A Review of Social Network Regulations and Mechanisms for Safeguarding Children's Privacy

Mykaele F. Abreu, Eduardo K. Viegas, and Altair O. Santin

Pontifícia Universidade Católica do Paraná | Pontifical Catholic University of Parana — PUCPR, Graduate Program in Computer Science — PPGIa, Curitiba, Brazil
{mykaele.abreu, eduardo.viegas, santin}@ppgia.pucpr.br

Abstract. The privacy challenges of social networks and their use by children online require the assessment of legal frameworks and the implemented service provider mechanisms to identify potential gaps. This paper reviews the scientific literature on privacy mechanisms for children on social networks. First, we extensively examine existing legal regulations governing minors' privacy on these platforms. Next, we overview the current scientific literature to assess the mechanisms implemented to safeguard the privacy of minors on social networks. Our findings suggest a lack of consistency in legal frameworks for defining child privacy mechanisms. Similarly, the existing literature often fails to consider the alignment of their proposed solutions with current privacy regulations, impeding their practical implementation in real-world scenarios.

Keywords: Privacy · Social Network · Privacy Mechanisms · Children

1 Introduction

Safeguarding children's privacy is paramount due to risks like inappropriate data collection, targeted advertising, and suspicious online interactions. According to a report [7], nearly a quarter of major social media users began using these networks in early childhood, even before reaching 6 years old. Notwithstanding, $\approx 90\%$ of the people aged from 9 to 17 actively maintain a profile on digital platforms. Consequently, the growing presence of children in the digital realm exposes them to the collection of personal and sensitive information, prompting considerable concerns regarding their security and privacy [10].

Over the past years, numerous laws have been enacted to safeguard personal data and ensure the protection of children. Examples include the General Data Protection Regulation (GDPR) in Europe and the General Data Protection Law (LGPD) in Brazil, which primarily focuses on personal data protection. Similarly, the Children's Online Privacy Act (COPPA) was specifically established in the United States to protect children's data [30]. In this context, the technological evolution of social networks poses several challenges in ensuring user privacy, necessitating ongoing regulatory adjustments.

Children's privacy holds significant relevance, given the escalating use of online technologies and mobile devices among minors in recent years [28]. While

this surge in children's engagement with the technological landscape has led to the routine collection and processing of data by service providers, it has concurrently exposed this group to substantial privacy risks [11]. Children can be considered vulnerable subjects due to various factors. Their vulnerability is underscored by inherent physical and psychological fragility and a limited capacity to make autonomous decisions. Special rights have been internationally and nationally acknowledged to address this vulnerable status, specifically tailored for this demographic group [1].

However, despite the existence of current regulations addressing the privacy of minors, there remains a lack of a clear definition regarding the concept of minors, whether considering the user's age or their mental capabilities. Childhood encompasses the stage of human development from birth to adolescence, marked by universally recognized characteristics like fragility and the need for special attention and care over a substantial period [22]. At the regulatory level, the Child and Adolescent Statute defines a child as a person up to the age of 12, while adolescents are those between twelve and eighteen years old, providing clarity on specific age groups. Conversely, it is noteworthy that LGPD, COPPA, and GDPR do not provide a unanimous definition of minors concerning privacy issues, leaving room for legal interpretations. The lack of a precise legal definition for the concept of minors contributes to the absence of unified and universal definitions in the realm of children's privacy on social networks [26]. Despite regulations mandating parental consent for minors to use social networks and data collection, service providers often neglect to implement compliance mechanisms. These may include measures such as photo verification of official documents, biometrics, or more robust security questions tailored to minors [20].

The absence of standardization poses challenges for global service providers, requiring them to navigate diverse regulations based on users' locations. This variability directly affects the uniform protection of children's data, as the security measures are contingent on each country's specific regulations and practices. Additionally, this lack of standardization gives rise to complications in adhering to laws, implementing specific processes, and incorporating security mechanisms to ensure compliance with the distinct legal requirements of each country. There is a scarcity of literature examining data privacy on social networks used by minors. This gap arises from the diverse nature of social media platforms, each with unique architecture, posing a challenge to unify and assess the implemented mechanisms [14]. Consequently, there is limited evidence regarding the protective mechanisms adopted by websites and applications for children, making it challenging to establish the effectiveness of existing laws. In practice, service providers often exploit legislation's lack of precise privacy definitions and the ambiguity in defining minors. Additionally, the widespread lack of transparency on many social networks hinders a proper understanding of their policies, data collection practices, and the implementation of security and privacy mechanisms [19].

In response to this gap, this paper undertakes an in-depth review of the scientific literature concerning implemented privacy mechanisms for minors to

safeguard their privacy on social networks. We commence with a comprehensive review of current legal regulations governing the privacy of minors on social networks. Subsequently, we present a literature review focusing on the mechanisms in place to safeguard the privacy of minors on social networks.

2 Data Privacy Regulations

The imperative for personal data protection has gained prominence by enacting judicial decisions in numerous countries. Multiple data protection laws have been implemented by sharing the idea that personal data warrants distinctive legal protection. From a legal standpoint, discussions about the right to privacy ensued due to new techniques and technological tools, enabling access and disclosure of information related to an individual's private sphere. Its primary focus is to protect the data holder rather than the data itself. Consequently, any breach of an individual's personal information jeopardizes their security and integrity [10]. Data privacy involves adherence to established norms governing the collection, disclosure, and use of information, encompassing elements such as name, age, sexual orientation, race, and religious and philosophical beliefs.

Modern endeavors by numerous countries strive to safeguard privacy rights in the digital realm, leading to the continual evolution of regulations on the subject [12]. Examples of these regulations on a global scale include the General Data Protection Law (LGPD) in Brazil, the Personal and Electronic Information Privacy Act (PIPEDA) in Canada, the California Consumer Privacy Act (CCPA) in California, the APPI Amendment of 2017 (APPI) in Japan, and the General Data Protection Regulation (GDPR) in the European Union. The subsequent subsections will explore privacy-related laws relevant to this work, specifically GDPR, LGPD, and COPPA.

2.1 General Data Protection Regulation (GDPR)

The GDPR is legislation within the European Union that became effective in 2018, aiming to establish regulations for processing personal data. Broadly, the GDPR is designed to support individuals with greater control over their data more responsibly and transparently. It sets a standard that has influenced the approach of numerous countries worldwide.

Concerning data processing, the GDPR includes the need for specific regulatory provisions for children. More specifically, it states that children warrant special protection concerning their data due to their limited awareness of associated risks and rights. This safeguarding, especially relevant in marketing, profiling, and direct service usage, should not necessitate parental consent for preventive or counseling services directly provided to the child.

The GDPR also delineates conditions for obtaining children's consent in the context of digital services, emphasizing key aspects of data processing, such as:

- *Minimum age for consent.* Establishes a minimum age of 16 for consent, requiring parental or guardian consent for processing data of children under such age.

- *Parental consent*. Stipulates that data processing is lawful only with parental consent, necessitating the controller to verify consent diligently, leveraging available technology.
- *Clear information for children*. Data controllers are mandated to furnish children with clear and accessible information regarding the processing of their data.

Therefore, while the GDPR does not feature a dedicated section on children's data protection, it comprehensively addresses the topic, encompassing crucial provisions such as minimum age and parental consent. Notably, specific data privacy laws may exist in some European Union states.

2.2 General Data Protection Law (LGPD)

The LGPD is a Brazilian legislation that safeguards citizens' data privacy by establishing regulations for collecting, storing, processing, and sharing personal information. Specifically addressing children's privacy, it emphasizes processing data in the "*best interests of the minor*," aligning with the protective system for children and adolescents.

Initially, concerns arose about the necessity of parental consent for data processing. However, a statement by the National Data Protection Authority (ANPD) clarified that data processing for children and adolescents is permissible under any legal scenario outlined in the LGPD, as long as the child's interests are respected. The law outlines the importance of special measures to ensure children's privacy and data security, acknowledging their vulnerability. However, the shift away from requiring parental consent for data processing is viewed by some as a regressive step, potentially easing the responsibilities of data controllers [7].

The law also outlines requirements for processing children's data. Notably, it mandates that information on data processing must be presented in a simple, clear, and accessible manner, incorporating audiovisual resources when appropriate. This approach aims to provide necessary information for parents or legal guardians and ensure comprehension by the child, discouraging complex language and technical terms. The use of drawings, diagrams, flowcharts, videos, and other resources is recommended to enhance accessibility for both children and guardians.

2.3 Children's Online Privacy Protection (COPPA)

COPPA is a U.S. legislation overseen by the Federal Trade Commission, established to safeguard the online privacy of children under the age of 13. Enacted in 1998 in response to concerns about collecting children's personal information on online platforms, COPPA applies to websites and online services directed at children. The Act mandates that websites and services targeting children must obtain parental consent before collecting and using personal information. The legislation is structured into sections covering Definitions, General Requirements for the Protection of Children's Privacy, Prohibitions, Administration and

Table 1: Regulatory overview on privacy aspects for the child.

Privacy Aspect	**LGPD**	**GDPR**	**COPPA**
Definition of personal data	✓	✓	
Definition of child	$\leq$ 12 y/o	$\leq$ 16 y/o	$\leq$ 13 y/o
Consent of parents or guardians	✓	✓	✓
Transparency of the use of information	✓	✓	✓
Limited Purpose	✓	✓	✓
Data Minimization	✓	✓	
Data collection without parental consent	✓	✓	✓
Data processing notice	✓	✓	✓
Right to Review the provided data	✓	✓	✓
Privacy-Oriented Design	✓	✓	
Confidentiality of Collected Information	✓	✓	✓

Enforcement, Civil Sanctions, Regulations and Procedures, and Studies and Reports.

It establishes the core provisions, including the obligation for websites to notify parents and secure verifiable parental consent before collecting, using, and disclosing information from children under 13. Websites are also required to secure the information collected from children and give parents the right to review the data. It also features prohibitions on certain practices, details the role of the Federal Trade Commission, and specifies penalties for violations.

2.4 Discussion

The absence of adequate protection for sensitive data leaves room for potential abuse, including the misuse of information for monitoring, manipulation, and harm to children, posing both short and long-term risks. Moreover, there is an observed deficiency in legal frameworks as they often fail to consider the risks to children associated with profiling sufficiently.

Table 1 shows the regulatory overview on privacy aspects for children. It is possible to note a lack of consensus on child privacy, even deviating from the regulatory definition of minor's age. This gap may stem from legislators not fully comprehending the specific risks to children, resulting in legislation that may not be promptly updated to address emerging concerns effectively.

3 Privacy on Social Networks

General data protection laws primarily concentrate on safeguarding broad rights, often neglecting the specific implications for children [8]. For instance, consent

requirements, privacy policies, and security measures are frequently not tailored for the child audience. Another challenge pertains to defining the *age of consent* (see Table 1). Establishing an accurate age for consent and comprehending its implications is complex, as it may vary for legal, cultural, and social reasons. This intricacy adds a layer of difficulty to addressing children's specific needs and considerations within the framework of data protection laws.

A pressing challenge involves constantly adapting laws in response to technological advances. The rapid growth of artificial intelligence, for instance, raises questions about safeguarding data in environments where autonomous algorithms process information in complex and often opaque ways. Establishing clear boundaries for the ethical and responsible use of data in such contexts presents a challenging task for policymakers and regulators.

The next subsections further explore the current literature on privacy mechanisms proposed for social networks.

3.1 Privacy on Social Networks

Social networks have become integral to the daily lives of millions worldwide, serving as a platform for connection, information sharing, and interaction. Notably, their utility extends beyond entertainment; companies analyze trends for personalized marketing, employers scrutinize candidate profiles, and the judiciary leverages social networks for crime-solving evidence. Social media even plays a role in influencing election outcomes [13]. This highlights that social networks accumulate diverse and comprehensive information, such as Facebook containing personal life details and LinkedIn featuring professional activities, enabling the creation of detailed individual profiles [18]. Nevertheless, the digital environment raises substantial privacy concerns, and the primary challenge in privacy solutions lies in balancing between preserving user privacy and not impeding the advantages of socializing and information sharing.

One of the main privacy problems is information leakage, which comes from users who put themselves at risk by interacting or disclosing their personal information. Still, leaks can also occur through third-party applications linked to social media accounts or even due to vulnerabilities in services provided by the social network. These information displays are of interest to different audiences, such as: (a) *Data Brokers*: sell personal information to other parties, such as banks, insurance companies, etc.; (b) *Service providers*: offer targeted services and advertisements; (c) *Criminals*: carry out social engineering, spear phishing or recovery of authentication techniques;

Concerning native privacy features, social networks usually allow users to limit access to their information, leaving it visible only to friends, for example. A user can create an account without explicitly revealing any information. This allows the user to leave their information public and/or private. However, there are privacy-related attacks that aim to infer user attributes that are incomplete or missing [10]. Several works in the literature explore attribute inference in social networks. These works can be classified into two main categories: friend-based inference and behavior-based inference [5].

Friend-based inference techniques leverage the homophily theory, positing that two friends are likelier to share the same attributes than two strangers. For instance, if most of an individual's friends on a social network are enrolled at a given university, it is plausible to infer that this individual is also a student at that university. Several studies have utilized machine learning techniques to validate this theory [24] [23]. Conversely, the behavior-based inference technique utilizes the user's and similar friends' public attributes. Weinsberg *et al.* [30] proposed a method for identifying user attributes, including gender, based on the list of liked films.

In this context, having fine-grained privacy settings is essential for users to have flexibility in controlling the exposure of their information. However, this fine granularity may demand a significant cognitive effort from users, leading them to ignore and trust only default privacy settings. Therefore, several authors have proposed techniques for fine-grained privacy controls. Kruk *et al.* [14] introduced an ontology-based access control mechanism that utilizes relationships between users. This proposal employs a generic definition of relationships ("*knows*") as a trust metric. It generates rules to control a friend's access to resources based on the degree of interaction in the social network [3]. Choi *et al.* [2] advanced Kruk's work with a more refined approach, considering more granular relationships (e.g., "*worksWith*", "*isFriendOf*", "*knows*") to model the social network and access control.

Fong *et al.* [8] introduces a Role and Relationship-Based Access Control (ReBAC) model that treats relationships as polyrelational (e.g., distinguishing teacher-student relationships from parent-child relationships) and directed (e.g., distinguishing teacher-student relationships from student-teacher relationships). This model maps multiple access contexts organized in a tree-like hierarchy. When access is requested in a context, relationships from all ancestral contexts are combined with relationships in the target access context to construct a network for making authorization decisions.

Research indicates that users on social networks frequently neglect available privacy controls. For instance, over 99% of Twitter users maintain the default privacy setting, exposing their name, follower list, location, website, and biographical information. Similarly, most Facebook users retain default settings [13]. The underutilization of privacy options is primarily attributed to a non-intuitive privacy setting interface, complex privacy settings, and an inherent trust in social media.

To enhance user engagement in configuring privacy settings, providing an appropriate graphical interface that facilitates understanding and reduces configuration time is crucial. Several studies have aimed to develop such interfaces. For instance, Paul *et al.* [19] introduced Colors for Privacy Settings (C4PS), employing colors to represent different visibility levels of attributes. For example: (red) signifies visibility to no one; (blue) indicates visibility to selected friends; (yellow) denotes visibility to all friends; (gray) represents visibility to anyone. This allows users to choose the color for each attribute.

The challenge with not changing default settings is that they often tend to be more open than users would prefer [13]. Approaches have been proposed to address this issue by automatically generating more suitable default privacy settings. PriMA [28] proposed a privacy preference generator based on user profiles similar to the account owner. The PolicyMgr [26] approach employed supervised machine learning with examples of privacy policies to build classifiers that automatically generate privacy policies [6].

3.2 Child Privacy

Many children are growing up in a "*digital-by-default*" world, where technologies mediate interpersonal, institutional, and commercial interactions. Online interactions enable children to connect, communicate, interact, and play comfortably [15]. Privacy is crucial in supporting children's autonomy, contributing to their psychosocial development, responsibility, resilience, confidence, and critical thinking skills. Societies worldwide increasingly recognize the importance of children's privacy and safety, given that privacy violations in the digital realm can manifest in various ways. Technologies can monitor children's physical location, store their personal information and preferences, and even influence their decision-making [25].

Daniel J. Solove [27] developed a taxonomy of privacy issues, encompassing 16 privacy concerns organized into four categories: information collection, information processing, information disclosure, and intrusions. Information collection involves surveillance and monitoring, encompassing obtaining information from children in problematic ways. Information processing is associated with storing, manipulating, and using information, including aggregating information for purposes other than those initially agreed upon. Information disclosure pertains to breaches of confidentiality involving the inappropriate disclosure of information that may harm a person's reputation. Finally, invasion occurs when someone intrudes upon another person's physical, psychological, or digital space or interferes with another person's decision-making.

Eva *et al.* [25] investigated children's perceptions of privacy. The research involved 25 children aged between 10 and 11 years who participated in a workshop with tests assessing various aspects, including (1) online activities of children; (2) understanding of personal information by children; (3) types of personal information requested by applications and games; (4) acceptable online behaviors according to children; (5) risks and concerns they have in the online environment. Overall, the tests revealed that children's understanding of privacy revolves around avoiding strangers and considering their home addresses as the most confidential information. This highlights the need for efforts to increase awareness of privacy among children. Several organizations have developed materials on educating children about privacy, which are being incorporated into school curricula [1].

In developing educational materials for children, there is no consensus on whether children should participate in creating these materials. However, approaches involving games or stories are more effective [15]. For instance, Raynes

et al. [20] created a game called "*The Vigilantes*," aiding children in understanding information collection and its applications. Similarly, the storybook "*Superheroes*" narrates the tale of a superhero imparting lessons on personal information, online chatting, location sharing, and cyberbullying.

Apart from raising children's awareness, applications, games, websites, and social networks must comply with laws such as COPPA, GDPR, and LGPD. However, the current scenario indicates that many platforms do not adhere to legal provisions. The American Federal Trade Commission (FTC) [1] highlights misleading transparency regarding mobile application privacy, providing parents with minimal or no privacy information. An FTC study revealed that parents often struggle to determine, before downloading an app, whether it poses risks related to collecting, using, and sharing their children's personal information.

Similarly, Ilaria *et al.* [16] demonstrates that although cell phone applications are aimed at children, several applications request sensitive permissions that are inappropriate and/or expected [9]. This is critical for understanding potential legal compliance violations, as it is difficult to be clear about what information is collected and/or used. Additionally, even if an application is inactive, there is no guarantee that the application is not collecting personal information. Developer companies make free or paid applications available in stores, with the latter earning revenue through advertising, while the paid version does not. It is often more profitable for companies to have a free application with advertising than a paid one due to targeted advertising using the collected data [29].

3.3 Child Privacy on Social Networks

Children's privacy on social networks remains a contentious issue, especially since many platforms, including Facebook, explicitly prohibit usage by children in their terms of service. However, research revealed that millions of children under 13 use Facebook, often providing false information about their age during registration [13]. This underscores that social networks are frequently not designed with children's best interests. Platforms such as Instagram and Twitter default to keeping new account profiles public. Additionally, children may not fully comprehend that agreeing to access a social network entails consenting to collecting and sharing their personal information, including their location.

The effectiveness of identity verification systems in most social networks and online services is compromised as they rely on remote verification, easily circumvented by users. Many parents prioritize age restrictions on social networks to filter inappropriate content for their children, often overlooking privacy risks. COPPA designates the age of 13 as a pivotal point in a child's life, emphasizing their capacity for decision-making. Studies suggest that, before the age of 11, children tend to be less critical in evaluating the trustworthiness of online content [15]. For instance, an investigation involving 135 children aged 8 to 10 found that a website's dynamic features (such as animations) influenced trust perceptions, with children rating a website with animated dog images as more trustworthy than a text-only version. While children aged 8 and above can iden-

Table 2: Literature overview on privacy for children on social networks.

Work	Child Privacy	Social Net. Privacy	Legal Aspects	Eval. Conf.	New Solution
Ghazaleh and Huan [5]		✓		✓	✓
Kruk *et al.* [14]		✓		✓	✓
Choi *et al.* [2]		✓		✓	✓
Fong [8]		✓		✓	✓
Kayes and Iamnitchi [13]		✓		✓	✓
Paul *et al.* [19]		✓		✓	✓
PriMA [28]		✓		✓	✓
Shehab *et al.* [26]		✓		✓	✓
Daniel J. Solove [27]	✓				✓
Eva *et al.* [25]	✓	✓	✓	✓	
Raynes [20]	✓	✓	✓		✓
FTC [1]	✓	✓	✓	✓	
Liu *et al.* [17]	✓		✓	✓	✓
Irwin *et al.* [21]	✓		✓	✓	✓
Alkhalifah *et al.* [4]	✓	✓			✓
Rochelau and Sonia [22]	✓	✓			✓

tify the selling intent in advertisements, they struggle to perceive persuasive intentions at this age [21].

3.4 Discussion

Table 2 presents the literature overview on privacy for children on social networks The observation underscores a critical gap in the current literature on children's privacy within social networks. Despite the proliferation of literature proposing innovative privacy solutions, a significant oversight is apparent in adequately addressing the legal dimensions of these proposals, particularly concerning minors. The prevailing regulatory mechanisms may not align with the proposed solutions, potentially rendering them impractical or non-compliant. This misalignment highlights a fundamental challenge where theoretical advancements in privacy protection for children on social networks face barriers in translating into effective, legally sound practices. Bridging this gap between theoretical innovation and regulatory reality is crucial for ensuring that proposed privacy measures are visionary and grounded in the legal frameworks that govern the online space for minors.

4 Conclusion

Children's privacy on social networks poses a multifaceted challenge in the ever-evolving digital landscape. As minors increasingly engage with online platforms, there is a pressing need to navigate the complex interplay between legal regulations, evolving norms, and the practical efficacy of existing privacy mechanisms. This paper thoroughly explores the scientific literature, delving into the mechanisms to safeguard children's privacy on social networks. The review showed a critical issue as most existing works often neglect to adequately address the legal dimensions of children's privacy, especially in social networks. This presents a notable gap, hindering the practical applicability of proposed privacy solutions within the constraints of current regulatory frameworks.

References

1. Federal trade commision study (2024), https://www.ftc.gov/
2. 14. H.C. Choi, S.R. Kruk, S.G.K.S.B.D.J.B.: Trust models for community aware identity management. Proceedings of the 2006 Identity, Reference and Web Workshop, in Conjunction with WWW **1**, 140–154 (2006)
3. Abreu, V., Santin, A.O., Viegas, E.K., Stihler, M.: A multi-domain role activation model. In: IEEE International Conference on Communications (ICC). IEEE (2017)
4. Alkhalifah, A., Alghafis, A.: The effect of privacy concerns on children's behavior on the internet: an empirical study from the parents' perspective (2022)
5. Beigi, G., Liu, H.: A survey on privacy in social media: Identification, mitigation, and applications. ACM/IMS Transactions on Data Science **1**(1), 1–38 (Feb 2020)
6. Bulle, B.B., Santin, A.O., Viegas, E.K., dos Santos, R.R.: A host-based intrusion detection model based on os diversity for scada. In: IECON 2020 Annual Conference of the IEEE Industrial Electronics Society. IEEE (Oct 2020)
7. Cetic.br: Tic kids online brasil. Tech. rep. (2023), https://cetic.br/pt/pesquisa/kids-online/
8. Fong, P.W.: Relationship-based access control: protection model and policy language. In: Proceedings of the first ACM conference on Data and application security and privacy. CODASPY '11, ACM (Feb 2011)
9. Geremias, J., Viegas, E.K., Santin, A.O., Britto, A., Horchulhack, P.: Towards multi-view android malware detection through image-based deep learning. In: IEEE International Wireless Communications and Mobile Computing (IWCMC) (2022)
10. Gong, N.Z., Liu, B.: You are who you know and how you behave: Attribute inference attacks via users' social friends and behaviors. In: Proceedings of the 25th USENIX Conference on Security Symposium. p. 979–995. SEC'16, USENIX Association, USA (2016)
11. He, J., Chu, W.W., Liu, Z.V.: Inferring Privacy Information from Social Networks, p. 154–165. Springer Berlin Heidelberg (2006)
12. Horchulhack, P., Viegas, E.K., Santin, A.O., Ramos, F.V., Tedeschi, P.: Detection of quality of service degradation on multi-tenant containerized services. Journal of Network and Computer Applications **224**, 103839 (Apr 2024)
13. Kayes, I., Iamnitchi, A.: Privacy and security in online social networks: A survey. Online Social Networks and Media **3–4**, 1–21 (2017)

14. Kruk, S.: Foam-realm: control your friends access to the resource. Proceedings of the First Workshop on Friend of a Friend **1** (2004)
15. Kumar, P.C., O'Connell, F., Li, L., Byrne, V.L., Chetty, M., Clegg, T.L., Vitak, J.: Understanding research related to designing for children's privacy and security: A document analysis. In: Proceedings of the 22nd Annual ACM Interaction Design and Children Conference. IDC '23, ACM (Jun 2023)
16. Liccardi, I., Pato, J., Weitzner, D.J.: Improving user choice through better mobile apps transparency and permissions analysis. Journal of Privacy and Confidentiality **5**(2) (Feb 2014)
17. Liu, M., Wang, H., Guo, Y., Hong, J.: Identifying and analyzing the privacy of apps for kids. In: Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications. HotMobile '16, ACM (Feb 2016)
18. Nissenbaum, H.: A contextual approach to privacy online. Daedalus **140**(4), 32–48 (Oct 2011)
19. Paul, T., Stopczynski, M., Puscher, D., Volkamer, M., Strufe, T.: C4PS - Helping Facebookers Manage Their Privacy Settings, p. 188–201. Springer (2012)
20. Raynes-Goldie, K., Allen, M.: Gaming privacy: a canadian case study of a children's co-created privacy literacy game. Surveillance Society **12**(3), 414–426 (Jun 2014)
21. Reyes, I., Wiesekera, P., Razaghpanah, A., Joel Reardon, N.V.R., Egelman, S., Kreibich, C.: is our children's apps learning?" automatically detecting COPPA violations (2017)
22. Rocheleau, J.N., Chiasson, S.: Privacy and safety on social networking sites: Autistic and non-autistic teenagers' attitudes and behaviors. ACM Transactions on Computer-Human Interaction **29**(1), 1–39 (Jan 2022)
23. dos Santos, R.R., Viegas, E.K., Santin, A.O., Tedeschi, P.: Federated learning for reliable model updates in network-based intrusion detection. Computers amp; Security **133**, 103413 (Oct 2023)
24. Santos, R.R.d., Viegas, E.K., Santin, A.O., Cogo, V.V.: Reinforcement learning for intrusion detection: More model longness and fewer updates. IEEE Transactions on Network and Service Management **20**(2), 2040–2055 (Jun 2023)
25. Schomakers, E.M., Biermann, H., Ziefle, M.: Users' preferences for smart home automation – investigating aspects of privacy and trust. Telematics and Informatics **64**, 101689 (Nov 2021)
26. Shehab, M., Cheek, G., Touati, H., Squicciarini, A.C., Cheng, P.C.: User centric policy management in online social networks. In: 2010 IEEE International Symposium on Policies for Distributed Systems and Networks. IEEE (2010)
27. Solove, D.J.: Understanding Privacy (2022)
28. Squicciarini, A.C., Paci, F., Sundareswaran, S.: Prima: a comprehensive approach to privacy protection in social network sites. Annals of Telecommunications **69**(1–2), 21–36 (Jun 2013)
29. Techcrunch: How free apps can make more money than paid apps. Tech. rep. (2012), https://techcrunch.com/2012/08/26/how-free-apps-can-make-more-money-than-paid-apps/
30. Weinsberg, U., Bhagat, S., Ioannidis, S., Taft, N.: Blurme: inferring and obfuscating user gender based on ratings. In: Proceedings of the sixth ACM conference on Recommender systems. RecSys '12, ACM (Sep 2012)