a need for educational campaigns to raise awareness of data privacy and protection (Napatanapong & Ariyasunthorn 2022).

A study of the right to be forgotten in Thailand revealed that while Section 33 of the PDPA protects this right, there are exceptions to its exercise. The lack of clear and comprehensive details on how to exercise the right to be forgotten is an issue, as Thailand does not have a law explicitly protecting this right. Additionally, personal information is not clearly defined, and there are no guidelines on how to make personal data non-identifiable. Therefore, there are no practical details on handling personal data in each case, including exceptions to exercising such rights (Eiamchamroonlarp 2022; Langkarpint 2023).

In conclusion, while Thailand has established a legal framework to protect personal data, including the PDPA, there are gaps in protecting children's personal data and exercising the right to be forgotten. Therefore, there is a need for further education and clear guidelines to protect personal data and privacy, particularly for children who are increasingly using social media.

In summary, the protection of children's personal data and the right to be forgotten is a complex issue that requires comprehensive legal frameworks and clear guidelines in different regions. In the United States, while privacy and personal data protection laws exist, there is a lack of a centralized privacy law and a specific right to be forgotten law, which conflicts with the fundamental right to free and open access to information. The GDPR recognizes the need for special protection for children's data and the right to be forgotten, but still has gaps when it comes to addressing the complexities of family life and household activities such as sharenting. Thailand has introduced the PDPA to protect personal data, but it does not explicitly address the protection of children's personal data and does not provide clear guidelines for exercising the right to be forgotten. Therefore, the legal framework, awareness campaigns and practical guidelines need to be further refined to ensure comprehensive protection of children's personal data and the right to be forgotten in the different regions.

3.Result:

Parents' motivations for sharing personal information about their children online vary greatly. These include sharing family moments with relatives or friends, seeking support for a child's illness, or seeking online fame. Regardless of the motivations, sharing children's personal information can have a direct or indirect impact on their lives—immediately or in the future (Blum-Ross & Livingstone 2017; Steinberg 2017).

Thailand enacted the Child Protection Act of 2003 (CPA) to protect children's personal information. Section 27 prohibits advertising or disseminating information about a child or his or her guardian through mass media or technology if it is intended to harm the child's mental, reputational, or other interests or to gain an undue advantage for oneself or others. Section 50 prohibits guardians and child protection workers from publishing a child's name, photograph, or personal details that could harm their reputation or rights (Chotchaisathit, 2014). However, this protection only applies to third parties, not parents. Parental disclosure of a child's personal details online does not contravene the CPA, as the law assumes parental responsibility for the child's welfare, which creates a gap in comprehensive protection.

The PDPA provides more robust protection for personal data, aligning with the United States' provisions that protect personal data for legal purposes only. Where a specific law infringes personal data, it must be protected unless exceptions apply, such as the collection, use, and disclosure of personal data, the rights of the data subject, and sanctions. Where specific laws do not contain provisions for complaints, powers to order expert committees, or regulatory duties, the PDPA applies. Unfortunately, Thai law does not restrict parents from posting their minor children's personal information online, which could allow it to be used without consent or for illegal purposes.

Regarding the right to erase personal data, Thai society is still adjusting to the new right of individuals to delete, restrict, or alter their historical data on the Internet. The data subject has the right to request deletion or destruction of their personal data under Section 33 of the PDPA. Section 37 (3), meanwhile, requires the personal data controller or processor to delete or destroy the data if it meets the criteria set by law (Eiamchamroonlarp 2022).

The Thai legal system protects children's personal information, but there are gaps in the protection provided by the CPA. The PDPA provides more comprehensive protection, but there are still limitations in the ability to erase personal data from the internet. As technology evolves, the legal system must adapt to provide more robust and comprehensive protection for children's personal information.

Thailand's privacy protection is still in its early stages, reflecting the nation's history of authoritarianism, in contrast to the liberal, individualist principles that underpin privacy protection in many developed countries. Privacy is, therefore, not a widely recognized concept in Thai culture.

In the digital age, sharing personal information online, especially about children, is a common practice among parents. The proliferation of social media platforms has facilitated the sharing of real names, birthdays, photos of birthday parties, and other personal details. However, this widespread sharing of personal information poses significant risks to children's privacy, as unauthorized parties can access and exploit this data (Steinberg 2017). In addition, children may come into conflict with their parents due to the information shared online, which can lead to negative psychological consequences (Duggan et al. 2015).

In Western societies, the protection of personal data has become a major concern, leading to the adoption of laws designed to prevent data breaches. However, the GDPR, a landmark data protection law, fails to address the problem of "sharenting" – a term used to describe the over-sharing of children's personal information by parents on social media platforms (Steinberg 2017). This omission leaves significant gaps in ensuring

adequate protection of personal data. The PDPA, which is modeled after the GDPR, also overlooks the problem of sharenting and currently provides no legal protection for personal information shared by parents on social media.

The PDPA outlines key principles for the protection of personal data in Section 19, such as prohibiting the collection, use, or disclosure of personal data without the consent of the data subject. Consent must be clear and unambiguous and obtained by written or electronic means, and it can be withdrawn at any time, unless otherwise provided by law. It is evident that existing data protection regulations, while making commendable efforts, still have significant gaps, particularly about the emerging issue of sharenting. Consequently, policymakers and legal experts must work together to constantly reassess and improve data protection laws and ensure that they remain comprehensive and adaptable to the evolving technological and societal landscape (Solove, 2021).

Section 24 of the PDPA aims to protect personal data and keep it confidential for the public interest. It includes exceptions for cases where it is necessary to prevent danger to an individual's life, health, or safety, or when the data is publicly available with the explicit or implicit consent of the owner. The collection, use, or disclosure of personal data may also be necessary for contract performance, carrying out a public interest mission, legitimate interests, or compliance with law or exercise of state power. In all cases, protecting the data subject's fundamental rights are considered. Comparing the principles of consent in the PDPA and the GDPR, it is evident that the PDPA in Thailand adheres to the same principles as those set forth in the GDPR.

Article 33 of the PDPA provides for the privacy protection of the data subject's personal data, allowing the data subject to demand that the data controller delete, destroy, or anonymize their personal data. However, this right is not absolute, as Parliament can enact laws waiving the exercise of such rights by personal data subjects.

In conclusion, while the PDPA is modeled after the GDPR, it overlooks the issue of sharing personal information on social media, known as "Sharenting". The PDPA outlines key principles for protecting personal data, including consent and protection of confidential information, while considering exceptions in cases such as public interest, contract performance, and compliance with the law. However, the right to delete or destroy personal data is not absolute and can be waived by Parliament. As privacy protection is still in its initial stages in Thailand, it is necessary to continue to evaluate and improve privacy laws to ensure adequate protection against breaches.

4. Discussion:

The protection of children's privacy is an important concern in Thailand, especially when parents upload photos or videos of their underage children to social networks. Such actions could expose the child's personal information and allow it to be used illegally or without the child's consent, who is the rightful owner of their personal information. While specific laws have been enacted in Thailand to protect personal data, these laws have been drafted based on the guidelines of the GDPR, which include the right of children to request the deletion of their parents' personal information on social media.

Despite these efforts, the Thai legal system has not yet comprehensively addressed this issue. While the PDPA follows the guidelines of the GDPR and recognizes the "Right to be forgotten" of children in Article 33 and Article 37 (2), the Act does not explicitly mention "the right to be forgotten," a provision contained in Article 17 of the GDPR. Consequently, there are no clear procedures in Thailand for the erasure, destruction, or de—identification of an individual's personal information.

Another challenge is that online data retrieval service providers may not be able to delete or destroy the data published by other data controllers. When parents upload their children's personal information to the internet, the child's

right to request the deletion of this data is unclear, which can be a cause for concern.

To address these issues, Thailand needs clear policies and procedures for the deletion of personal data, especially children's data. These policies and procedures should include provisions to ensure that online data retrieval service providers can delete or destroy data published by other data controllers, as well as clear procedures for children to exercise their right to be forgotten.

In summary, the protection of children's privacy in Thailand is a complex issue that requires careful consideration and attention. While progress has been made through the enactment of laws such as the PDPA, there is still work to be done to ensure that children's personal information is protected and their right to privacy is respected. Thailand can take a significant step towards achieving this goal by developing clear policies and procedures for the deletion of personal data.

5. Conclusion:

Thailand has taken measures to protect children's personal information through laws such as the CPA and the PDPA. However, there are gaps in protection that need to be addressed. For example, the CPA does not extend to the protection of parents' personal data and the right to erasure of personal data under the PDPA is limited, highlighting the need to prioritize the protection of children's data online.

Parents play a critical role in protecting their children's privacy when they share their personal information online. However, to improve the protection of children's personal information, the government could consider amending existing laws or regulations to define measures that set limits on the exercise of individual rights and freedoms, particularly where parents may infringe their children's rights to personal information. Specifically, the following amendments could be considered:

1. The Child Protection Act:
   - Expand the scope of the CPA to include provisions to protect children's personal information, not just their physical safety and well-being.
   - Define clear guidelines for parents or guardians regarding the collection, use and disclosure of their children's personal information online.
   - Establish mechanisms for children to report instances where their personal data has been misused by their parents or guardians or shared without consent.
2. The Personal Data Protection Act:
   - Clarify and strengthen the right to erasure of personal data, especially for minors and their parents/ guardians.
   - Define the circumstances in which the right to erasure of personal data can be exercised, considering the best interests of the child and the child's stage of development.
   - Establish a procedure for minors to request the erasure of their personal data, either directly or through their parents/ guardians, with appropriate safeguards and controls.
   - Introduce specific provisions for the processing of children's personal data to ensure that their data is treated with a higher level of protection and care.

In addition, the government could consider introducing education campaigns and awareness programs to inform parents and children about the risks associated with sharing personal data online and the importance of responsible data handling. These campaigns could cover topics such as online safety, best data protection practices and the potential consequences of data breaches.

Continuous evaluation and improvement of data protection laws is essential to keep pace with the ever-evolving digital landscape and new technologies. By closing the gaps in the existing legal framework and prioritizing the data protection of children, Thailand can better protect the fundamental rights and freedoms of its citizens, especially the most vulnerable members of society.

In summary, while Thailand has taken steps to protect children's personal data, further changes and measures are needed to close the gaps in the existing legal framework. By clarifying and defining the boundaries for the exercise of individual rights and freedoms, especially in cases where parents violate their children's rights to personal data, Thailand can strengthen its commitment to protecting the privacy and personal information of its citizens, especially children.

References:

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding.* Brooks/Cole Publishing Company.

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.

Anderson, M., & Jiang, J. (2018). Teens, social media & technology 2018. *Pew Research Center, 31*(2018), 1673-1689.

Bambauer, D. E. (2013). Privacy versus security. *Journal of Criminal Law and Criminology, 103*(3), 667-702. https://scholarlycommons.law.north western.edu/jclc/vol103/iss3/2

Barnes, R., & Potter, A. (2021). Sharenting and parents' digital literacy: An agenda for future research. *Communication Research and Practice, 7*(1), 6-20. https://doi.org/10.1080/22041451.2020.1847819

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics.* Oxford University Press, USA.

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

Bolson, A. P. (2016). Flawed but fixable: Section 230 of the Communications Decency Act. *Rutgers Computer & Technology Law Journal, 42.*

Brosch, A. (2016). When the child is born into the Internet: Sharenting as a growing trend among parents on Facebook. *The New Educational Review, 43*(1), 75-85. https://doi.org/10.15804/tner.2016.43.1.19

Brosch, A. (2018). Sharenting–Why do parents violate their children's privacy? *The New Educational Review, 54,* 75-85. https://doi.org/10.15804/tner.2018.54.4.06

Chotchaisathit, R. (2014). Child protection in Thailand: Towards an improved system (Doctoral dissertation). Charles Sturt University. https://researchoutput.csu.edu.au/ws/portalfiles/portal/9311717/56563

Datareportal Digital. (2023). *Digital 2023: Global overview report.* https://datareportal.com/reports/digital-2023-thailand

De Miguel Asensio, P. A. (2020). Data protection in the internet: A European Union perspective. In *Data protection in the internet* (pp. 457-477). Springer.

Donovan, S. (2020). Sharenting: The forgotten children of the GDPR. *Peace Human Rights Governance, 4*(1), 35-59.

Dowdell, J. W. (2017). An American right to be forgotten. *Tulsa Law Review, 52*(3), 311-337.

Duggan, M., Lenhart, A., Lampe, C., & Ellison, N. B. (2015). Parents and social media. *Pew Research Center: Internet, Science & Tech.* https://policycommons.net/artifacts/618977/parents-and-social-media/1600051/

Eiamchamroonlarp, P. (2019). Right to be forgotten under the Personal Data Protection Act B.E. 2562. *Thammasat Law Journal, 3,* 704-736.

Fazlioglu, M. (2021). The United States and the EU's general data protection regulation. In *Data protection around the world* (pp. 231-248). TMC Asser Press.

Gajda, A. (2018). Privacy, press, and the right to be forgotten in the United States. *Washington Law Review, 93,* 201-264.

Goldman, E. (2007). Search engines defeat "must-carry" lawsuit–Langdon v. Google. *Technology & Marketing Law Blog.* http://blog.ericgoldman.org/archives/2007/02/search_engines_3.htm/

Greenleaf, G., & Suriyawongkul, A. (2019). Thailand–Asia's strong new data protection law. *International Report, 161.*

Haley, K. (2020). Sharenting and the (potential) right to be forgotten. *Indiana Law Journal, 95*(3), 1005-1020.

Hirsch, D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. *Seattle University Law Review, 34*(2), 439-461.

Keith, B. E., & Steinberg, S. (2017). Parental sharing on the internet: Child privacy in the age of social media and the pediatrician's role. *JAMA Pediatrics, 171*(5), 413-414.

Langkarpint, K. (2023). Problems of the protection and enforcing the rights to be forgotten with the Personal Data Protection Act 2562 B.E. in Thai universities. *The Journal of Law, Public Administration and Social Science, 7*(1), 1-24.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635-654. https://doi.org/10.1111/jcpp.12197

Napatanapong, C., & Ariyasunthorn, A. (2023). Protecting children on social media. *Bangkok Post.* https://www.bangkokpost.com/opinion/opinion/2433342/protecting-children-on-social-media

Nimnoo, N. (2019). The legal measures to protect the rights to personal data protection (Doctoral dissertation). National Institute of Development Administration (NIDA).

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. *California Law Review, 102*(4), 877-916.

Siibak, A., & Traks, K. (2019). The dark sides of sharenting. *Catalan Journal of Communication & Cultural Studies, 11*(1), 115-121.

Solove, D. J. (2010). *Understanding privacy.* Harvard University Press.

Solove, D. J. (2021). The myth of the privacy paradox. *Georgetown Washington Law Review, 89*(1). https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2738&context=faculty_publications

Srihatai, N. (2019). Use of an injunction to order access providers to disable access to copyright infringing materials (Doctoral dissertation). National Institute of Development Administration (NIDA).

Steinberg, S. B. (2017). Sharenting: Children's privacy in the age of social media. *Emory Law Journal, 66,* 839-884. https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2

