IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Protecting Children's Privacy In The Digital Age: Balancing Legal Frameworks, Parental Consent, And Online Commerce

Dr shashank misra

Principal

Dewan Law College

Abstract: Emphasizing the legal systems and regulations controlling the acquisition, use, and distribution of children's data, this paper investigates the evolving dynamics of children's privacy in the digital age. Emphasizing the challenges in balancing the protection of children's rights with the demands of online commerce, this study investigates the consequences of international legal frameworks including the EU General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA) in the United States as well as various national legislation. Particular focus is on the nuances of parental consent, the definition of age criterion for agreement, and the growing concerns about online behavioural advertising targeted at minors. Emphasising parental assent and the age of majority, the growing legislative frameworks—best shown by the Digital Personal Data Protection Act in India—recognize the need of flexibility in the treatment of children's data. Particularly with age limitations and content moderation, this study systematically examines the complex balance between protecting children's rights and enabling safe digital engagement. The paper discusses the need of openness, privacy by design, and data protection impact assessments in the safeguarding of personal data of children. It supports a more complex and flexible approach for data protection that considers children's evolving cognitive and developmental capacities as well as their rights to privacy and freedom of expression against too invasive intrusion. Emphasizing their practical relevance and the impact of future technologies on children's online experiences, it finally assesses the effectiveness of present regulatory systems in providing enough protection.

Keywords: Children's privacy, data protection, GDPR, COPPA, parental consent, online advertising, privacy by design, legal frameworks.

1. Introduction

Approved by the 30th International Conference of Data Protection and Privacy Commissioners on October 17, 2008, the Strasbourg Resolution addresses concerns regarding the massive gathering of personal data from minors in digital environments. Particularly with relation to micro-targeting and behavioral advertising, the Commissioners underlined the need for regulations limiting the acquisition, use, and distribution of personal data for children.[1] To help children understand and consent on data harvesting, they

[1] 30th International Conference of Data Protection and Privacy Commissioners, *Resolution on Children's Online Privacy* (Strasbourg, Oct. 17, 2008), ¶ 2.

also urged companies to create succinct and straightforward privacy policies and user agreements.[2] They also supported the development of educational tools to help children safely negotiate the internet and protect their privacy. The Resolution underlines three main reasons why children's internet privacy calls for special attention. Given their age and inexperience, children are more sensitive than adults.[3] They often lack the tools or technological knowledge needed to handle the privacy risks connected to online behavior, including photo sharing, messaging, and blogging. Second, digital footprints left by children can be more negative than those of adults. Children's immaturity makes them more prone to make mistakes online, which leads to lifelong records that could later cause shame or difficulty to clarify as they grow. Protecting children's privacy means stopping the production of negative or permanent digital content that might damage their security, dignity, or privacy.[4] Third, the United Nations Convention on the Rights of the Child (CRC) defines children's private rights by mandating that governments respect and protect these rights.[5]

The CRC is important since it imposes clear responsibilities for governments over children's rights.[6] The CRC emphasizes the need of increased care and attention for children since it recognizes their particular position inside the larger framework of human rights laws protecting personal privacy.[7] The basic concept guiding laws affecting minors should be the "best interests of the child." Legislators have thus to ensure that every rule advances the welfare of children. The "3 Ps"—provision, protection, and participation—regulates children's rights under the CRC.[8] These covers ensure a suitable media environment, protecting children from inappropriate internet activities.[9], and making sure they can make decisions influencing their own life.[10] Still, children's growing maturity calls for parents to be very important in guiding their decision-making process.[11] This paper looks at how certain countries have addressed children's privacy concerns. At first, the book looks at the rise of children's privacy as a major issue of worry for Americans, particularly with the Children's Online Privacy Protection Act (COPPA).[12] The paper compares the American approach with that of Canada and Australia, where general data protection policies have been applied to protect children's privacy.[13] The study looks at how Europe's commitment to privacy as a basic human and children's right has affected both current and new legislation, most famously the General Data Protection Regulation (GDPR), from broad privacy protections to targeted rules for children.

2. The Emergence of Children's Online Privacy as A Trade Issue In The United States, Canada And Australia

Although both governmental and commercial institutions were compiling personal information about minors, there was no clear reference to children's privacy in the 1970s when data protection laws were first passed in Europe and North America.[14] Children's medical visits and school attendance, for instance, produced comprehensive records that followed them all their life.[15] Collected demographic data on

[2] *Id.* ¶ 12. See also 38th International Conference of Data Protection and Privacy Commissioners, *Resolution for the Adoption of an International Competency Framework on Privacy Education* (Marrakesh, Oct. 18, 2016).
[3] *Id.* ¶ 5.
[4] *Id.* ¶ 8.
[5] Convention on the Rights of the Child, Nov. 20, 1989, U.N. Treaty Series, 1577, art. 5.
[6] *Id.* art. 5.
[7] *Id.* ¶¶ 6–7.
[8] See, e.g., Universal Declaration of Human Rights, art. 12, Dec. 10, 1948, G.A. Res. 217A (III).Id. art. 17. See also Valerie Steeves, *Snoops, Bullies and Hucksters: What Rights Do Young People Have in a Networked Environment?* in N.A. Jennings & S.R. Mazzarella (eds.), *20 Questions About Youth and Media* (2d ed., New York: Peter Lang, 2017).
[9] *Id*. art. 3(2).
[10] CRC, supra note 5, arts. 17, 31.
[11] CRC, supra note 5, Preamble.
[12] *Id.* art. 3(1).
[13] Ann Quennerstedt, *Children, But Not Really Humans? Critical Reflections on the Hampering Effect of the "3 P's"*, 18 INT'L J. CHILD. RIGHTS 619 (2010).
CRC, supra note 5, arts. 16–17.
[14] Valerie Steeves, *It's Not Child's Play: The Online Invasion of Children's Privacy*, 3 U.O.L.T.J. 169 (2006); Sara M. Grimes & Leslie Regan Shade, *Neopian Economics of Play: Children's Cyberpets and Online Communities as Immersive Advertising in Neopets.com*, 1 INT'L J. MEDIA & CULTURAL POL. 181 (2005); Kathryn Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (2007) MIT Press; Kathryn Montgomery, *Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications*, 39 TELECOMM. POL'Y 771 (2015).
[15] 15 U.S.C. §§ 6501–6506.

children's tastes in toys, games, and fashion, including warranty registration cards and magazine subscriptions, informed marketing plans.[16] Children and their parents eventually have access to data kept by public sector companies, particularly in the domains of health and education.[17] Generally, it was assumed that national general data protection laws would control the growing market for children's information.[18] The scene was transformed when the World Wide Web first emerged in the 1990s, as websites started the creation of online environments specifically targeted at luring children and encouraging them to provide personal information for profit.[19] Acting with the Children's Online Privacy Protection Act (COPPA) in 1998, the United States was the first jurisdiction to recognize this as a separate privacy issue.[20]

Legislation aimed at safeguarding children's privacy, COPPA mandates parental permission before the gathering, use, or disclosure of personal information from anybody under the age of 13. Like consumer protection laws, it functions as a business regulator under control by the Federal Trade Commission (FTC).[21] COPPA requires that owners of websites and other online services—including linked toys and mobile apps—distribute privacy notifications to let parents and children know of data collecting practices.[22] Parental permission for the gathering, use, and distribution of personal data is necessary for these services. Moreover, parents have the right to examine the data of their children; so, services have to uphold integrity, confidentiality, and security of the acquired data. To give parents control over the personal data gathered from their children online, COPPA stresses parental rights over those of the children.[23] COPPA includes thorough, risk-based requirements for obtaining parental permission. Services using children's data for internal purposes could employ a simpler permission process, such as an email to the parent followed by a confirmation step, sometimes called the "Email plus" method.[24] Services that let minors publicly reveal information, engage in behavioral advertising, or distribute personal data to other parties must follow stricter consent procedures. These could call for parents to send consent documentation by fax, email, mail, credit card number, or identify identification using official documentation or video conference.[25]

Third-party verification services could be used to maximize the process by lowering the volume of personally handled directly by the service provider.[26] Several strategies have been proposed, including facial recognition technology to verify that a consenting person is the child's parent and knowledge-based authentication—where users answer questions depending on "out-of-wallet" information.[27] Industry standards of behavior could specify how one gets parental permission.[28] COPPA has affected policies

[16] Under COPPA, children 13 and over can consent on their own behalf.
[17] Former Federal Trade Commission Chairman Jon Leibowitz stated: "Let's be clear about one thing: under this rule, advertisers and even ad networks can continue to advertise, even on sites directed to children. Business models that depend on advertising will continue to thrive. The only limit we place is on behavioral advertising, and in this regard our rule is simple: until and unless you get parental consent, you may not track children to build massive profiles for behavioral advertising purposes. Period." Quoted in Katy Vachman, *FTC Restricts Behavioural Targeting of Kids: New Rules Go Into Effect Next July*, ADWEEK (Dec. 19, 2012), http://www.adweek.com/digital/ftc-restricts-behavioral-targeting-kids-146108/ (accessed Jan. 10, 2019).
[18] United States Electronic Code of Federal Regulations, Title 16, Chapter 1, Subchapter C, Part 312, § 6502(b)(1)(A).
[19] *Id.* § 312.5.
[20] *Id.* § 6502(b)(1)(B).
[21] *Id.* § 6502(b)(1)(D).
[22] Fed. Trade Comm'n, *Complying with COPPA: Frequently Asked Questions* (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions (accessed Jan. 10, 2019).
[23] Fed. Trade Comm'n, *Imperium, LLC Proposed Verifiable Parental Consent Method Application* (FTC Matter No. P135419) (Dec. 23, 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf (accessed Jan. 10, 2019).
[24] Fed. Trade Comm'n, *Commission Letter Approving Application Filed by Jest8 Limited (Trading As Riyo) For Approval of A Proposed Verifiable Parental Consent Method Under the Children's Online Privacy Protection Rule* (Nov. 19, 2015), https://www.ftc.gov/public-statements/2015/11/commission-letter-approving-application-filed-jest8-limited-trading-riyo (accessed Jan. 10, 2019).
[25] Art. 40(2)(g).
[26] Valerie Steeves, *Terra Cognita: Surveillance of Young People's Favourite Websites*, in Tonya Rooney & Emmeline Taylor (eds.), *Surveillance Futures: Social and Ethical Implications of New Technologies of and Children and Young People* (Routledge 2016).
[27] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31-50.
[28] Industry Canada & Department of Justice, *Building Canada's Information Economy and Society: The Protection of Personal Information* (White Paper, C (2nd series), 1998).

worldwide mostly because of the great popularity of American websites among children all over.[29] Many services targeted at children have adopted the age-based COPPA model, which requires parental consent only for those under 13, even in areas without age specificity of the law. Data security policies in many other countries have been shaped by the corporate interests driving COPPA.[30] Australia and Canada are shining examples of how non-American countries have handled similar problems. Both countries have thorough personal data protection laws combining federal, state, provincial, and territorial limitations. Initially, data protection laws from the 1980s have controlled public sector data harvesting in Canada.[31] Until after the 1995 changes to EU laws, which restricted cross-border data flows to countries without sufficient data protection, Canada concentrated on private sector data protection. Private sector legislation was seen as an economic necessity to boost consumer confidence in the growing information economy.[32] The main federal law in Canada controlling the compilation of personal data by private sector companies is the Personal Information and Protection of Electronic Documents Act (PIPEDA).[33] It applies everywhere unless a province or territory passes similar laws. Through the Australian Privacy Principles, the Federal Privacy Act 1988 controls public and private sectors including credit reporting agencies in Australia.[34]

Still, neither of these models addresses minors as data subjects nor sets an age at which they can consent to have their data processed. Children lack the legal capacity to make decisions about their personal information until they reach adulthood or are recognized as mature minors, so complicating enforcement.[35] Establishing an unofficial standard, the Children's Online Privacy Protection Act (COPPA) in the United States requires most services aimed at minors under 13 years of age to gain parental clearance. Privacy commissioners from Australia and Canada have aggressively tackled concerns related to children.[36] The Strasbourg Resolution was developed in great part by the Canadian Commissioner, and their rulings in the 2009 Facebook case and the 2013 Nexopia case were vital in applying broad data protection standards to limit the gathering of personal information on social networking sites. Similarly addressing children's privacy issues, the Australian Commissioner has provided clear recommendations on how to control children's authorization and has used legislative actions. Following the passage of COPPA in the United States, the debate over children's privacy in Australia started earnestly with the Privacy Amendment (Private Sector) Act in 2000. Introduced but rejected was a proposal to require parental permission for the gathering of personal data from minors under 13.[37] In 2001, a group on children's privacy was formed, yet it lacked clear results. Reviewing the Privacy Act 1988 years later, the Australian Law Reform Commission (ALRC) recommended changes to strengthen children and adolescent safety.[38] The ALRC suggested a consent model whereby individual evaluation would be combined with a presumption that those 15 years of age and above possessed the capacity to make decisions.[39] They understood that evaluating every child

[29] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.
[30] The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came into force on Mar. 12, 2014.
[31] See, e.g., Steeves, *Terra Cognita: Surveillance of Young People's Favourite Websites*, supra note 28.
[32] Privacy Commissioner of Canada Investigation, *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, PIPEDA Report of Findings #2009-008.
[33] Privacy Commissioner of Canada Investigation, *Social Networking Site for Youth, Nexopia, Breached Canadian Privacy Law*, PIPEDA Report of Findings #2012-001.
[34] See, e.g., Office of the Australian Information Commissioner (OAIC), *Proposed Changes to Facebook Data Use Policy and Statement of Rights and Responsibilities – OAIC Letter to Facebook* (Sept. 12, 2013), https://www.oaic.gov.au/media-and-speeches/statements/changes-to-facebooks-statement-of-rights-and-responsibilities-and-data-use-policy#proposed-changes-to-facebook-data-use-policy-and-statement-of-rights-and-responsibilities-oaic-letter-to-facebook (accessed Jan. 10, 2019); Statements on Facebook and Cambridge Analytica, *Investigation into Facebook Opened* (Apr. 5, 2018), https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica#investigation-into-facebook-opened (accessed Jan. 10, 2019).
[35] Commonwealth of Australia, Parliamentary Debates, Senate, Nov. 30, 2006, 20302 (N. Bolkus). The amendment was supported by the Australian Democrats: Commonwealth of Australia, Parliamentary Debates, Senate, Nov. 29, 2000, 20162 (N. Stott Despoja), 20165.
[36] D. Williams (Attorney-General), *First Meeting of Consultative Group on Children's Privacy* (Press Release, June 4, 2001), cited in Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol. 3, 2008) at 2254.
[37] Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol. 3, 2008).
[38] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines: Privacy Act 1988* (Mar. 31, 2015) at 12–13.
[39] *Id.*

individually—especially in online environments—may not always be feasible or practical.[40] As such, they recommended a broad assumption that those 15 years of age and above possessed the capacity to assent, unless there are specific grounds to doubt their understanding.[41] Later on, this model was included into the non-binding recommendations of the Australian Commissioner, which advise companies to assess every situation to determine whether parental or guardian permission is needed or if a kid can consent.

3. The European Union and The Human Rights Approach To Children's Online Privacy

Strong protections for privacy as a fundamental human right have molded EU privacy laws.[42] Many EU policy documents highlight the increasing attention paid to children's rights, particularly in the digital sphere.[43] The Charter of Fundamental Rights especially expresses the EU's will to protect children's rights.[44] Originally universal, privacy rules have evolved to recognize the unique circumstances of children's online privacy both inside the EU and globally.[45] Differentiating the treatment of children and adults about data privacy has both normative and pragmatic reasons.[46] From a normative standpoint, it is necessary to protect children's rights—more especially, their best interests—while preventing conflicts between the rights of adults and children using developing capacities and involvement.[47] Children come across increased online hazards according to empirical research because of complex data collecting techniques and their natural vulnerability as online users.[48] Studies in social science have revealed that children—especially teenagers—show more inclination for risk-taking and impulsive behavior, which could compromise their ability for autonomous long-term decision-making. Researchers have linked children's developmental needs—including identity building and autonomy—with their internet behavior and privacy decisions.[49] Online data-collecting techniques therefore often take advantage of these shortcomings, which causes concerns among academics and legislators both.[50] Unlike adults, these elements make youngsters more susceptible to internet damage, including victimizing and financial exploitation of their data. Children under the EU's general data protection rules of Directive 95/46/EC have been included since 1995, classed as a homogeneous group of data subjects with adults.[51] Regardless of age or nationality, this directive seeks to protect every person whose data is handled inside the EU.[52] Lack of clear legal guidelines on children's data across the EU has resulted in different state laws, therefore

[40] *Id.*
[41] *Id.*
[42] Besides a right to private life enshrined in art. 7, the Charter of Fundamental Rights of the European Union, [2000] O.J. C 364/1, recognizes the protection of personal data as a separate right under its art. 8.
[43] Commission (EC), *European Strategy for a Better Internet for Children*, COM/2012/0196 final (May 2, 2012); Commission (EC), *An EU Agenda for the Rights of the Child*, COM/2011/0060 final (Feb. 15, 2011).
[44] Charter of Fundamental Rights of the European Union, [2000] O.J. C 364/1, art. 24.
[45] Council of Europe, *Strategy for the Rights of the Child 2016-2021* (Mar. 2016); U.N. Committee on the Rights of the Child, *Digital Media and Children's Rights* (Report of the 2014 Day of General Discussion, May 2015); UNICEF, *Privacy, Protection of Personal Information and Reputation Rights* (Discussion Paper, 2017); UK Children's Commissioner, *Growing Up Digital: A Report of the Growing Up Digital Taskforce* (Jan. 2017); UK House of Lords Committee on Communications, *Growing Up with the Internet* (2nd Report of Session 2016–17, Mar. 2017).
[46] Simone van der Hof, *I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, 34(2) WIS. INT'L L.J. 409 (2017); Eva Lievens, *Children's Rights and Media: Imperfect But Inspirational*, in Eva Brems, Wouter Vandenhole & Ellen Desmet (eds.), *Children's Rights Law in the Global Human Rights Landscape: Isolation, Inspiration, Integration?* (Routledge 2017); Sonia Livingstone, *Children: A Special Case for Privacy?* 46(2) INTERMEDIA 18 (2008).
[47] Kirsty Hughes, *The Child's Right to Privacy and Article 8 European Convention on Human Rights*, in Michael Freeman (ed.), *Current Legal Issues: Law and Childhood Studies* Vol. 14 (Oxford University Press 2012).
[48] Cheryl B. Preston & Brandon T. Crowther, *Legal Osmosis: The Role of Brain Science in Protecting Adolescents*, 2014 HOFSTRA L. REV. 447.
[49] Jochen Peter & Patti M. Valkenburg, *Adolescents' Online Privacy: Toward a Developmental Perspective*, in Sabine Trepte & Leonard Reinecke (eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Springer 2011); Wouter M.P. Steijn & Anton Vedder, *Privacy under Construction: A Developmental Perspective on Privacy Perception*, 40(4) SCIENCE, TECH. & HUM. VALUES 615 (2015).
[50] Montgomery, *Youth and Surveillance in the Facebook Era*, supra note 16.
[51] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [1995] O.J. L 281, 31-50.
[52] *Id.* art. 4.

creating an inconsistent regulatory environment.[53] For children's permission regarding personal data processing, some EU countries—including Hungary, the Netherlands, and Spain—have set clear age limits. Except for vital information like the child's identification and address, which is required for getting parental authorization, Spain's Personal Data Protection Law restricts the gathering of data of minors' family members without approval.[54] Contract law clauses have been used by other countries to determine whether kids could be making decisions about their data.[55] In certain cases, children might consent to fundamental data processing operations if they can independently engage in basic legal actions free from parental approval.[56]

Most EU nations evaluate the matter separately considering factors like the child's best interests, maturity, understanding of the consequences of consent, and the type of the data involved.[57] The UK Information Commissioner's Office (ICO) says a child's competence to consent to data processing should determine comprehension rather than age.[58] Parental permission is required for children under twelve in the UK when services target them. Parental permission is needed in Belgium when a child cannot understand the consequences of consenting to data processing, particularly in circumstances involving sensitive data or when the processing does not benefit the child.[59] Many nations have lately granted special rights to children and their parents so that they may access and erase personal information.[60] Establishing the presumption that those aged 12 or above have the maturity to understand and exercise their rights, the UK Data Protection Act created policies to preserve data protection rights in Scotland. France granted kids the "right to be forgotten" in 2016 so they may quickly delete their internet personal information.[61] Moreover, minors 15 years of age and above in France can use their rights of access, rectification, and objection; they may also choose to prevent their parents from being informed or accessing their personal information.[62] Declaring that the child's right to privacy trumps freedom of expression and press freedom, some countries have put policies in place to protect children's data in non-criminal judicial processes and media reporting.

The different national approaches for children's data protection inside the EU led to uncertainty on the application of relevant laws. Services compiling children's data regularly ran against legal uncertainty and had to coordinate several legal systems.[63] Among European privacy experts, the subject of the age at which minors might agree to data processing has been dubbed "the million-euro question".[64] Non-binding rules published by several data protection agencies have helped to somewhat offset the lack of clear data protection laws for minors in many EU countries.[65] These rules comprise comprehensive recommendations for protecting children's online privacy. Moreover, particular authorities have sent parents and children booklets, articles, and websites. Comprising representatives from all EU data protection agencies, the Article 29 Working Party, an advisory body, published a view on children's data, particularly with relation

[53] Parental consent was required for the processing of personal data of children under the age of 14 in Spain (art. 13 of the Spanish Royal Decree 1720/2007 of 21 December) and 16 in the Netherlands (art. 5 of the Dutch Personal Data Protection Act [25 892] of 23 November 1999) and Hungary (s. 6[3] of the Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information).

[54] In many other EU countries, even without explicit provisions, no collection of data on family would be allowed from a minor as this, under the general data protection principles, would be considered excessive in relation to the purpose and unfair.

[55] See, e.g., Czech Republic and Portugal, *Global Privacy and Information Management Handbook* (Baker McKenzie, 2017).

[56] Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, WP 160 (Feb. 11, 2009).

[57] UK Information Commissioner's Office, *Personal Information Online* (Code of Practice, 2010).

[58] Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 Concerning the Protection of the Private Life of Minors on the Internet* (2002).

[59] *Id.*

[60] UK Data Protection Act 1998, § 66.

[61] Law No. 2016-1321 of Oct. 7, 2016 for a Digital Republic ("French Digital Law"), arts. 40, 58.

[62] *Id.*

[63] Italian Data Protection Code (Legislative Decree No. 196 of 30 June 2003) §§ 50, 52.5; Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities, [1998] O.J. 179, § 7.

[64] Giovanni Buttarelli, *The Children Faced with the Information Society* (Speech, 1st Euro-Ibero American Data Protection Seminar 'On Protection of Minors', Data Protection, Cartagena de Indias, May 26, 2009).

[65] Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 Concerning the Protection of the Private Life of Minors on the Internet*, supra note 60; Dutch Data Protection Authority, *Guidelines for the Publication of Personal Data on the Internet* (2007).

to educational institutions.[66] Using ideas from the Convention on the Rights of the Child (CRC), including the child's best interest, protection, care, participation, and emerging maturity, within the framework of data protection, this point of view highlighted a child rights perspective.[67] The Working Party looked at how the field of education may benefit from general data protection concepts—that is, data quality, fairness, validity, proportionality, and data subject rights.[68] The Working Party took a flexible approach to consent, suggesting instead of enforcing strict age limits for parental permission that the child's maturity and the complexity of data processing be assessed.[69] Children's data need more strict protection and care than that of adults, the Working Party underlined.[70]

4. The European Union General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) has made significant changes, particularly to meet the needs of minors as data subjects.[71] It especially acknowledges that, especially in online situations, kids need more protection than adults since they might not fully understand the dangers, consequences, and protections connected with the handling of their data (Recital 38).[72] For children, the GDPR creates a two-layered protection system.[73] The first tier consists of generic GDPR rules relevant to children's online behavior including the right to erasure, data portability, data protection by design and by default, and data protection impact assessments.[74] The second tier comprises particular rules for children, including restrictions on marketing and profiling, most famously the ban on automated decisions that significantly affect children (Article 8), and the need for parental agreement (Article 8).[75] Under the GDPR, the most important—though controversial—requirement is the parental permission duty. Article 8(1) GDPR permits personal data collecting and processing for minors under 16 only with parental permission or agreement.[76] The law lets EU Member States lower the age of consent to 13, therefore creating different national age regulations. This independence has led to differences inside the EU, which challenges companies providing cross-border services and compromises the expected GDPR harmonization.[77] Article 8 has not been implemented consistently and lacks empirical support. First attempts to follow US norms, including COPPA, ran against challenges and various age restrictions were recommended without any justification. Furthermore, the EU missed a chance to improve child protection in relevant legislation, such as the

[66] Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, WP 160 (Feb. 11, 2009).
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] Article 29 Working Party, *Opinion 02/2013 on Apps on Smart Devices*, WP 202 (Feb. 27, 2013); *Opinion 2/2010 on Online Behavioural Advertising*, WP 171 (June 22, 2010).
[71] 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), 2016 O.J. (L 119) 1–88.
[72] Milda Mačėnaitė, *From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation*, 19(5) NEW MEDIA & SOC'Y 765 (2017).
[73] The age thresholds indicated in national laws are the following: 13 in Belgium, Denmark, Estonia, Finland, Latvia, Poland, Portugal, Spain, Sweden, UK; 14 in Austria, Bulgaria, Cyprus; 15 in Czech Republic, France, Greece, Slovenia, and 16 in Croatia, Germany, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, Romania, Slovakia, the Netherlands. Please note that the chapter was drafted in 2018 and it does not take into account the latest legislative developments and guidelines adopted by the EU member states.
[74] Milda Mačėnaitė & Eleni Kosta, *Consent of Minors to Their Online Personal Data Processing in the EU: Following in US Footsteps?*, 26(2) INFO. & COMM. TECH. L. 146 (2017).
[75] Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), [2017] 2017/0003 (COD).
[76] Information Society Services are defined as services that are 'normally offered for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services'. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services (Text with EEA Relevance), [2015] O.J. (L 241) 1, art. 1.1(b).
[77] According to the Article 29 Working Party, in order to avoid the application of the parental consent requirement, an information society service provider should "make(s) it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans)." *Guidelines on Consent under Regulation 2016/679*, WP 259, 25 (Apr. 10, 2018).

proposed ePrivacy Regulation, which did not distinguish between adults and children as data subjects nor handle the particular consent requirements for minors.[78]

Although the GDPR establishes a benchmark for the protection of children's data both inside and outside of Europe, certain of its provisions—especially Article 8—need more explanation to ensure effective application.[79] Whether some online services—including those provided by non-profits or those with major offline components—qualify as information society services and hence call for parental consent requirements is debatable.[80] Moreover, services meant for adults yet used by children still generate questions about their GDPR compliance.[81] Whether a service targets children will depend on factors like content, the usage of animated characters, and advertising; legal precedents could help to clarify this point.[82] While the Article 29 Working Party has argued for a reasonable approach to consent gathering, consistent with the idea of data minimization, the GDPR lacks particular means for obtaining or validating parental assent.[83] The working group notes that, in low-risk circumstances, a simple email confirming parental permission could be sufficient.[84] Still, in high-risk situations more thorough verification could be needed. The working party emphasizes that the degree of verification should match the risks related to the data processing engaged in. Moreover, the GDPR suggests indirectly in some cases even though it does not specifically demand age verification. Should a kid consent without meeting the age requirements, data processing is considered illegal. Controllers are obliged to use reasonable steps to determine the age of the child; these steps are appropriate for the type and hazards related to the processing. Should a child say they are under the age of consent, controllers must obtain parental permission, therefore confirming that the person providing consent is either a parent or legal guardian. The verification technique cannot involve pointless data processing. Recital 30 of the GDPR specifies a special exception to the parental consent mandate in some instances, including directly offered preventive or counseling services to minors.[85] This exemption is based on the idea that minors could need access to particular services for their welfare and that requiring parental permission could prevent that access. Online helplines for victims of sexual abuse might provide treatment without involving parents since parental involvement may worsen these circumstances.

5. Children, Consent, and Data Protection under the Digital Personal Data Protection Act, 2023

The Act's[86] Main goal is to legally acknowledge, in line with accompanying constitutional rulings and the Supreme Court of India's established right to privacy, legally.[87] Under this recognised right, one has personal autonomy via which they may regulate their information. Under this approach, the main operator works through consent-based procedures. The present state of affairs raises several important questions around kid categorisation, approval rights for data collecting and permissible data usage limits. The issues highlighted need to be addressed if we are to ascertain the course children will follow to become India's "*Digital Nagariks*" (Digital Citizens). Published for public consultation in November 2022, the Draft Digital Personal Data Protection Bill of 2022[88] Defines the majority age as 18 years old.[89] The Bill outlines

[78] Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679*, WP 259, 25 (Apr. 10, 2018).
[79] *Id*. at 25–26.
[80] *Id*.
[81] *Id.* at 25.
[82] *Id*.
[83] Mačėnaitė, supra note 74; van der Hof, supra note 48; Valerie Verdoodt & Eva Lievens, *Targeting Children with Personalized Advertising: How to Reconcile the (Best) Interests of Children and Advertisers*, in Gert Vermeulen & Eva Lievens (eds.), *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance and Big Data* (Maklu-Publishers 2017).
[84] Mačėnaitė, supra note 74.
[85] As the ALRC noted, "it provides certainty and enables practical operation in those situations where individual assessment is not reasonable or practicable." Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol. 3, 2008) at 2287.
[86] **The Digital Personal Data Protection Act, 2023** ("Act").
[87] **Justice K. S. Puttaswamy v. Union of India** (2017) 10 SCC 1 (Puttaswamy-I); **Justice K. S. Puttaswamy v. Union of India** (2019) 1 SCC 1 (Puttaswamy-II).
[88] **The Digital Personal Data Protection Bill, 2022** ("Draft"), available here https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022.
[89] *Id* at **Section 2(3), Draft**.

several illegal activities.[90] And lays severe guidelines on how personal data can be acquired and handled. Review of the 20,000 public comments along with multiple conversations revealed that this data processing method required both changes and corrections.[91] Providing goods and services to young people in the new digital economy has become essential since it meets their particular demands independent of content type. While providing information appropriate for their age range, protection of children's privacy and data security takes front stage.

Age verification combined with adult content filtering and mental health service delivery need particular protection measures since these purposes demand secured data handling practices. Children between 0 and 18 are classified as minors with limited stated limitations under Indian law since 1875[92]. Since minors under the law lack competence to sign contracts, most agreements need consent from their parents or guardians.[93] The exclusive reliance on parental consent or consent from a single source cannot sufficiently explain the presence of minor users on online programs due to the allowed specific exceptions, which favour the kid.[94] The Act and Draft[95] especially identify children between the ages of 0 and 18.[96] The structure is based on ideas established by GDPR[97] and CCPA[98], so defining adaptable degrees of data security guidelines.[99] According to the Draft rules[100], the Act calls for parental consent before handling any personal data.[101] While the suitable laws specify the procedures to be followed for verification, a validation process has to confirm the permission. The Act mandates guardians of all children under their control—including those with disabilities—confirm consent for them.[102] The Act gives the government power to approve exemptions allowing for the processing of personal data for children. Depending on set criteria, specific coverages from exclusions apply to some Data Fiduciaries[103] and specific objectives (the "*Class Exemption*").[104] The act allows a Data Fiduciary to get parental permission by demonstrating security within their data handling procedures (the "*safety dilution*").[105] The adjustment seeks to strike a compromise between modern service operational needs and children's data protection.

Like the Draft[106], the Act notes parents and legal guardians as "*data principals*" for their children.[107] Usually, processing personal data of a minor requires parental permission.[108] Particularly when parents and children disagree over permission, the application of Data Principal rights, or the resolution of grievances, the possibility of totally substituting a child's autonomy with that of the parent creates great challenges. Though the new phrase lets a child exercise their rights in tandem with their parent, the broad definition of "*processing*"[109] and the clear directive for "*verifiable parental agreement*" could cause Data Fiduciaries to

---

[90] *Id* at **Section 10, Draft**.
[91] International Association of Privacy Professionals, Government receives more than 20K submissions on India's proposed DPDPB, May 1, 2023.
[92] **The Indian Majority Act, 1875**.
[93] **Section 11, The Indian Contract Act, 1872**.
[94] See: **Section 30, Partnership Act, 1932**.
[95] *Supra* note at 88 **Section 2(3), Draft**.
[96] *Supra* note of 86 **Section 2(f), Act**.
[97] **Article 8, GDPR**: follows a graded approach for processing personal data of children, and the valid age for consent ranges from 13 to 16 years depending on Member State, subject to a minimum age of 13 years.
[98] **Section 1798.120, California Consumer Privacy Act**: provides that businesses can sell personal information of a child under the age of 16 years if they get affirmative authorization and under the age of 13 with opt-in consent of the parent or guardian.
[99] However, this is not true globally, for instance, the **Singapore Personal Data Protection Act, 2012** (here) does not specifically call out obligations in relation to children, and the **Personal Data Protection Commission of Singapore's 'Advisory Guidelines on Key Concepts in the Personal Data Protection Act'** (May 16, 2022, available [here]), state that a "child or young person" is defined as someone below 18 years of age.
[100] *Supra* note at 88 **Section 10(1), Draft**.
[101] *Supra* note at 86 **Section 2(t), Act**: "personal data" means any data about an individual who is identifiable by or about such data.
[102] *Supra* note at 86 **Section 9(1), Act**.
[103] *Supra* note at **Section 2(i), Act**: "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.
[104] *Supra* note at **Section 9(4), Act**.
[105] *Supra* note at **Section 9(5), Act**.
[106] *Supra* note at 88 **Section 2(6), Draft**.
[107] *Supra* note at 86 **Section 2(j), Act**.
[108] *Supra* note at 97 **Article 8, GDPR**.
[109] Supra note at 86 **Section 2(x), Act**.

turn down such requests.[110] Moreover, by following the age of majority, the Act ignores the child's capacity for judgment—a consideration taken into account in present Indian penal law.[111] This leads one to investigate, if any, minors' rights regarding their personal information outside of parental control. Whether by rulemaking, Data Protection Board (DPB) rulings, or often asked questions, clarity on this issue would be much appreciated. With harm defined as bodily injury, identity theft, harassment, obstruction of approved benefits, or infliction of significant loss, the Draft proposed that Data Fiduciaries be forbidden from processing personal data in a manner that could jeopardise a child.[112] The Act has deleted the concept of "*damage*,"[113] and Data Fiduciaries are now forbidden from any handling that might compromise the welfare of a kid.[114] Data fiduciaries have to act in a fiduciary capacity, aggressively thinking through any negative consequences their data processing could cause for children. The Act also imposes restrictions on "*tracking or behavioural monitoring of minors*" and "*targeted advertising aimed at minors,*" just like the Draft does. These rules might also cover techniques like age gating and content screening, which ensure that advertising and content are appropriate for children, even if the meanings of these terms remain very unclear.

Unlike the Draft[115], the Act[116] Let's Class Exemption and Safety Dilution apply on the restrictions on data processing for minors.[117] This adaptability allows exemptions for protective measures, including age gating and sophisticated age verification, therefore guaranteeing the ongoing availability of age-appropriate content and services, including educational and entertainment resources for teenagers. Together with the bans on tracking, behavioural monitoring, and profiling, the rules specified in the Act will be crucial in defining the specific categories of Data Fiduciaries and the settings in which the criteria for getting verifiable consent are inapplicable. Like the Draft, the Act keeps the punishment for violating extra responsibility with children's data at two hundred crore rupees.[118] This punishment highlights the need for explicit, specific delegated law, which is necessary to give businesses certainty regarding compliance and legislative intent in the management of personal data of children. The Act's clauses particularly benefit businesses targeted at this demographic and industries serving children since they allow them to engage with children in a way that is both safe and safeguarding of their interests. Along with the potential of a lowered age threshold for parental assent in some cases, the exemption of specific data processing activities gives companies a more defined strategy to correctly handle children's data while preserving their welfare.

6. Discussion

The privacy of children necessitates specific protection, both in the digital domain and the physical environment. A digital trail made by children begins before birth yet continues until their death. Digital services demand personal information sharing from children, though they typically do not grasp how such data sharing entails potential risks or theoretical concepts involved. The Hon'ble Apex Court emphasized this matter correctly when it declared privacy as an essential human right in "*K.S. Puttaswamy*." The rapidly developing digital world makes child personal data protection a key issue for this generation. Children's rising involvement with online services has triggered multiple data collection events, which lead to privacy concerns because appropriate safety measures have not been established. The Digital Personal Data Protection (DPDP) Act, 2023 of India creates a complete regulatory structure that safeguards personal data at all stages including data belonging to minors. Records of children receive special handling because they face privacy risks more intensely than adults under the Digital Personal Data Protection (DPDP) Act framework. An initial explanation of both "*children's personal data*" definition and its included information types must precede examining the law's child-related specifications. The Digital Personal Data Protection Act, 2023 through its Section 2(f) defines children as all persons who remain younger than 18

[110] Supra note at 86 **Section 9(1), Act**.
[111] **Section 82, Indian Penal Code, 1860**.
[112] *Supra* note 88 at **Section 10(2), Draft**.
[113] *Supra* note at 88 **Section 2(10), Draft**.
[114] Supra Note at 86 **Section 9(2), Act**.
[115] Supra note at 86 **Section 10(3), Draft.**
[116] *Supra* note at 86 **Section 9(3), Act**.
[117] Supra note at 86 **Sections 9(4), 9(5), Act.**
[118] Supra note at 86 **Entry 3, Schedule, Act.**

years old. The category of Children's Personal Data includes all data about children which allows identification through direct methods or alternative means. The set of identifying information includes name, residence data, date of birth and biometrics, as well as school reports and distinct pieces of information which can either directly or indirectly identify a child or shed light on their activities. Online activities pursued by children produce a wide variety of data because their activities cover a full spectrum of options.

The three central elements under the DPDP Act for understanding data duration rules are Data Principal, Data Fiduciary, and Data Processor. These three entities collectively provide critical support in maintaining proper lawfulness for child personal data management. A person who owns personal data falls under the category of Data Principal. Under minors' regulations, the child functions as the individual responsible for data purposes. Since children lack proper understanding of data privacy protection, they need a Data Principal who functions as their legal representative, such as parents or guardians. When a child joins an e-learning platform, their parent usually provides basic information about the child, alongside consent to allow data collection. A Data Fiduciary refers to an entity which stands as a business or organization that creates aims and methods for handling personal data processing. Data Fiduciaries maintain legal responsibility to handle all processes of personal data collection and storage, and processing activities. The company operating a social networking platform serves as the Data Fiduciary during instances when young users interact with the application. Alternatively, there exists a Data entity which guarantees that all data stays confined to its designated purpose while also obtaining parental consent. The Data Fiduciary authorizes people or businesses to act as Data Processors for personal data tasks. The database administration for children's data passing to a third-party service provider makes the supplier become the Data Processor. In data processing endeavours, the Data Processor operates under the directives given by the Data Fiduciary.

According to the National Commission for Protection of Child Rights (2021), a substantial 30.2% of children aged 8 to 18 used smartphones or electronic devices for their virtual educational needs.[119] These platforms collect detailed personal information, including academic records, together with personal details, which creates concerns about storing and sharing this information. Social media and gaming systems provide attractive features to young users who might not fully grasp the online consequences of information sharing. Google and Facebook receive most of the data obtained from children's applications according to research findings, although Google takes in the highest proportion.[120] Studies revealed that eighty-five percent of assessed applications accessed sensitive personal information without required consent, thereby endangering the privacy of children to a great extent. E-Commerce platforms serving young customers systematically collect user interaction data to justify stringent privacy safeguards in their operations. The $11 billion in advertising revenue earned by social media platforms from child and adolescent audiences prompted the need for new regulations in this field according to the 2022 Harvard study.[121] The DPDP Act establishes clear rules for child data collection and processing and storage operations. Among the principal responsibilities are:

a) The DPDP Act through Section 9 requires Verifiable Parental approval before processing or collecting personal data that involves children.[122]

[119] Isha Suri & Pallavi Bedi, *Shepherding Children in the Digital Age*, THE TIMES OF INDIA, https://timesofindia.indiatimes.com/blogs/voices/shepherding-children-in-the-digital-age/ (last visited Mar 14, 2025).
[120] Annapurna Roy, *Google, Facebook Skim Most Data from Apps for Kids: Study*, THE ECONOMIC TIMES, Jan. 29, 2024, https://economictimes.indiatimes.com/tech/technology/google-facebook-skim-most-data-from-apps-for-kids-study/articleshow/107209705.cms?from=mdr (last visited Mar 14, 2025).
[121] Elizabeth Napolitano, *Social Media Apps Made $11 Billion from Children and Teens in 2022 - CBS News*, (2023), https://www.cbsnews.com/news/facebook-instagram-tiktok-snapchat-children-advertising-2022-harvard-study/ (last visited Mar 14, 2025).
[122] Aditi Agrawal, *NCPCR Likely to Seek Clause for Parents' Consent under Data Protection Rules*, HINDUSTAN TIMES (2024), https://www.hindustantimes.com/india-news/ncpcr-likely-to-seek-clause-for-parents-consent-under-data-protection-rules-101724180521788.html (last visited Mar 14, 2025).

b) Any given consent requires unconditional status and must be voluntary, together with transparency, explicit confirmation and also needs to be both informed and unequivocal.[123]
c) The Act states clearly that the collected information serves only the approved purpose, but additional data acquisition requires substantial necessity.[124]
d) Data Fiduciaries must protect child welfare by refraining from harmful data management tasks that violate the provisions of the Act.[125]
e) According to Section 9(3) of the DPDP Act, Data Fiduciaries must refrain from tracking children technically, while also refraining from conducting profiling and behavioral monitoring operations and advertising services to them.

According to data guidelines, data retention for children applies only to what is necessary to complete the specific reasons of data collection. The data destruction process becomes mandatory once the utilization of the information stops. The Act provides several rights to Data Principals which allow them to fix personal data and request alterations or deletion together with consent withdrawal anytime.[126] Security Protocols require Data Fiduciaries to implement proper security and organizational processes and technical measures so they can protect data from breaches and keep within data protection laws.[127] Selected violations of regulations lead to substantial monetary and administrative penalties for non-compliant organizations. Child data violations trigger monetary punishments that reach up to 200 crore rupees.[128]

Data compliance violations lead to immediate damage of an organization's reputation and bring about loss of trust from stakeholders as well as decreased client numbers and economic decline. Organizations that fail to comply must face legal actions that cost them both court costs and possible payment of damages.[129] Privacy legislation in both European Union jurisdictions and across the entire global domain have set strict guidelines about protecting children's data through regulations such as the General Data Protection Regulation (GDPR).[130]

The video-sharing service paid 345 million euros as a penalty in 2023 due to its failure to verify parental consent properly, and Meta received 405 million euros for GDPR violations during child data protection in 2022. Microsoft faced legal charges for privacy violations related to child data collection without consent from parents during the lawsuit regarding Microsoft Chromebooks. The Danish Data Protection Authority (DPA) imposed a processing ban on Microsoft because the company failed to properly assess risks before the company could resume data operations. The DPDP Act receives anti-democratic critiques because of Draft Rule 10 as well as other provisions that trigger fundamental violations of privacy rights even though the law was introduced to protect private rights.[131] The requirement to verify user ages poses multiple operational problems because it requires entire system-wide validation for all users, thus creating potential difficulties in maintaining compliance requirements. Under the DPDP Act 2023 organizations must strictly protect children's data or face substantial penalty fines. Executive teams must work closely together with

[123] Aihik Sur, *DPDP Rules: NCPCR to Recommend MeitY to Bring in KYC-Based Age Verification for Children*, MONEYCONTROL (2024), https://www.moneycontrol.com/technology/dpdp-rules-ncpcr-to-recommend-meity-to-bring-in-kyc-based-age-verification-for-children-article-12801563.html (last visited Mar 14, 2025).
[124] *Supra* note at 86 Section 9(2).
[125] Anuradha Gandhi & Rachita Thakur, *SAFE For Kids Act: Protecting Young Users from Harmful Social Media Feeds*, S.S. RANA & CO. (2024), https://ssrana.in/articles/safe-for-kids-act-law-protecting-young-users-harmful-social-media-feeds/ (last visited Mar 14, 2025).
[126] *Supra* note ay 86 Section 12
[127] INPLP, *Insufficient Legal Basis to Use Google Workspace as an Educational Tool in Schools*, INTERNATIONAL NETWORK OF PRIVACY LAW PROFESSIONALS (2024), https://inplp.com/latest-news/article/insufficient-legal-basis-to-use-google-workspace-as-an-educational-tool-in-schools/ (last visited Mar 14, 2025).
[128] Adam Satariano, *Meta Fined $400 Million for Treatment of Children's Data on Instagram*, THE NEW YORK TIMES, Sep. 5, 2022, https://www.nytimes.com/2022/09/05/business/meta-children-data-protection-europe.html (last visited Mar 14, 2025).
[129] Anuradha Gandhi & Isha Sharma, *TikTok's Liability: Violation of Children's Data*, S.S. RANA & CO., https://ssrana.in/articles/tiktoks-liability-violation-of-childrens-data/ (last visited Mar 14, 2025).
[130] Alan J, *European Center For Digital Rights Believes Microsoft Intruded On Privacy Of Schoolchildren*, (Jun. 4, 2024), https://thecyberexpress.com/european-center-for-digital-rights-microsoft/ (last visited Mar 14, 2025).
[131] Live Law, *Parental Consent Needed For Children To Join Social Media, Gaming Platforms : Proposal In Draft Digital Personal Protection Rules*, (2025), https://www.livelaw.in/top-stories/parental-consent-needed-for-children-to-join-social-media-gaming-platforms-proposal-in-draft-digital-personal-protection-rules-279950 (last visited Mar 14, 2025).

governments, along with organizations and public groups, to carry out these rules properly in India and worldwide. Detailed execution requires comprehensive collaboration.

7. Conclusion

It gets more difficult to ensure that youngsters fully understand the mechanisms of data collecting, use, and dissemination as internet companies obtain and profit from their information. Age limits on data collecting are controversial since it is impossible to assign young children the responsibility for mitigating these risks.[132] Though they try to solve this problem, parental permission rules are not the best one, especially considering the Convention on the Rights of the Child (CRC). Academics argue that since they usually give either too much protection or the demands of online commerce top priority, existing consent rules often ignore both the welfare of children and their need for autonomy. Moreover, severe demands for parental agreement could limit children's rights to freedom of expression and knowledge access.[133] Maintaining practical application, the Australian integrated strategy for kid data protection offers flexibility by considering children's cognitive development, autonomy, and involvement. This approach departs from the frameworks set forth by the Children's Online Privacy Protection Act (COPPA) in the United States and the General Data Protection Regulation (GDPR) in the European Union, which rely on a predefined age limit and neglect individual assessments of a child's capacity to consent. Practically, the European and Australian methods may produce similar outcomes.[134] Parental permission for information society services—that is, internet services—is necessary under the GDPR when personal assessments of a child's maturity prove impractical. Though this is not particularly stated in the statute, the GDPR allows individual evaluations for offline processing of personal data. Previously, EU data protection authorities underlined the need for tailored assessments when getting consent from children; nevertheless, this approach is challenging to enforce legally since it depends on clear guidelines and obligations for data controllers to prevent significant penalties.[135]

Many data protection models include social responsibilities on online services targeted at children to balance the needs of online commerce with children's rights. Early legislation, like COPPA, required explicit privacy rules written in understandable language to support informed permission.[136] The GDPR also emphasizes for data controllers openness, responsibility, and the need for rules of behavior.[137] Research shows, however, that privacy policies often show too much complexity for young understanding, which reduces compliance rates with privacy laws. Thus, including privacy by design and doing data protection impact analyses might help to enhance the protection of personal information for children.[138] We have to respect the opinions and needs of young people. Studies show that even young people who spread knowledge online nevertheless worry about their privacy. Studies reveal that people use different devices for different purposes, including texting or using ephemeral technology like Snapchat for more private discussions.[139] On these networks, the data collecting and disclosure policies reflect those of more public venues like Instagram and Twitter. This shows that even if children try to protect their privacy by limiting

---

[132] Article 29 Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, WP 160 (Feb. 11, 2009).

[133] Anca Micheti, Jacquelyn Burkell & Valerie Steeves, *Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand*, 30(2) BULL. OF SCI. TECH. & SOC'Y 130 (2010).

[134] For example, a recent study in the US reports that the majority of over 5,000 popular children's apps are potentially in violation of COPPA: Irwin Reyes, Primal Wijesekera, Joel Readon, Amit Elaxai Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez & Serge Egelman, *Won't Somebody Think of the Children?: Examining COPPA Compliance at Scale*, 3 PROC. PRIVACY ENHANCING TECHS. 63 (2018).

[135] Simone van der Hof & Eva Lievens, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR*, 23(1) COMM. L. 33 (2018).

[136] Valerie Steeves, *Privacy, Sociality and the Failure of Regulation: Lessons Learned from Young Canadians' Online Experiences*, in Beate Roessler & Dorota Mokrosinska (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015); Alice E. Marwick & danah boyd, *Networked Privacy: How Teenagers Negotiate Context in social media*, 16 NEW MEDIA & SOC'Y 1051 (2015).

[137] Matthew Johnson, Valerie Steeves, Leslie Shade & Grace Foran, *To Share or Not to Share: How Teens Make Privacy Decisions about Photos on Social Media* (Ottawa: MediaSmarts 2017).

[138] *Id.*

[139] Steeves, *Terra Cognita: Surveillance of Young People's Favourite Websites*, in Tonya Rooney & Emmeline Taylor (eds.), *Surveillance Futures: Social and Ethical Implications of New Technologies of and Children and Young People* (Routledge 2016). See also Irwin Reyes et al., *Won't Somebody Think of the Children?: Examining COPPA Compliance at Scale*,

their intended audience, the information they provide is nonetheless obtained and used to affect their online behavior and self-image. The capacity of current strategies to limit the collection of children's data helps one to assess their effectiveness in protecting their online privacy.[140] Examining the 50 most visited websites among Canadian children found that commercial data collecting was rather common—96% of these sites used an average of five trackers to collect user information. Although eighty percent of websites featured privacy choices, just twelve percent had default privacy settings set to private. This implies that authorities in data protection have to keep working to ensure that laws provide enough protection of privacy for minors.

[140] *Supra* note 90.