

Equal Concerns, Unequal Response: A Comparative Examination of Children's Digital Privacy Protections in East Asia

Slava Osipov

Fall 2025

Abstract: *This paper examines the legal frameworks for digital privacy protections in East Asia, with a specific focus on children's digital privacy rights. With the increased digitization of daily life, the rights to privacy and data protection are emerging as key legal concerns. Children are especially vulnerable to economic and interpersonal exploitation through internet technologies, which sets their privacy needs above those of the general user. However, literature on these issues is dominated by studies of the European Union and the United States, where the discourse on privacy first evolved. East Asian states are overlooked despite their growing presence as leaders and consumers of digital technologies. Following the standards of critical comparative law, this paper draws on relevant literature, statutes, and case law to examine the development, enforcement, and effectiveness of privacy law frameworks in this understudied area. It calls for better development of oversight authorities and underscores the benefits of strong civil and criminal law protections for privacy rights.*

INTRODUCTION

The right to privacy is a relatively new specialization in the sphere of legal studies. The earliest academic arguments for the right to privacy emerged in the United States in response to the increased information access enabled by the advent of mass printing and early telecommunications technologies throughout the late 19th century (Warren & Brandeis 1890). However, most foundational statutes protecting the right to privacy emerged in European legislation towards the end of the 20th century. The timing coincides with several potential causes. The first privacy law of its kind was passed in the west German state of Hesse in 1970 (Dowd 2022). Still recovering from twelve years of surveillance-heavy Nazi rule and acutely aware of the Stasi activities in the German Democratic Republic, privacy may have held more cultural relevance for the average citizen than in other regions. However, there is a more material cause for the emergence of privacy laws—the 1960s and 1970s saw an increased use of computing

technologies for mass data processing by governments, especially to support welfare services. The first national privacy law was passed by Sweden in 1973, coinciding with the increase in demand for information to support its growing welfare state (Dowd 2022). Similarly, the United States passed its first privacy act in 1974 as its government agencies began to rely on automated data processing technology, especially by financial agencies such as the Internal Revenue Service (Zang 2024).

In the modern day, privacy law is inextricable from the concepts of digital rights and cybersecurity. The rapid digitization of daily life has made data-reliant technologies a regular part of human interaction. Data is a broad term encompassing general quantitative, factual, or statistical information about a subject. Data is currently collected on individuals by everyone, from governments to mass corporations. A technological society is an information society, and as information technologies require mass collection and processing of digital data to

function and develop, raw personal data has become an increasingly valuable market commodity.

Responding to these concerns, international law has moved to include the digital space in privacy discourse. Much of the investigation and promotion of digital privacy concerns has been handled by the United Nations Office of the High Commissioner on Human Rights, solidifying the digital rights framework as the main means of approaching digital privacy and data protection (Yilma 2018). In 2020, the United Nations Human Rights Council adopted a resolution on “The right to privacy in the digital age”, which, although dubiously binding, has set precedent and definitions for digital privacy discourse in the sphere of international law (United Nations General Assembly 2020). On the side of transnational business, organizations such as the Asia Pacific Economic Cooperation (APEC) and Association of Southeast Asian Nations (ASEAN) have promoted their own internal parameters for digital privacy and data protection (Greenleaf 2014).

Modern privacy laws encompass multiple aspects, from information ownership to secrecy and the rights to be anonymous or forgotten, yet they are also closely tied to the concept of safeguarding. Guaranteeing citizens’ privacy ensures a higher level of personal safety from malicious actors, organizations, companies, or even the state itself. For certain populations, the right to privacy is a greater safety concern than for others. Children growing up in the current technological society face unique vulnerabilities regarding privacy and data protection. Children are exposed to data-driven technologies as early as infancy, such as when parents use a baby monitor that connects to the internet and collects personal data for user optimization. Many children also grow up regularly using digital technology like computers, tablets, or

smartwatches at either the behest of parents or, increasingly, educational institutions. As a result, children growing up today have the most data collected on their daily activities (Van der Hof et al. 2020). As early users of internet technologies, children may not be able to adequately comprehend what information is collected about them, how much of their personal information is collected, and how exactly this data is used by the service providers. These circumstances lead to easy exploitation and violation of personal rights, with a victimization profile uniquely different from adult users (Nair 2006). This paper examines and analyzes the legal frameworks for children’s digital privacy protection, exploring how differences in legal frameworks and case law precedent affect enforcement and implementational efficacy.

KEY TERMINOLOGY

PRIVACY AND DATA COLLECTION

As a legal concept, privacy benefits from its vagueness and broad scope. There is an ongoing debate in the legal literature around the exact definition of the scope and exact limits of the right to privacy (Bennett 2019). This paper aligns with the definition of privacy outlined by Chinese scholar Liming Wang, who suggests that “the right to privacy is a right of personality, enjoyed by a natural person, and he/she can dispose of all personal information, private activities and private areas which belong only to the person and have no relation to public interests” (as cited in Wang 2012, 142). This definition is directly linked to information ownership and disposal and is therefore most interlinked to the scope of digital privacy and data ownership. This paper takes Rebekah Dowd’s (2022) definition of digital data as “any data that is created, stored, used, transferred, and/or manipulated using computer technology, in this case, data of a personal nature” (Dowd 2022, 4). The right to digital

privacy is therefore the right to dispose of all digital personal information, private activities, and private areas which belong only to the person.

DATA CONTROLLERS AND DATA PROCESSORS

There is disagreement in the literature on the correct naming and labelling of agencies that collect, store, and process data. This paper follows the definition of *personal information controller* as outlined in the APEC Privacy Framework, where the *personal information controller* is the agent, “person or organization who controls the collection, holding, processing or use of personal information” (APEC Privacy Framework, 6). However, data may sometimes be processed by a separate organization on behalf of the *personal information controller*. The APEC definition excludes these organizations from the title of controller and fails to adequately define them. In these cases, the agent in the paper is referred to as the *data processor* as per the definitions set out in the EU General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Articles 28-29).

DATA GOVERNANCE

Data governance refers to the internal corporate methods of managing and using data assets. Deeply tied to regulatory compliance, data governance regulates how companies store, use, and dispose of data, making sure that all stages of the process are adequately secure and accurate (Varveris and Fereniki 2019). The data governance framework of a corporation determines how they set and execute data collection and privacy policies. Data governance practices vary between

industries, regions, and corporations, but are largely influenced by the laws and trade treaties of the corporation’s host state.

CONSENT AND CONTRACT

User consent is a common legal basis for the processing of personal data by a data controller/processor. Consent, when provided by a user, must be informed, freely given, and unambiguous, meaning that the user providing consent must be clearly informed of all aspects of data collection and processing by the data controller. Regarding children’s digital privacy, it is generally understood that minors cannot provide informed consent, even though the legal definition of minors varies by state and jurisdiction. A common substitute requirement is parental consent in place of the child; however, there are generally accepted vulnerabilities with this framework, such as the potential for deception on behalf of the child (Verdoodt et al. 2024). The second most common legal basis for data processing is the execution of contractual responsibilities. Contract forms a legal basis for data processing when the controller demonstrates that the processing of personal data is necessary to the fulfilment of contractual obligations (GDPR, Article 6).

RESEARCH GOALS

This paper aims to examine the legal frameworks for children’s digital privacy protection among four leading technologically dependent Asian states: the People’s Republic of China, the Republic of Korea, Japan, and the Republic of China (Taiwan). Despite the rapid rise of Asia as a technological leader and consumer, most research on digital privacy is Eurocentric in scope and analysis. The European privacy framework is extensive and strictly implemented, which makes it an easy point of baseline and comparison. However, taking the EU GDPR as a

baseline presumes the acceptance of European cultural understandings of social society and privacy, which can be incongruent with those found in Asian societies. Additionally, despite the increasing political pushes for increased children's data protection, the standards for children's online safety and privacy are less examined by researchers. This paper therefore contributes a unique perspective both in regional focus and subject matter.

First, the paper overviews existing literature on privacy law, digital rights, and data ownership, and children's digital privacy. The study then compares the existing legal frameworks for children's digital privacy, combining laws on digital privacy, children's protection, cybersecurity, and relevant international treaties. Isolating two key variables— independent oversight authority and enforcement authority—the paper outlines key differences between states and evaluates the relative effectiveness of existing children's digital protection. Examination is based on the hypotheses that 1) the existence of an independent oversight authority streamlines regulation and decreases loopholes, and 2) strong prosecutorial enforcement through a cybersecurity framework is the only method of effective restriction. Finally, the paper follows with a discussion on common deficiencies and future considerations for researchers.

LITERATURE REVIEW

Literature on privacy law and digital data privacy is simultaneously diverse and limited. Most literature is country-specific and concerned with analyzing how privacy factors into the state's legal and human rights framework. Global discussions are split between policy-focused comparative critique and a cybersecurity-focused perspective that integrates privacy with aspects of national and human security. As will be explored

later in the review, the global comparative perspective is limited by regional polarization, with the European Union, the United States, and the People's Republic of China dominating much of the conversation. Meanwhile, private sector case studies provide an alternate route for analyzing the actual implementation of privacy laws. The difficulties with analyzing privacy law frameworks stem largely from scope—privacy encompasses civil law, corporate compliance, criminal law, and, in some cases, human rights law, which requires a large-scale overview of the field.

AN EXCEPTION

A relatively large subfield of privacy law literature is focused on privacy in healthcare, such as enforcement of patient-doctor confidentiality and processing of patients' digital information (Rich 1991; Goodman and Anderson 2002; Emam 2008; Mišić and Mišić 2008; Koontz 2017; McClelland and Harper 2022). This is a long-established and important subfield that deserves consideration and exploration; however, it is outside the scope of this paper.

Privacy in healthcare is often legislated, regulated, and administered by agencies completely unrelated to those enforcing civil privacy law. Additionally, as most healthcare data is classified as sensitive data by default, the compliance standards for the processing of this data are uniquely strict, as is enforcement (Seitz 2010). The relative isolation of this field of data privacy protection makes it difficult to equate and analyze together with civil digital privacy. Literature on this subject is detailed and diverse; in fact, compared to the rest of the literature, this field has an outstanding amount of experimental and empirical research on the effectiveness of specific data governance policies or digital systems (Abouelmehdi et al. 2017; Yin et al. 2019; Chen 2020; De Moraes et al. 2022; Khan et al.

2023; Yadav et al. 2023). This perspective offers invaluable insight into real privacy protection practices that can benefit both the private sector, and there is room for studies that work to integrate the fields through both legal standards and methodologies. However, within the limits of this rather small project, the key legal foundations of medical privacy law are too disparate to be easily compared to the literature examined in the rest of the paper.

LEGAL ANALYSES

A majority of the literature on digital privacy law consists of country-specific policy analysis. Often, this is intended to either draw a genealogy of local privacy law or spotlight the legal basis for developing privacy frameworks (Dowd 2022; Chen and Liu 2024). This literature is especially significant among non-European states that may not share the EU's legal heritage. Literature varies by region and likely by legal structure. For example, literature from civil law countries such as Taiwan, Japan, Korea, and Indonesia often bases itself more on the policy perspective and government response (Murakami 2004; Chen 2012; Shahrullah et al. 2024). Meanwhile, common law literature is more aligned with a genealogical approach that traces the existing precedent for the recognition of privacy as a legally protected right (Murphy 2002; Lamont 2004; Ren et al. 2022).

The comparative law perspective on privacy literature in literature is primarily concerned with exploring global networks and inequalities in existing privacy law standards. Most literature is either exploratory or critical comparative analysis, which, while limited, does complement state-centric privacy law literature. For example, comparative literature on privacy law and data processing policies reveals a crucial incongruence between intent and practical usability of data localization laws, which mandate that sensitive

data must be stored on domestic servers and handled by domestic companies (Varveris and Fereniki 2019). Although this seems beneficial for the country, it does not yield practical results given the practical nature of data processing and storage concerns (Pantos 2021). Similarly, the literature is in agreement that transnational elements of states' privacy policies, while useful, are best served when supported with international treaties or privacy frameworks adopted by transnational organizations (Blackmer 2019; Yilma 2023).

It is important to spotlight the People's Republic of China when discussing both comparative and country-specific privacy literature. The PRC has been proactive in the implementation and development of extensive privacy laws, spanning cybersecurity, civil liability, and regulatory standards. Chinese privacy and data protection laws are comparable with the United States and EU in depth and scope, setting the country apart as not only a regional, but a global leader (Calzada 2022). Chinese authors such as Wang (2012) and Ma (2023) have contributed uniquely Chinese perspectives to the theoretical foundations of privacy law that augment and question elements of the global Eurocentric model of privacy. Additionally, Chinese literature has demonstrated a greater focus on prosecutorial analysis and case precedent as means of evaluating the enforcement of privacy law, despite the PRC not being a common law country (Han 2018; Pyo 2021; Zhang 2023). This provides a refreshing and evidence-based perspective that can serve as a foundation for further similar research outside the PRC.

ENFORCEMENT AND PRIVATE SECTOR CASE STUDIES

Much of the global enforcement-centered literature is centered on compliance in the private

sector. Certain scholars have analyzed the implementation of digital privacy laws from the exclusive perspective of private businesses, pointing out that stricter regulation had generally led to increased consumer trust, positive market outcomes, and decreases in stock-crash risks (Dosis and Sand-Zantman 2023; Song 2024). However, as Dosis and Sand-Zantman (2023) have pointed out, the finer details of how businesses perceive the tradeoff between privacy and data monetization depend on market conditions and are therefore inextricable from the laws and policies that the business is responsible for.

Compliance analysis provides both a convenient source of data and a reasonably simple method of analysis. Multiple studies have been conducted into how top websites collect data and whether these methods are compliant with key privacy laws (Aladeokin et al. 2017; Lin et al. 2022; Conde et al. 2025). These studies are particularly useful in providing empirical data, which can be used for further policy analysis. Conde et al. (2025) is a standout case study that synthesized factual data with a comprehensive legal and regulatory analysis. Similarly, another means of implementational analysis is studying the privacy policies of key internet providers and websites (Yang et al. 2017; Ghahremani and Nguyen 2024). However, there is a noticeable lack of data on real data processing mechanisms as they are implemented beyond the privacy policy and after data on a user has been gathered. Although this is a natural limitation of the field due to the difficulty of such research, it does raise concerns for critical evaluation. A privacy policy is only as effective as it is enforced.

THE CYBERSECURITY PERSPECTIVE

Cybersecurity is a foundational aspect of state-wide data protection frameworks, and the fields of cybersecurity and privacy law are deeply interconnected in modern literature. Unlike

privacy law, which mostly falls under civil tort litigation, cybersecurity is part of criminal law and therefore enforced and legislated through different means. States where ownership, processing, and sale of illegally obtained data are prosecuted under criminal law have access to a stronger enforcement mechanism in the form of criminal litigation (Chen 2018; Mishra et al. 2020; Bui and Lee 2023). Cybersecurity has also raised concerns over the role of the government as a data collecting and processing agent. Privacy laws in countries such as the PRC and Vietnam exclude the government from select data privacy regulations, leading to concerns over cybersecurity and malicious activity on behalf of the government (Bui and Lee 2023; Stancu and Patel 2023). Unfortunately, there is a lack of empirical evidence on this subject, and some literature is tainted with preconceived biases against less democratic states, such as the unfortunate references to the alleged Chinese social credit system by Calzada (2022).

CHILDREN'S DIGITAL PRIVACY

There is a general agreement in the literature that children are an especially vulnerable population in regard to online safety and digital privacy (Kravchuk 2021; Domazet and Šušak-Lozanovska 2023). Scholars agree that children's data is uniquely sensitive due to the risk of its misuse for criminal purposes, with or without involvement of the child (Livingstone et al. 2012; Kravchuk 2022). However, children also face additional risks of exploitation, such as targeted advertising and misinformation that the child is less likely to critically engage with (Tatlow-Golden and Garde 2020; Van der Hof et al. 2020). Moreover, children themselves are less capable of understanding the permanence and scope of their online presence, leading to questions over their ability to consent to terms of service. Consent frameworks that do exist are

largely based on American and European standards, which have limitations in regard to the enforcement of adequate consent mechanisms and age-specific data sensitivity classifications (Macenaite and Kosta 2017). Overall, the literature is unanimous in the fact that current legal approaches to children's digital privacy are underdeveloped and require additional legal protections. However, as with the rest of the literature, there is little comparative analysis, with Verdoodt et al. (2024) as a standout case in its depth and critical examination.

EUROCENTRISM AND BIAS

Global literature on privacy law, data protection, and digital rights is noticeably Eurocentric, both in authorship and subject matter. Some of this bias is natural for the field – the earliest privacy laws were implemented in European countries, European countries led the development of a human-rights-focused digital privacy framework, and the European Union's General Data Protection Regulation (GDPR) remains a leading standard for data protection and digital privacy (Dowd 2022). This is also realistic from the technical and business perspective, as most of the leading global internet providers and digital services are based in either the EU or the United States. Changing policies or legal liability in these regions is more threatening to the business than a local fine in a country where these services are less used.

However, the elevation of the European perspective, especially the use of the GDPR as a standard of comparison for theory development, is also a limitation on the field. This is especially visible in comparative literature. The EU GDPR is often held up as a default global privacy standard, no matter how incomparable its legal foundation may be with the country being analyzed. The modern concept of privacy has largely evolved in Europe and had to be translated to fit different

cultures and legal landscapes. For example, Prasad & Aravindakshan (2021) point out that sociocultural awareness of privacy as a right and common privacy concerns is quite low in South Asian countries, due in part to the digital divide and high illiteracy in the region. This results in less government attention to the issue, and can be considered a cause for the slow, unequal development of general and internet-specific privacy legislation. Scholars also point out that cultural dimensions can significantly affect internet users' approaches to privacy and information disclosure (Lowry et al. 2011; Reed et al. 2016; Meso et al. 2021). In this complex environment, a truly equal comparison between the EU GDPR and countries with a completely divergent privacy history and culture becomes nearly impossible. While it is natural to hold up the GDPR as a milestone in comprehensive and effective privacy protection, scholars should be cautious in setting it as a baseline for comparative literature. In fact, there remains space for further research on why certain aspects of 'western' privacy law have been less adapted in other regions. Regional comparisons that account for shared history and culture while remaining aware of national differences reduce variability and external factors and can better illustrate unique aspects of local privacy challenges.

DISCUSSION

Literature on digital privacy is a vast and actively developing field; however, it does suffer from certain limitations. Methodologically, a significant amount of analysis is limited to legal interpretation or comparative critique. While these methods have their benefits, they are difficult to use as a means of evaluation. Evaluation methods themselves are constrained by research capabilities since detailed analysis of data processing methods requires government and private sector cooperation. In this context,

the Chinese research model with its focus on prosecutorial precedent is a useful baseline for further research, but there may be difficulties with adapting it outside of the country.

As pointed out earlier, regional gaps exist as well, with most comparative analyses either focused or dependent on European and American privacy standards. When examining children's digital privacy, this gap becomes especially noticeable since on a global scale, the EU, the US, and the PRC are relatively anomalous in the extent of their children's digital protection. This paper aims to examine this less studied area by focusing on children's privacy law frameworks in developing Asian countries, a less studied field.

METHODOLOGY

This research aims to explore and evaluate variances in enforcement and effectiveness of the existing legal frameworks for children's digital privacy protection among leading technologically dependent states. To counteract the Eurocentric bias present in much of the literature on digital privacy, this study examines four Asian countries: the People's Republic of China, the Republic of Korea, Japan, and the Republic of China (Taiwan). These countries were chosen as case studies for both their highly developed, flourishing technological private sectors and relative political variability. Despite sharing the same demand for data protection, the states vary in population diversity, political structure, and legal heritage. In order to eliminate extraneous influences and inequalities in analysis, case selection was limited to civil law countries with at least one specialized digital data protection law in effect. Additionally, case selection was limited to only four states by the short research time of the student paper project and the lack of access to English-language sources.

RESEARCHING SECRET

Working with private data provides unique challenges for researchers due to the secret nature of the most relevant data. By design, personal data is meant to be hidden and inaccessible to most people and therefore inaccessible to research. Data privacy must be respected and protected during the course of any research and policy evaluation, and if a framework is truly effective, no personal information will be accessible to the unauthorized researcher. Therefore, just as when working with secrets, the researcher derives an understanding of the subject by probing its boundaries yet never seeing its contents. Exceptions set the rule. Most people become aware of their data privacy standards following news of a data leak, not after carefully reading the terms and conditions for each service they access. A privacy law is only proven ineffective in hindsight after a violation has been brought before the court. In an ideal scenario, the law is passed and obeyed silently. Therefore, effectiveness evaluation is challenging and done in comparative hypotheticals, rather than with strong data to support an argument.

As a result, evaluation within the scope of this study is conducted through critical legal comparison and analysis of relevant publicly available case law. Critical legislation comparison is a foundational aspect of comparative law. By examining relative standards and enforcement methods of different countries, it is possible to outline trends that can be attributed to the variables examined (Zweigert and Kötz 1973). Where possible, statistics on enforcement, prosecutions, and relevant legal cases are used to demonstrate the practical aspects of policy.

HYPOTHESES

The first hypothesis examined is that the existence of an independent privacy oversight authority leads to more effective enforcement of

privacy protections. Under this hypothesis, states that have a unique agency for digital privacy regulation are better able to enforce privacy protections compared to states where enforcement of privacy law is entrusted to multiple relevant federal agencies. ‘Independent’ in this context refers to a digital privacy focused government agency not directly subordinate to a ministry or department and therefore less likely to be affected by undue internal influence. As noted in the literature, although data processing laws, privacy laws, and child protection laws may intersect, they usually develop independently under different agencies and as a result of unrelated political processes. As these laws come together to form a comprehensive digital privacy framework, their divergent origins increase the risk of bureaucratic inconsistencies or overlaps, which make enforcement more challenging. This hypothesis tests whether an independent oversight agency is able to counteract these challenges, as a separate agency would have more resources to concentrate on developing clear laws and protection standards than agencies for whom privacy is a secondary aspect of governance compliance.

Currently, there are no transnational standards or enforcement mechanisms for privacy protection in East Asia. Relevant treaties such as APEC are, while binding, functionally toothless, and mostly exist to set recommended standards for practice (APEC Privacy Framework). Meanwhile, global comparisons of the EU GDPR, China’s PIPL, and other similar laws reveal large discrepancies in governing bodies and bureaucratic structure (Calzada 2022, 1136). One of the reasons for the favoritism of the European framework as a global standard is its creation of an independent agency—the European Data Protection Supervisor—as an independent monitoring body (Regulation (EU) 2018/1725). It

is therefore useful to test whether similar efforts on a domestic level have yielded fruitful results.

This hypothesis is tested through an analysis of relevant legislation, publicly accessible government agency records, and enforcement directives. Effectiveness is evaluated on the presence and relative comprehensiveness of a state’s privacy protection legislation, as well as the existence of any disciplinary actions or interventions taken against companies found to be in violation of privacy protection laws. When possible, relevant literature is consulted for additional information on these agencies’ practices.

The second hypothesis examined presumes that strong prosecutorial enforcement through a cybersecurity framework is a method of effective data protection. Under this hypothesis, if the state has a precedent of prosecutorial enforcement of digital privacy, civil or common law, the state is able to compensate for deficiencies such as a lack of explicit privacy protection in the civil code. As the literature points out, even when relevant digital privacy legislation and enforcement authorities exist, their effective enforcement capabilities are often limited to issuing guidelines, fines, and regulatory standards, while the actual compliance enforcement is left to internal corporate data governance policies (Varveris and Fereniki 2019). Legal prosecution is left to cases where citizens raise lawsuits against a company for individual privacy violations, rather than by the state for violations of the law. In states where civil law is less developed or accessible for the citizens, this system renders many policies unenforceable and is especially vulnerable to issues such as corruption and white-collar crime.

However, cybersecurity law is a legal area that does show evidence of ample state prosecution and is an aspect of many digital protection frameworks in selected states. This is especially

true in the People's Republic of China. The hypothesis is tested through an examination of relevant states' cybersecurity law, data protection law, and case law precedent, and a macroscopic case law comparison.

CASE PRESENTATION

REPUBLIC OF CHINA (TAIWAN)

Out of the cases examined, the Republic of China, commonly known as Taiwan, was the first to implement a digital privacy law. Taiwan first passed the Personal Data Protection Act (PDPA) in 1995, even though it has since then undergone significant amendments in 2010, 2012, 2015, 2016, and most recently in 2023 (Personal Data Protection Act 2023). Personal information controllers are required to inform subjects of the purposes and scopes of data collection and obtain user consent for data processing (Ibid, Articles 7, 15, 16, 19, 20). The data subject is guaranteed the rights of access, cessation, correction, and deletion. The Taiwanese civil code Article 195 recognizes the right to privacy, allowing private citizens to bring civil suits for the infringement of privacy against corporations or private individuals, which is unique among other examined cases (Civil Code, Article 195).

Before the 2023 amendments, Taiwan did not have an independent oversight authority such as the Personal Information Protection Commission, and enforcement responsibility was split between government ministries, most often the Ministry of Justice and the Ministry of Digital Affairs. Following the 2023 amendments, the PDPA was modified to include provisions for the creation of a Personal Information Protection Commission. As of April 2025, the commission is still in preparatory stages and unable to act as an oversight authority in administrative capacity (MaMattina 2025).

The PDPA does not have any explicit standards for children's digital privacy or

additional regulatory requirements for processing children's personal data (Tseng and Huang 2024-25). Due to the lack of a unified oversight authority, relevant regulatory authorities may independently levy higher standards for children's data, such as requiring parental consent; however, there is no government or industry standard.

JAPAN

Japan introduced its comprehensive privacy law relatively early in 2003. The Act on the Protection of Personal Information (APPI) set out legal duties for the safeguarding of personal information by both government agencies and private corporations and established the Personal Information Protection Commission (PIPC-J), a centralized government authority directly under the office of the Prime Minister. The APPI has been regularly amended and updated since 2003, with significant changes in 2020 that introduced stricter user consent requirements, standards for the processing of biometric data, proposed the implementation of fines, and additional clarifications (Act on the Protection of Personal Information (Act No. 57 of 2003), Articles 131, 132). Personal information controllers are required to clearly inform users of data collection purposes and methods, disclose any third-party personal information processors, and obtain the consent of the user for data collection. The private individual is guaranteed the right to cease the provision of data, as well as the rights to access, correction, and deletion. In terms of enforcement, the Personal Information Protection Commission issues guidelines as well as improvement orders for private corporations deemed to be lacking in regulatory practices. Despite theoretical capacity, the agency itself has not issued any administrative fines for misconduct (Pardieck 2023).

Similar to Taiwan, the APPI lacks additional regulations for the processing of children's data. The APPI does recognize that minors aged between 12 and 15 years of age do not have the capacity to critically give consent; however, there are no further regulations for any proxies, such as parental consent (Hayashi and Yukawa n.d.). Since the 2020 amendments, interim reports published by the PIPC-J have regularly referenced the need to develop policies that address children's digital privacy; however, no such act or amendment has yet been passed.

KOREA

Korea's digital privacy rights are guaranteed under the Personal Information Protection Act (PIPA), passed in 2011. Under the PIPA, personal information controllers are required to minimize the amount of data collected on users, inform the user in detail about the purposes and methods of data processing, obtain user consent in most cases, and provide methods for the user to request information on data collected as well as acquiesce to deletion and correction requests from the user. Contract and legitimate interest are defined as instances where the personal information controller can forgo explicit user consent (Personal Information Protection Act (16930), Articles 15-19). The Personal Information Protection Law is enforced by Korea's own Personal Information Commission (PIPC-K), a central oversight ministry created to continuously develop and amend data privacy policy as well as handle legal concerns regarding the enforcement of the PIPA (Ibid, Article 7). Similar to Japan, the PIPC-K lacks enforcement authority and primarily issues guidelines and recommendations on privacy standards (Ko et al. 2017). However, as of 2024, the Personal Information Protection Commission is also endowed with the power to serve as a mediator in legal disputes (Ibid, 105). Furthermore, the Commission operates several

sub-agencies that handle misconduct reports, information requests, and data deletion request services for citizens.

Amendments introduced in 2023 enshrined essential regulations for the protection of children's digital privacy. Minors under 14 are unable to provide consent, and personal information controllers are required to obtain the consent of a parent for processing data (Personal Information Protection Act, Article 22-2). The same rights of data access, correction, and deletion are guaranteed to the legal representative of the child as to all citizens (Ibid, Article 37-2). This is supported by a 2023 PIPC-K guideline that introduced the right to erasure, or the right to be forgotten, as a key issue for children's digital wellbeing. Although this is a good foundation, these are relatively simple protections. There is no additional mandate to classify children's data as inherently sensitive information, and there are no limitations on how children's data may be processed by personal information controllers.

THE PEOPLE'S REPUBLIC OF CHINA

The PRC is unique for the deep relationship between privacy and national security law. Digital privacy in the PRC is guaranteed by the 2016 Cybersecurity Law, 2021 Data Security Law, and 2021 Personal Information Protection Law. As of 2021, the Civil Code also guarantees a right to privacy and a method for civil litigation in instances of privacy infringements. Article 253a of the PRC Criminal Code makes the sale of personal information in violation of state regulation a crime punishable by both fines and potential imprisonment between 3 and 7 years.

The PRC does not have a singular oversight or enforcement authority for digital privacy. Criminal investigations and penalties are enforced by the Ministry of Public Security, while policy development and coordination are

primarily under the authority of the Cyberspace Administration of China (Data Security Law of the People's Republic of China, Article 6). Sector-specific privacy administration, however, is delegated to relevant ministries.

Under the PIPL, citizens also have the right to access, correct, or delete personal data, as well as to withdraw consent. While consent and contract are primary justifications for data processing, the PIPL also includes permissions such as the necessity of ensuring public safety and, in limited situations, of conducting news reporting or opinion supervision (Personal Information Protection Law, Article 13). Out of the four cases, Chinese law has the most thorough safeguards for children's digital privacy. The PIPL is explicit and strict in regulating how children's digital data is processed. Personal data processors are required to classify any information collected from minors under the age of 14 as sensitive. Just as in Korea, a minor's data can only be processed with the explicit consent of the minor's parent (Ibid, Articles 30, 31).

THE VALUE OF INDEPENDENT OVERSIGHT AUTHORITIES

Of the four examined cases, only Korea and Japan have established independent oversight authorities—the PIPC-J and PIPC-K. Among the existing frameworks, the Personal Information Protection Commissions of Korea and Japan show significant administrative benefits. The Commissions are able to regularly update the laws to address developing trends and, when necessary, supplement the text of the law with even more regular enforcement decrees and interpretations. This keeps the law “alive” and malleable enough to address the rapidly changing concerns of the digital environment, despite limitations of the civil law system. For example, PIPC directives have served as the mechanism for promoting children-specific data processing

standards among Korean companies, and the 2023 “Protection of Children's Personal Information” amendment can contribute to its work (Kim and Chang 2022). Meanwhile, Japan's PIPC served as the country's international representative on data privacy issues and was responsible for the passage of the General Data Protection Regulation Adequacy Decision between the European Union and Japan—an EU decision that recognized Japan's APPI as equivalent in protection to the EU GDPR and has allowed for the open flow of data between Japan and EU member states (Wang 2019).

However, there is a valid concern that these commissions are functionally toothless in terms of enforcement capabilities and real proactive data protection. Recommendations and directives published by PIPC-K and PIPC-J are unenforceable, and neither agency has utilized its authority to levy fines on infringing parties. Both Korea and Japan leave the enforcement of digital privacy standards to “relevant authorities” such as telecommunications and digital affairs ministries, which are able to deliberate on industry-specific standards. Although the mediation authority of the PIPC-K is a promising move towards a more proactive direction, it is a recent decision, and neither Japan's APPI nor Taiwan's proposal for its own Personal Information Protection Commission shows a similar trend.

The existence of a Personal Information Protection Commission does not guarantee stricter standards for children's digital privacy. Neither Japan nor Korea has resoundingly strong child-centered privacy protections, with Japan especially lagging behind in lacking both consent restrictions and sensitive data classification requirements. Meanwhile, there are noticeable differences between the ambitious guidelines of the PIPC-K, which include genuinely innovative, considerate points such as a requirement for the destruction of the minimal necessary data on a

child under 14 to obtain their parents' consent after it has been obtained, and the real, limited protections passed into law in 2023. This demonstrates not just enforcement, but also advisory limitations of these organizations, since neither the PIPJ-J nor the PIPIC-K has been able to lobby for a comprehensive amendment on children's data protection despite recognized awareness of the issue and their theoretical position as the national authority on data privacy management.

CYBERSECURITY PROSECUTION AND CIVIL LITIGATION

China and Japan stand out as flourishing examples of effective litigation-focused approaches to data privacy. While Japanese civil law does not explicitly recognize a right to privacy, the right has been argued and supported through multiple significant court decisions, with civil litigation providing the most direct privacy enforcement method. For example, the Supreme Court's monumental 2003 decision in *X vs. Waseda* ruled against Waseda University for disclosing personal identifying information such as names, addresses, and phone numbers of student protestors to police (Pardieck 2024). This ruling set a precedent for recognizing limitations on disclosure of personal information to third parties and of a subject's authority over their own data. In 2014, following a large-scale data breach from Japanese company Benesse, about 12,000 citizens filed a class action lawsuit against the company seeking damages. Following an initial acquittal, the case moved to the Supreme Court, which reversed and ruled that the leak was an infringement of the plaintiff's privacy and the personal data in question was legally protected (Ibid, 21). With the PIPC-J lacking in any enforcement capacity, a strong precedent of civil litigation and Supreme Court decisions that uphold the right to privacy make up for the

inadequacies of the administration. Although this is a posthumous, not proactive, system, a credible threat of litigation may serve as an adequate motivator for companies to implement stricter data governance frameworks that fit APPI standards.

Among the analyzed cases, the PRC stands out for guaranteeing the right to information privacy in both civil and criminal law. Just as in Japan, China has a strong history of data breach litigation, although cases have not reached the Supreme Court due to fundamental differences in legal foundations. Moreover, lawsuits are regularly brought against companies by the People's Prosecutors rather than private parties. Conde et al. (2025) analyze the case of Didi, a transit company that illegally collected user data without adequately informing customers or obtaining user consent. The Cyberspace Administration of China and the People's Procuratorate found the company to be in violation of criminal, civil, consumer rights laws, as well as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. The company was fined and temporarily removed from app stores within the country (Conde et al. 2025, 5). Legal liability also extends to the individual citizen, with case law precedents such as *Wang Fei v. Zhang Leyi* for the illegality of publicly revealing private identifying information by citizens (Han 2018, 442).

The DIDI case is unique, as it was initiated by the government and the People's Procuratorate following an investigation by the Cyberspace Administration. Out of all four countries examined, China is the only one where the state itself has initiated legal action for violation of privacy laws. Although prosecution is again a posthumous activity, the legal decisions enacted by the Cyberspace Administration of China are some of the clearest examples of proactive policy enforcement, where government agencies

cooperate with state prosecutors to independently investigate and later prosecute breaching offenders. Compared to all other cases, the PRC's framework is the most aggressive, and although new, already shows signs of effective enforcement beyond best practice recommendations. As civil litigation may be inaccessible to citizens due to prohibitive costs, time investment, or complexity, this provides an alternative pathway for accountability and justice that represents all citizens. Paradoxically, this practice can be argued as less accessible, as all citizens are represented by the Procuratorate, yet none are direct plaintiffs who could benefit financially.

DISCUSSION

This project failed to find support for the first hypothesis that oversight administrations strengthen privacy protection policies or enforcement. While oversight authorities show administrative benefits, it is difficult to definitively argue that they guarantee a safer digital privacy environment, and, in practice, many do not currently function as enforcement agencies. The most thorough privacy framework, both generally and regarding children's digital privacy, was in the PRC, the one state without an independent oversight authority.

In both Japan and Korea, the PIPCs already have all the necessary foundations to serve as enforcement commissions. They oversee bodies that conduct market research, collect and respond to citizen complaints, and compile reports on entities that violate the law. It is not difficult to imagine these foundations used to develop a collaboration with the relevant justice ministries to issue fines or citations for offending companies. There is also room to develop the mediation role that PIPC-K currently holds. Mediation is notably limited to an advising capacity, and giving the PIPC arbitration

authority may lead to innovative developments of privacy litigation and administration where the binding decisions create a third avenue for legal precedent that does not require lengthy litigation. This may also fit the political climate in Korea, where the government serves not as judge and prosecutor, as in China, but as a guiding authority amicable to both citizen and corporation.

Evidence generally supports the second hypothesis, demonstrating a correlation between increased civil litigation, criminal litigation, and policy enforcement, especially in the People's Republic of China. However, this hypothesis can be challenged by isolating the PRC for its uniquely centralized political structure and ease of government oversight. By framing citizens' privacy as both a human right and an aspect of national security, the PRC is able to engage the state apparatus for privacy law enforcement. Enshrining privacy in criminal law allows the state to prosecute cases on behalf of the citizen, rather than leaving it to the victim.

This practice is difficult to translate to states where the relationship between state, citizen, and corporation is loose. Korea, Japan, and Taiwan are capitalist states with relatively relaxed corporate regulations. It is not surprising that all have been reluctant to bring the power of the state against private business. Japan, the alternate example of developed privacy litigation, has no precedent for state agency involvement, with the outcomes of these cases affecting the judicial system, not government policy. The stricter separation of government makes a comparison with the PRC limited, and this takeaway may benefit from future comparative study of the PRC and other relatively more statist countries, such as Vietnam or Nepal.

CONCLUSION

This paper examined digital privacy frameworks in four East Asian states with a

specific focus on children's digital privacy protections. Overall, while all four states contain well developed legal privacy protection frameworks, children's digital privacy is less standardized, with only Korea and the PRC enshrining requirements into explicit law. Taiwan and Japan are most underwhelming, with no outstanding legal protections and meager efforts from relevant agencies to promote stricter standards. The focus on children's privacy illuminates legal shortcomings. As previously mentioned, the European Union has recognized Japan's APPI as functionally equivalent in degree of privacy protection through the General Data Protection Regulation Adequacy Decision. The lack of child-specific privacy protections in the APPI, however, places this equivalency into question.

The states analyzed in this paper are less examined in the general literature, with only the PRC receiving significant attention from Western privacy experts. This study contributes a novel comparison that centers on the regional context and builds on previous research regarding digital privacy standards in East Asia. It is difficult to argue generalizability since the study was specifically limited to concentrating on unique aspects of privacy law development in East Asia. The PRC, ROC, Japan, and Korea are far more socially and technologically developed than other East Asian countries. However, it is possible to expand this comparison to research that includes Southeast Asia, a region that is deeply connected to its East Asian neighbors in culture, markets, and technological developments. An earlier, more ambitious version of this project sought to include the Republic of Singapore, Republic of Indonesia, Socialist Republic of Vietnam, and Malaysia in comparison. The inclusion of these states would provide more data on the state of data protections in technologically developed

Asian states and better illustrate the regional perspective on privacy in practice.

Additionally, evaluating policy efficacy is difficult without access to empirical data that may be available to a federal agency and not a student. The area of comparative law generally lacks an empirical approach, which could be compensated through larger statistical analyses of litigation trends. Finally, future studies that work more closely with the text of specific court decisions and interpretations may provide fruitful insight into the variability in perception and framing of privacy between different legal structures.

This study also examined the contributions of two legal aspects, independent oversight authorities and litigation precedent, on the effectiveness of privacy law enforcement. Overall, it can be inferred that prosecutorial orientation and case law precedent create a strong foundation for practical privacy rights enforcement, with the cybersecurity and national security perspective contributing the most direct government oversight. The role of oversight agencies is quite complex, and it is difficult to directly associate their existence with improved policy enforcement. Currently, these agencies mostly practice as advising and investigative bodies, especially useful in standardizing and promoting policy development, but have yet to fully realize their potential as effective enforcement or oversight authorities.

POLICY RECOMMENDATIONS

The recommendation that Personal Information Protection Commissions should develop internal agencies with practical authority to levy fines and sanctions seems self-evident. As discussed previously, this addition would consolidate research, enforcement, and policy development under the same standalone government body, which in turn would lend greater authority to the agencies and enable

governments to better protect citizens’ digital privacy rights. States still developing privacy rights and protection commissions, such as Taiwan, would benefit in learning from the examples of Japan and Korea and incorporate enforcement authority from the outset. If that is impossible due to the division of administrative powers, it is beneficial to immediately develop means of information sharing and collaboration with relevant government ministries that have direct prosecutorial authority.

Innovations pioneered by the PRC, such as the codifying of privacy protections into criminal law and strict standards for children’s digital data protection, are genuinely unique and deserve both praise and additional research. Governments should seek to emulate this degree of legal protection, although it is important to keep in mind that the PRC has the most developed legal digital security protections of all examined cases,

and this can be attributed to a unique political climate. Therefore, these standards may be difficult to emulate in other states.

Companies and legal professionals navigating privacy law in East Asia find themselves in a relatively unbalanced field that still has room for better developments. Large transnational businesses operate in all countries with especially great overlap between Japan, Korea, and Taiwan. Yet, there exist no regional equivalency treaties such as the one between Japan and the European Union, and privacy guidelines from treaties such as APEC are explicitly non-binding. As these are all countries that have demonstrated a history of concern and attention to privacy rights, greater collaboration and standardization, in either the public or private spheres, would benefit the region overall. As more Asian corporations take global center stage, this is a field that will only increase in relevance.

APPENDIX

Relevant Legislation	Taiwan (ROC)	Japan	Korea	China (PRC)
Telecommunications Security	Communication Security and Surveillance Act (1999)	Telecommunications Business Law (1984); Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (2000)	Telecommunications Business Act (1995); Act on the Protection of Information and Communications Infrastructure, Etc (2001); Protection of Communications Secrets Act (1993)	Telecommunications Regulations of the People’s Republic of China (2000)
National Encryption	n/a	n/a	n/a	Regulations on the Administration of Commercial Encryption, State Council Directive (1999); Cryptography Law (2020)

Network Security	Regulations Governing Network Interconnection among Telecommunications Enterprises (2017)	Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (2000) Articles 22, 26; The Basic Act on Cybersecurity (2014)	Act on Promotion of Information and Communications Network Utilization and Information Protection (2001)	Cybersecurity Law (2022) Articles 22, 23, 48, 76; Regulations on Network Data Security Management (2024)
Consumer Protections	Consumer Protection Act (2015); Financial Consumer Protection Act (2023)	Basic Act on Consumer Policies (1968); Consumer Contract Act (2000)	Consumer Protection Act (1980)	China Consumer Protection Law (1993)
E-Commerce	n/a	Act on Specified Commercial Transactions (1976); Act on Improving Transparency and Fairness of Specified Digital Platforms (2020)	Act on the Consumer Protection in Electronic Commerce (2002); Guidelines for Consumer Protection in Electronic Commerce, Etc (2003)	E-Commerce Law (2018)
Privacy	Personal Data Protection Act (1995)	Act on the Protection of Personal Information (2003)	Personal Information Protection Act (2011)	Personal Information Protection Law (2021); Data Security Law (2021)
Cybersecurity	Cyber Security Management Act (2021)	The Basic Act on Cybersecurity (2014)	n/a	Cybersecurity Law (2016)
Children's Rights/Protection	The Protection of Children and Youths Welfare and Rights Act (2021)	Child Welfare Act (1947); Child Abuse Prevention and Treatment Act (2000)	Child Welfare Act (2011)	Law on the Protection of Minors (1991)
Children's Digital Privacy	n/a	n/a	Personal Information Protection Act Articles 4-6(3), 22-2, 38-2, 64, 70 (2023)	Personal Information Protection Law (2021) Articles 28, 31; Law on the Protection of Minors (2022) Articles 72, 73, 74

REFERENCES

- Abouelmehdi, Karim, Abderrahim Beni-Hssane, Hayat Khaloufi, and Mostafa Saadi. 2017. "Big Data Security and Privacy in Healthcare: A Review." *Procedia Computer Science* 113: 73–80.
<https://doi.org/10.1016/j.procs.2017.08.292>.
- Aladeokin, Adeyemi, Pavol Zavorsky, and Neelam Memon. 2017. "Analysis and Compliance Evaluation of Cookies-Setting Websites with Privacy Protection Laws." *2017 Twelfth International Conference on Digital Information Management (ICDIM)*.
<https://doi.org/10.1109/ICDIM.2017.8244646>.
- Blackmer, W. Scott. 2019. "Data Protection in the Private Sector: Convergence or Localisation of Rights and Expectations?" In *Human Rights, Digital Society and the Law: A Research Companion*, edited by M. Susi. Taylor & Francis Group.
- Bennett, Thomas D.C. 2019. "Triangulating Intrusion in Privacy Law." *Oxford Journal of Legal Studies* 39 (4): 751–778.
<https://doi.org/10.1093/ojls/gqz024>.
- Bui, Ngoc Son, and Jyh-An Lee. 2023. "Comparative Cybersecurity Law in Socialist Asia." *Vanderbilt Journal of Transnational Law* 55 (3): 631.
<https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss3/2>.
- Calzada, Igor. 2022. "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)." *Smart Cities* 5 (3): 1129–1150.
<https://doi.org/10.3390/smartcities5030057>.
- Chen, Chi-shing. 2012. "Privacy and the new legal paradigm: Tradition and development in Taiwan." *Review of Policy Research* 29 (1): 119-130.
<https://doi.org/10.1111/j.1541-1338.2011.00540.x>.
- Chen, Bing, and Yongji Liu. 2024. "Promotion and Advancement of Data Security Governance in China." *Electronics* 13 (10): 1905.
<https://doi.org/10.3390/electronics13101905>.
- Chen, David. 2020. "Open Data: Implications on Privacy in Healthcare Research." *Blockchain in Healthcare Today*, September 21, 2020.
<https://doi.org/10.30953/bhty.v3.144>.
- Chen, Ji. 2018. "Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China," *International Lawyer* 51 (3): 537-552.
https://scholar.smu.edu/til/vol51/iss3/6?utm_source=scholar.smu.edu%2Ftil%2Fvol51%2Fiss3%2F6&utm_medium=PDF&utm_campaign=PDFCoverPages.
- Conde, Inma, Yixian Li, and Ravi Prakash Vyas. 2025. "Global Companies and China's Data Privacy Laws: Analysing DIDI'S Case and Regulatory Compliance Implications." *Chinese Journal of Transnational Law* 2 (1).
<https://doi.org/10.1177/2753412X241288770>.
- De Moraes Rossetto, Anubis Graciela, Christofer Sega, and Valderi Reis Quietinho Leithardt. 2022. "An Architecture for Managing Data Privacy in Healthcare with Blockchain." *Sensors* 22 (21): 82-92.
<https://doi.org/10.3390/s22218292>.

- Domazet, Siniša, and Ivona Šušak-Lozanovska. 2023. "Children's Data and Privacy Online: Growing up in a Digital Age." *Politika Nacionalne Bezbednosti* 24 (1): 153–173. <https://doi.org/10.5937/pnb24-44680>.
- Dosis, Anastasios, and Wilfried Sand-Zantman. 2023. "The Ownership of Data." *The Journal of Law, Economics, and Organization* 39 (3): 615–641. <https://doi.org/10.1093/ileo/ewac001>.
- Dowd, Rebekah. 2022. *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-82969-8>.
- Emam, Khaled El. 2008. "Heuristics for De-Identifying Health Data." *IEEE Security & Privacy Magazine* 6 (4): 58–61. <https://doi.org/10.1109/msp.2008.84>.
- Ghahremani, Shahram, and Uyen Trang Nguyen. 2024. "Comprehensive Evaluation of Privacy Policies Using the Contextual Integrity Framework." *SECURITY AND PRIVACY* 7 (4): 380. <https://doi.org/10.1002/spy2.380>.
- Greenleaf, Graham. 2014. "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories," *Journal of Law, Information and Science* 23 (1): 4-49. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877.
- Goodman, Kenneth W., and James G. Anderson. 2002. *Ethics and Information Technology*. Springer.
- Han, Dong. 2018. "Search Boundaries: Human Flesh Search, Privacy Law, and Internet Regulation in China." *Asian Journal of Communication* 28 (4): 434–447. <https://doi.org/10.1080/01292986.2018.1449229>.
- Hayashi, Hiromi, and Masaki Yukawa. N.d. "Data Protection Laws and Regulations, Japan." Global Legal Group. <https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan>.
- Khan, Muhammad Ayaz, Subhan Ullah, Tahir Ahmad, Khwaja Jawad, and Attaullah Buriro. 2023. "Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol." *Sensors* 23 (12): 5518. <https://doi.org/10.3390/s23125518>.
- Kravchuk, Natalya. 2021. "Privacy as a New Component of "The Best Interests of the Child" In the New Digital Environment." *The International Journal of Children's Rights* 29: 99-121. <https://doi.org/10.1163/15718182-29010006>.
- Kravchuk, Natalya. 2022. "Privacy of a Child in the Digital Environment: New Risks Unaddressed." *Legal Issues in the Digital Age* 3 (2): 73–89. <https://doi.org/10.17323/2713-2749.2022.2.73.89>.
- Ko, Haksoo, John Leitner, Eunsoo Kim, and Jonggu Jeong. 2017. "Structure and Enforcement of Data Privacy Law in South Korea." *International Data Privacy Law* 7 (2): 100–114. <https://doi.org/10.1093/idpl/ix004>.
- Koontz, Linda D. 2017. *Information Privacy in the Evolving Healthcare Environment*. 2nd edition. CRC Press.

- Lamont, Duncan. 2004. "Privacy-Confidentiality in England: Courts Don't Go West in High-Profile Cases: England Proposes to Avoid Pitfalls of a Privacy Law through Strengthening the Law of Confidentiality and a New Human Rights Law Protecting Private Information." *Defense Counsel Journal* 71 (3): 274-282.
<https://en.humanrights.cn/2023/12/28/fd8a291c5f6d4fce93d7dd8ecba84727.html>.
- Li-Reilly, Yun. 2017. "Remembering, forgetting, reinvention and freedom: social media and children's right to be forgotten." *Advocate* 75 (5): 661-676.
https://farris.com/content/uploads/2019/04/20170914-RTBF_Article_2.pdf.
- Lin, Xinjie, Han Liu, Zhen Li, Gang Xiong, and Gaopeng Gou. 2022. "Privacy Protection of China's Top Websites: A Multi-Layer Privacy Measurement via Network Behaviours and Privacy Policies." *Computers & Security* 114: 102606.
<https://doi.org/10.1016/j.cose.2022.102606>.
- Livingstone, Sonia, Leslie Haddon, and Anke Görzig. 2012. *Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective*. Bristol University Press. <https://doi.org/10.2307/j.ctt9qgt5z>.
- Lowry, Paul Benjamin, Jinwei Cao, and Andrea Everard. 2011. "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures." *Journal of Management Information Systems* 27 (4): 163-200.
<https://www.jstor.org/stable/41304596>.
- Ma, Changshan. 2023. "The Chinese Vision for Digital Human Rights," *Journal of Human Rights* 22 (4): 766-774.
- Macenaite, Milda, and Eleni Kosta. 2017. "Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?" *Information & Communications Technology Law* 26 (2): 146-197.
<https://doi.org/10.1080/13600834.2017.1321096>.
- MaMattina, Lilly. 2025. "Taiwan to Set up Personal Data Protection Commission | Taiwan News | Feb. 3, 2025 19:45." *Taiwan News*, February 3, 2025.
<https://taiwannews.com.tw/en/news/6028406>.
- McClelland, Roy, and Colin M. Harper. 2022. "Information Privacy in Healthcare — The Vital Role of Informed Consent", *European Journal of Health Law* 30 (4): 469-480.
<https://doi.org/10.1163/15718093-bja10097>.
- Meso, Peter, Solomon Negash, and Philip F. Musa. 2021. "Interactions Between Culture, Regulatory Structure, and Information Privacy Across Countries:" *Journal of Global Information Management* 29 (6): 1-14.
<https://doi.org/10.4018/JGIM.20211101.0a49>.
- Mišić, Jelena, and Vojislav Mišić. 2008. "Enforcing Patient Privacy in Healthcare WSNs through Key Distribution Algorithms." *Security and Communication Networks* 1 (5): 417-429.
<https://doi.org/10.1002/sec.40>.
- Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill. 2022. "Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations." *Computers & Security* 120: 102820.
<https://doi.org/10.1016/j.cose.2022.102820>.

- Murakami, Y. 2004. "Privacy Issues in the Ubiquitous Information Society and Law in Japan." *2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No.04CH37583)* 6: 5645–5650.
<https://doi.org/10.1109/ICSMC.2004.1401093>.
- Murphy, Bridget K. 2003. "Developments in the Law of Invasion of Privacy in New Zealand and England." *Auckland University Law Review* 9 (3): 1031-1042.
<https://heinonline.org/HOL/P?h=hein.journals/auck9&i=1051>.
- Nair, Abhilash. 2006. "Mobile Phones and the Internet: Legal Issues in the Protection of Children." *International Review of Law, Computers & Technology* 20 (1-2): 177–85.
<https://doi.org/10.1080/13600860600579779>.
- Pantos, Alexander. 2021. "How the World's Largest Economies Regulate Data Privacy: Drawbacks, Benefits, & Proposed Solutions," *Indiana Journal of Global Legal Studies* 28 (2): 267-292.
<https://www.repository.law.indiana.edu/ijgls/vol28/iss2/7/>.
- Pardieck, Andrew M. 2024. "Privacy Matters: Data Breach Litigation In Japan." *Washington International Law Journal* 33 (1): 1-43.
<https://digitalcommons.law.uw.edu/wilj/vol33/iss1/3/>.
- Prasad, Smitha Krishna, and Sharngan Aravindakshan. 2021. "Playing Catch up – Privacy Regimes in South Asia." *The International Journal of Human Rights* 25 (1): 79–116.
<https://doi.org/10.1080/13642987.2020.1773442>.
- Pyo, Grace. 2021. "An Alternate Vision: China's Cybersecurity Law and Its Implementation in the Chinese Courts." *Columbia Journal of Transnational Law* 60 (1): 228–75.
<https://www.jtl.columbia.edu/volume-60/an-alternate-vision-chinas-cybersecurity-law-and-its-implementation-in-the-chinese-courts>.
- Reed, Philip J., Emma S. Spiro, and Carter T. Butts. 2016. "Thumbs up for Privacy?: Differences in Online Self-Disclosure Behavior across National Cultures." *Social Science Research* 59: 155–170.
<https://doi.org/10.1016/j.ssresearch.2016.04.022>.
- Ren, Raphael, Saw Tiong Guan, Sujata Balan. 2022. "Is There a Private Right to Privacy in Malaysia?" *IJUM Law Journal* 30 (1): 1-32.
<https://heinonline.org/HOL/P?h=hein.journals/iiumlj30&i=258>.
- Rich, Ben A. 1991. "The Assault on Privacy in Healthcare Decisionmaking." *Denver University Law Review* 68 (1): 1-56.
<https://pubmed.ncbi.nlm.nih.gov/11651237/>.
- Seitz, Esther. 2010. "Privacy (Or Piracy) Or Medical Records: HIPAA and its Enforcement." *Journal of the National Medical Association* 102 (8): 745-748.
[https://doi.org/10.1016/S0027-9684\(15\)30651-9](https://doi.org/10.1016/S0027-9684(15)30651-9).
- Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. 2024. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10 (1): 1-20.
<https://doi.org/10.20956/halrev.v10i1.5016>.

- Sørensen, Lene, Knud Erik Skouby, and Samant Khajuria. 2022. *Cybersecurity and Privacy - Bridging the Gap*. 1st ed. River Publishers. <https://doi.org/10.1201/9781003337812>.
- Song, Ziwei. 2024. "Personal Data Security and Stock Crash Risk: Evidence from China's Cybersecurity Law." *China Journal of Accounting Research* 17 (4): 100393. <https://doi.org/10.1016/j.cjar.2024.100393>.
- Stancu, Adriana-Iuliana, and Tal Pavel. 2023. "Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies." *Perspectives of Law and Public Administration* 12 (4): 643–650. https://www.researchgate.net/publication/377110754_Unveiling_Israel's_Cyber_Legal_Landscape_A_Comprehensive_Analysis_of_Cybersecurity_Regulations_and_Policies.
- Tatlow-Golden, Mimi, and Amandine Garde. 2020. "Digital Food Marketing to Children: Exploitation, Surveillance and Rights Violations." *Global Food Security* 27: 100423. <https://doi.org/10.1016/j.gfs.2020.100423>.
- "The Personal Information Protection Commission's Announcement of Guidelines for Protection of Personal Information of Children and Adolescents." 2022. *Kim & Chang*. https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=25476.
- Totterdale, Robert L. 2010. "Globalization and Data Privacy: An Exploratory Study." *International Journal of Information Security and Privacy* 4 (2): 19–35. <https://doi.org/10.4018/jisp.2010040102>.
- Tseng, Ken-Ying, and Sam Huang. 2025. "Data Protection Laws and Regulations Taiwan 2024-2025." Global Legal Group. <https://iclg.com/practice-areas/data-protection-laws-and-regulations/taiwan>.
- United Nations General Assembly. 2020. *The Right to Privacy in the Digital Age*. United Nations Digital Library. <https://digitallibrary.un.org/record/3896430?ln=en&v=pdf>.
- Van Der Hof, Simone, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, and Ton Liefwaard. 2020. "The Child's Right to Protection against Economic Exploitation in the Digital World." *The International Journal of Children's Rights* 28 (4): 833–859. <https://doi.org/10.1163/15718182-28040003>.
- Varveris Alexandros, and Panagopoulou Fereniki. 2019. "The Challenge of Personal Data Protection in the Digital Era and Global Responses." In *Human Rights, Digital Society and the Law: A Research Companion*, edited by Mart Susi. Taylor & Francis Group.
- Verdoodt, Valerie, Yueming Zhang, and Eva Lievens. 2024. "Safeguarding the Child's Right to Privacy and Data Protection in the European Union and China: A Tale of State Duties and Business Responsibilities." *The International Journal of Human Rights* 28 (2): 125–47. <https://doi.org/10.1080/13642987.2023.2233917>.
- Wang, Hao. 2012. "The Conceptual Basis of Privacy Standards in China and Its Implications for China's Privacy Law," *Frontiers of Law in China* 7 (1): 134-160.

<https://journal.hep.com.cn/flc/EN/10.3868/s050-001-012-0007-4>.

Wang, Flora Y. 2019. "Cooperative Data Privacy: The Japanese Model Of Data Privacy And The EU-Japan GDPR Adequacy Agreement." *Harvard Journal of Law & Technology* 33: 661-691.

<https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf>.

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193-220.

<https://doi.org/10.2307/1321160>.

Yang, Lianfeng, Qiuying Chen, and Yonhong Hu. 2017. "An Exploratory Study on the Measuring of Privacy Policies." *WHICEB 2017 Proceedings*.

<https://aisel.aisnet.org/whiceb2017/32>.

Yilma, Kinfe Micheal. 2023. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press.

Yilma, Kinfe Micheal. 2018. "The 'Right to Privacy in the Digital Age': Boundaries of the 'New' Un Discourse." *Nordic Journal of International Law* 87 (4): 485-528.

<https://doi.org/10.1163/15718107-08704004>.

Yin, Xiao Chun, Zeng Guang Liu, Bruce Ndibanje, Lewis Nkenyereye, and S. M. Riazul Islam. 2019. "An IoT-Based Anonymous Function for Security and Privacy in Healthcare Sensor Networks." *Sensors* 19 (14): 3146.

<https://doi.org/10.3390/s19143146>.

Zang, Dongsheng. 2024. "The Privacy Act of 1974: The American Bill of Rights on Data and Its Unfinished Business." *University of Pittsburgh*

Law Review 86 (1).

<https://doi.org/10.5195/lawreview.2024.1051>.

Zhang, Jie. 2023. "The Prosecutorial Protection of Digital Human Rights," *Journal of Human Rights* 22 (5): 1016-1039.

Zweigert, Konrad, and Hans-Jurgen Puttfarcken.

1973. "Critical Evaluation in Comparative Law." *Adelaide Law Review* (5): 343-356.

<https://search.informit.org/doi/10.3316/informit.T2025073100014291378358948>.