17. Data protection and children's online privacy

Valerie Steeves and Milda Mačėnaitė

I. INTRODUCTION

On 17 October, 2008, the 30th International Conference of Data Protection and Privacy Commissioners issued a resolution on children's online privacy (Strasbourg Resolution), raising specific concerns about the 'vast amounts of personal information' that are being collected from and about children in networked environments.[1] Together, the Commissioners called for legislation to limit the collection, use and disclosure of children's information, especially in the context of micro-targeting and behavioural advertising. They also urged organizations to develop plain language privacy policies and user agreements to facilitate the consent process, and supported the creation of educational resources to help young people access 'a safe online environment respectful of their privacy'.[2]

The Resolution suggests that children's online privacy is a special case, for three inter-related reasons. First, children are more vulnerable than adults to pressures to disclose information about themselves simply because they are young; in the Commissioners' words, they often 'lack the experience, technical knowledge and tools to mitigate [the privacy] risks'[3] they encounter as they blog, text, share photos, play games and interact online. Second, the creation of a permanent digital record may be more harmful to children than it is to adults. Not only are children more likely to make missteps because of their relative immaturity, those missteps may be especially difficult or embarrassing to explain when individuals are publicly called to account for them as adults in the future. Accordingly, the protection of children's privacy requires that there be 'no lasting ... record of content created by children on the Internet which challenges their dignity, security and privacy or otherwise renders them vulnerable now or at a later stage in their lives'.[4] Third, children's privacy is contextualized by the United Nations Convention on the Rights of the Child[5] (CRC) which calls upon states to 'respect and ensure the rights of children, including the right to the protection of their privacy'.[6]

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

[2] Ibid., para 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, 18 October 2016).

[3] Ibid., para 5.

[4] Ibid., para 8.

[5] United Nations General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, 1577. The Convention has been ratified by every state in the world except the United States of America.

[6] Ibid., paras 6–7.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

The CRC is of particular note. Although privacy rights are included in general human rights instruments,[7] the CRC imposes additional obligations on states with respect to children. Under its provisions, children are entitled to 'special care and assistance'[8] because of their status as children, and the standard to be applied when drafting legislation affecting children's rights is in the 'best interests of the child'. [9] Legislators must accordingly ensure that regulations are crafted in ways that promote children's well-being.[10] CRC rights are also governed by the '3 Ps': provision; protection; and participation.[11] Provisions that protect children from inappropriate information practices[12] are simply one part of meeting the obligations on states pursuant to the CRC. States are also required to provide children with an appropriate media environment[13] and ensure that young people are able to participate in decisions that affect them in that environment.[14] At the same time, their evolving maturity also means that parents are expected to play a key role in children's decision-making.[15]

This chapter examines the ways in which key jurisdictions have responded to the special privacy needs of children. In particular, we map the emergence of children's privacy as a trade issue in the United States, and outline the provisions of the Children's Online Privacy Protection Act. We contrast the child-specific approach taken in the US with the application of general private-sector data protection principles to children's privacy issues in Canada and Australia. We then explore the transition in the EU from general protection to child-specific provisions, and the ways in which the European commitment to privacy as both a human right and a child's right have shaped existing regulations as well as the newly enacted General Data Protection Regulation.

II. THE EMERGENCE OF CHILDREN'S ONLINE PRIVACY AS A TRADE ISSUE IN THE UNITED STATES, CANADA AND AUSTRALIA

When data protection regulation was first enacted in Europe and North America in the 1970s, there was no mention of children or children's privacy in spite of the fact that both private and public sector organizations were collecting information from children at the time. For example, children's attendance in school and visits to hospitals generated a plethora of records that literally followed the child from cradle to grave, and marketing tactics like warranty registration cards and magazine subscriptions collected demographic details that could be linked to

---

7 See, for e.g., art 12 of the *Universal Declaration of Human Rights*, 10 December 1948, United Nations General Assembly, Resolution 217A.

8 CRC (n 5), Preamble.

9 Ibid., art 3(1).

10 Ibid., art 3(2).

11 Ann Quennerstedt, 'Children, But Not Really Humans? Critical Reflections on the Hampering Effect of the "3 p's"' (2010) 18 *IJCR* 619.

12 CRC (n 5), arts 16–17.

13 Ibid., art 17. See also Valerie Steeves, (2017). 'Snoops, Bullies and Hucksters: What Rights Do Young People Have in a Networked Environment?' in N.A. Jennings and S.R. Mazzarella (eds.), *20 Questions about Youth and Media*, (2nd ed., New York: Peter Lang).

14 Ibid., arts 17, 31.

15 Ibid., art 5.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

children's interests in toys, games, popular culture and fashion. Over the years, access rights to information held by the public sector were given to children and/or their parents in particular contexts, particularly education and health, but it was generally assumed that the burgeoning market in young people's information would be governed by general data protection legislation enacted within a particular jurisdiction.

The advent of the World Wide Web in the 1990s significantly changed the landscape, as website operators developed online playgrounds designed both to attract children and to encourage them to disclose their personal information for commercial purposes.[16] The first jurisdiction to respond to this as a distinct privacy issue was the US which passed the Children's Online Privacy Protection Act[17] (COPPA) in 1998.

COPPA is child-specific data protection legislation that requires parental consent for the collection, use and disclosure of personal information of children under 13 years of age.[18] It is commercial legislation,[19] akin to other forms of consumer protection, and as such is administered by the Federal Trade Commission (FTC). Its provisions require website operators and other online services (including mobile apps and connected toys) to publish privacy notices that provide children and their parents with information about their information practices,[20] and to obtain parental consent[21] to the collection, use and disclosure terms that are set out in the privacy notice. Parents also have the right to access their children's personal information,[22] and services are required to take steps to protect the information's confidentiality, security and integrity.[23] As such, the focus of the legislation is on parents' rights as opposed to children's rights: in the words of the FTC website, the 'primary goal of COPPA is to place parents in control over what information is collected from their young children online'.[24]

---

[16] Valerie Steeves, 'It's Not Child's Play: The Online Invasion of Children's Privacy' (2006) 3 *UOLTJ* 169; Sara M. Grimes and Leslie Regan Shade, 'Neopian Economics of Play: Children's Cyberpets and Online Communities as Immersive Advertising in Neopets.com' (2005) *1 International Journal of Media & Cultural Politics* 181; 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' (2015) 39 *Telecommunications Policy* 771.

[17] 15 U.S.C. §§ 6501–6506.

[18] Under COPPA, children 13 and over can consent on their own behalf.

[19] In the words of former Federal Trade Commission Chairman Jon Leibowitz:

> 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' (Ad Week, 19 December 2012) http://www.adweek.com/digital/ftc-restricts-behavioral-targeting-kids-146108/ accessed 10 January 2019.

[20] United States Electronic Code of Federal Regulations, Title 16 Chapter 1, Subchapter C, Part 312, as per 6502 (b)(1)(A).

[21] Ibid., Part 312.5.

[22] 6502 (b)(1)(B).

[23] 6502 (b)(1)(D).

[24] Federal Trade Commission, 'Complying with COPPA: Frequently asked questions' (20 March 2015) https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions accessed 10 January 2019.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

To satisfy this goal, COPPA has developed nuanced risk-based requirements for parental consent. Where a service uses children's data for internal purposes, it has to employ a lighter consent mechanism, such as the sending of an email to the parent and taking an additional confirming step after receiving the parent's response (the 'email plus' method). The highest risk services are those that disclose personal data to third parties, use behavioural advertising and enable children to publicly post information. These services must comply with the most rigid consent mechanisms, such as parents filling in and returning consent forms by mail, fax or scan, the provision of a credit card number, contacting the service provider via a toll-free number or video conference, and the verification of an official identification document.

Under the legislation, trusted third-party verification services can be developed and used, to minimize the amount of personal data the service has to process itself. Several technologies have been proposed by American corporations in this respect. Examples include the use of a knowledge-based authentication method (a way to verify the identity of a user by asking a series of challenge questions, typically that rely on so-called 'out-of-wallet' information[25]) or the use of a 'face match to verified photo identification' method[26] to verify that the person providing consent for a child is in fact the child's parent. Codes of conduct can also be proposed by industry setting out how parental consent is to be obtained.[27]

COPPA has had a significant impact on practices outside the US. Part of this reflects the popularity of American sites with non-American children, but many services targeted at children rely on the bright age-line approach and only require parental consent for children under 13 even when their domestic legislation is not age-specific.[28] In addition, the commercial imperatives behind COPPA have shaped non-American approaches.

Canada and Australia are good examples of this dynamic. Both Canada and Australia have comprehensive personal data protection schemes in place, which are a combination of federal and state/provincial and territorial Acts. In Canada, public sector collection is governed by first-generation data protection legislation that was enacted in the 1980s. The federal government only turned its mind to private sector legislation when the EU changed its regulations in 1995 to restrict cross-border flows of information to jurisdictions without adequate levels of protections.[29] Because of this, private sector data protection regulation was cast as a commercial issue and a necessary step in building consumer confidence in the emerging information

---

[25] Federal Trade Commission, 'Imperium, LLC Proposed Verifiable Parental Consent Method Application (FTC Matter No. P135419)' (23 December 2013) https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf accessed 10 January 2019.

[26] Federal Trade Commission, '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' (19 November 2015) https://www.ftc.gov/public-statements/2015/11/commission-letter-approving-application-filed-jest8-limited-trading-riyo accessed 10 January 2019.

[27] Art 40(2)(g).

[28] Valerie Steeves, 'Terra Cognita: Surveillance of Young People's Favourite Websites' in Tonya Rooney and Emmeline Taylor (eds), *Surveillance Futures: Social and Ethical Implications of New Technologies of and Children and Young People* (Routledge 2016).

[29] 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] *OJ L 281, 31-50.*

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

economy.[30] The resulting federal legislation, the Personal Information and Protection of Electronic Documents Act[31] (PIPEDA), applies across the country unless substantially similar legislation is passed to govern private sector collection of personal information within the provinces or territories. In like vein, the main piece of legislation in Australia, the Federal Privacy Act[32] 1988, incorporating the Australian Privacy Principles, is applicable to the federal public sector agencies as well as credit reporting organisations and the private sector.

Despite the extensive coverage of these specific and comprehensive schemes, both frameworks neither explicitly acknowledge children as data subjects nor refer to a specific age threshold after which children can give consent to their personal data processing. Enforcement of the general rules that apply to everyone is complicated by the fact that children do not have the legal status to make decisions about their information until they reach the age of majority or are recognized in law as mature minors. Because of this vacuum, COPPA has in practice set the de facto standard for networked services as most non-American services aimed at children tend to ask for parental consent for children under 13.[33]

At the same time, both the Canadian and Australian privacy commissioners have been actively engaged with children's privacy issues. The Canadian Commissioner took the lead role in creating the Strasbourg Resolution, and her findings in complaints against Facebook[34] in 2009 and Nexopia[35] in 2013 were important landmarks in using general data protection principles to restrain the collection of children's information on social media sites. The Australian Commissioner has also exercised his jurisdiction against children's services[36] and, in explicitly addressing his regulatory choices, has followed an articulated line of thinking about the regulation of children's consent.

The first Australian discussions about the need to address children's privacy took place at the time of passage of the Privacy Amendment (Private Sector) Act 2000 (Cth), shortly after the adoption of COPPA in the US. Initially, there was an identical, yet unsuccessful, effort to introduce an amendment that would require commercial service providers to obtain the consent of a child's parent before collecting, using or disclosing personal information of

---

[30] Industry Canada and Department of Justice, *Building Canada's Information Economy and Society: The Protection of Personal Information* (White Paper, C (2nd series), 1998)

[31] Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

[32] The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came into force on 12 March 2014.

[33] See, e.g., Steeves, 'Terra Cognita: Surveillance of Young People's Favourite Websites' (n 28).

[34] 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.

[35] Privacy Commissioner of Canada Investigation, 'Social networking site for youth, Nexopia, breached Canadian privacy law' PIPEDA Report of Findings #2012-001.

[36] 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' (12 September 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 10 January 2019; Statements on Facebook and Cambridge Analytica, 'Investigation into Facebook opened' (5 April 2018) https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica#investigation-into-facebook-opened accessed 10 January 2019.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

a child aged 13 or under.[37] The issue remained on the political agenda. In 2001, a consultative group on children's privacy was established by the Attorney-General's Department, but again no tangible outcome was achieved.[38]

Some years later, the issue was again picked up by the Australian Law Reform Commission (ALRC) which in 2008 investigated the extent to which the Privacy Act 1988 provides effective protection for individuals, including children and young people, and recommended reforms.[39] In a nutshell, the ALRC recommended a model for consent that combines individual assessment and a minimum age of presumption of capacity. Recognizing that 'individual assessment is the fairest and most appropriate way to determine if an individual under the age of 18 has the capacity to make a decision',[40] the ALRC concluded that such an assessment is not always practicable and reasonable, for example due to the online nature of the interaction or inadequate training of an organization's staff. Therefore, the ALRC recommended a combined model to consent, which was later embraced by the Commissioner in his non-binding guidelines.[41] In line with the ALRC view, the guidelines of the Commissioner state that organizations should consider in each case whether an individual child has capacity, i.e., sufficient understanding and maturity, to give consent, to make a request or exercise a right of access under the Privacy Act or whether a parent or guardian has to consent on behalf of a child.[42] Where such an assessment on a case-by-case basis is not reasonable or practicable, a general presumption exists that a person 15 and older has capacity to consent, unless any reasons suggest otherwise.[43]

III. THE EUROPEAN UNION AND THE HUMAN RIGHTS APPROACH TO CHILDREN'S ONLINE PRIVACY

Private sector regulation of privacy in the EU has been contextualized by strong protections for privacy as a human right in EU law.[44] The growing importance of children's rights in all policies and measures affecting children, including the digital environment, has been affirmed in many strategic EU policy documents.[45] The EU commitment to safeguard children's

---

[37] Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 November 2006, 20302 (N Bolkus). The amendment was supported by the Australian Democrats: *Commonwealth of Australia*, Parliamentary Debates, Senate, 29 November 2000, 20162 (N Stott Despoja), 20165.

[38] D Williams (Attorney-General), 'First Meeting of Consultative Group on Children's Privacy' (Press Release, 4 June 2001). Cited in Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol 3, 2008) 2254.

[39] Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol 3, 2008).

[40] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines*: *Privacy Act 1988* (31 March 2015) 12–13.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Besides a right to private life enshrined in art 7, the Charter of Fundamental Rights of the European Union ([2000] OJ C364/1) recognises the protection of personal data as a separate right under its art 8.

[45] Commission (EC), **'**European Strategy for a Better Internet for Children' (Communication) COM/2012/0196 final, 2 May 2012; Commission (EC), 'An EU Agenda for the Rights of the Child' (Communication) COM/2011/0060 final, 15 February 2011.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

rights to protection and care has been explicitly enshrined in the Charter of Fundamental Rights.[46] Although early iterations of privacy laws have been universal in application, recently a child-specific perspective in the context of online privacy has been increasingly embraced by policy makers not only in the EU but also on a broader regional and international level.[47]

The normative reasons to treat children differently to adults in data protection law include the need to respect the specific catalogue of the child rights, in particular the best interest of the child, their evolving capacity, and participation,[48] and to avoid conflicts between adults and child rights.[49] The practical reasons to design a child-tailored data protection regime relate to more recently collected empirical data vis-à-vis the risks for children and excessive and complex children's data collection practices online, all witnessing against the age-blind approach to children's privacy in the online context. A growing body of social science research on children's online behaviour demonstrated the need to account for particular characteristics and potential vulnerabilities of children as internet users and to address the potentially more serious impact of harm on them. The developmental science added further claims that children, particularly adolescents, are potentially more risk-prone and impulsive, i.e., the behavioural features suggesting them being in a different position than adults when making long-term decisions and acting on their own behalf.[50] Also, academics have established the link between developmental needs and interest, such as identity formation, developing one's agency and establishing autonomy, and creating peer relations and online privacy behaviour of adolescents.[51] Consequently, it has been claimed that the online data-gathering techniques are often tailored to satisfy adolescents' needs and to exploit vulnerabilities, all fears that have raised concerns among academics and policy makers.[52] In sum, the specific developmental features and needs might influence children's online behaviour and increase the possibility of online victimisation among peers, as well as the possibility of commercial personal data exploitation, to a level higher than that of cases involving adults.

---

[46] Charter of Fundamental Rights of the European Union [2000] OJ C364/1, art 24

[47] Council of Europe, Strategy for the Rights of the Child 2016-2021 (March 2016); UN 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' (January 2017); UK House of Lords Committee on Communications, 'Growing up with the internet' (2nd Report of Session 2016–17, March 2017).

[48] Simone van der Hof, 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2017) 34(2) *Wis. Int'l L.J.* 409. Eva Lievens, 'Children's Rights and Media: Imperfect But Inspirational', in Eva Brems, Wouter Vandenhole and 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?' (2008) 46(2) *Intermedia* 18.

[49] 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* (OUP 2012).

[50] Cheryl B. Preston and Brandon T. Crowther, "Legal Osmosis: The Role of Brain Science in Protecting Adolescents (2014*) Hofstra Law Review* 447.

[51] Jochen Peter and Patti M. Valkenburg, 'Adolescents' Online Privacy: Toward a Developmental Perspective' in Sabine Trepte and Leonard Reinecke (eds), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Springer 2011). Wouter M.P. Steijn and Anton Vedder, 'Privacy under Construction: A Developmental Perspective on Privacy Perception' (2015) 40(4) *Science, Technology, & Human Values* 615.

[52] Montgomery, 'Youth and surveillance in the Facebook era' (n 16).

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

Since 1995, in the EU children have been covered by the age-generic data protection provisions of Directive 95/46/EC[53] placing them in one single group of data subjects together with adults. In line with the universal human rights perspective, the Directive 95/46/EC was in essence designed to protect all the natural persons whose data is processed by organizations or institutions (data controllers) established or using data processing means in the EU, despite the age, nationality, or the place of residence of these persons.[54] The lack of harmonized legal provisions governing children's personal data in the EU opened the door for individual countries to regulate the matter as they deemed necessary, resulting in an uneven and diverging European regulatory picture.

Some countries chose to add more specifics on minors' consent in their national data protection laws. Hungary, the Netherlands and Spain introduced exact age thresholds for consent to personal data processing.[55] The Spanish Personal Data Protection Law added some additional protections: it prohibited the collection of data from minors regarding members of their family, such as their profession or financial information, without the consent of these family members.[56] The sole exception was data regarding the child's identity and address for the purpose of obtaining parental consent.

Some countries remained silent on the age threshold for consent in data protection law and in practice relied on other branches of law, especially contract law provisions establishing when a person becomes fully competent to acquire and assume rights and obligations. If children could carry out basic legal acts without the consent of their representatives in civil law, such as conclude small, daily transactions, they were also allowed to consent to some basic personal data processing operations.[57] In contrast, the majority of the EU countries tried to assess the concrete situation on a case-by-case basis applying the general criteria of the child's best interest, level of moral and psychological development, and capacity to understand the consequences of giving consent as well as other specific circumstances (such as the age of the child, the purpose of data processing, and the type of personal data involved).[58] Although such an evaluation is both context-specific and child-specific, data protection authorities typically developed assumption-based exemplar age thresholds for consent.

For example, the United Kingdom's Information Commissioner (ICO) indicated that 'assessing understanding, rather than merely determining age, is the key to ensuring that per-

---

[53] 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] *OJ L 281, 31-50.*

[54] Ibid., art 4.

[55] 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).

[56] 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.

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

[58] 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, 11 February 2009).

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

sonal data about children is collected and used fairly'.[59] However, when services were directed at children, the UK ICO required services to obtain parental consent for children under the age of 12. In Belgium, the data protection authority acknowledged the gradual development of minors and the need for more independence with growth, but advised services to get parental consent when a child is not mature enough to be able to understand the implications of the giving of consent.[60] Yet, it stated that parental consent should be required for the collection of sensitive data from children under 16, and in all cases when data processing was not in the interest of the child.[61]

Other countries have increasingly provided specific rights to enable children and their parents to access and erase their personal data. The UK Data Protection Act included a special section on the exercise of data protection rights in Scotland and established a presumption that a person of 12 years of age or more is of sufficient age and maturity to understand and exercise these rights.[62] In 2016, France introduced the right to be forgotten for minors allowing to erase their online personal data through an accelerated procedure.[63] France also made it possible for minors of 15 years or older to exercise their rights of access, rectification and opposition and to refuse to allow their parents to be informed and have access to their personal data.[64] Finally, some countries provided specific safeguards in data protection law against the dissemination of personal data related to children in judicial non-criminal proceedings and press coverage, explicitly stating that the child's right to privacy takes precedence over both freedom of expression and freedom of the press.[65]

The diversity of national approaches across the EU resulted in a lack of clarity regarding the interpretation of data protection requirements in relation to children. Services collecting children's information often faced legal uncertainty and were subjected to diverging legal rules. The question 'at what age can children consent to have their personal data processed' even became ironically known as 'the million euro question' among European privacy experts.[66]

It should be noted, that the lack of specific data protection provisions for children in the rest of the European countries was to a limited extent compensated by legally non-binding guidelines. Some data protection authorities issued comprehensive advice on the protection of children's online privacy.[67] Other authorities partially covered the topic when raising awareness among children and parents through leaflets, articles and opinions, and specific awareness

---

[59] UK Information Commissioner's Office, *Personal information online* (Code of Practice, 2010).

[60] Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet* (2002).

[61] Ibid.

[62] UK Data Protection Act 1998, s 66.

[63] Law no. 2016-1321 of October 7, 2016 for a Digital Republic ("French Digital Law"), art 40, art 58.

[64] Ibid.

[65] Italian Data Protection Code (Legislative Decree no. 196 of 30 June 2003) s 50 and 52.5. Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities [1998] OJ 179, s 7.

[66] 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, 26 May 2009).

[67] Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet* (2002). Dutch Data Protection Authority, *Guidelines for the publication of personal data on the internet* (2007).

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

raising websites. At the EU level, the Article 29 Working Party, an independent advisory body made up of the representatives from all the EU data protection authorities (DPAs), adopted an opinion dedicated to children's personal data with a particular focus on schools.[68] The Working Party emphasized the child rights perspective, examining the main principles embedded in the CRC (such as the best interest of the child, protection and care, participation and evolving maturity) in the context of data protection.[69] It also focused on how the general principles of data protection (e.g., data quality, fairness, legitimacy, proportionality, retention, and data subject rights) apply to the field of education.[70] It took a flexible approach to the question of consent; rather than setting precise age limits for parental consent, it underlined the importance of taking the maturity of a child and complexity of the data processing at hand into account.[71] In addition, in several other subject-specific opinions, the Working Party made it clear that children's personal data should be processed with more protection and care than that of adults.[72]

IV. THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

The EU General Data Protection Regulation[73] (GDPR) has significantly changed the *status quo* and addressed specific needs of children as data subjects. It explicitly recognized that children deserve more protection than adults, especially online, as 'they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data' (Recital 38). Such specific protection is afforded through a two-tiered protection regime.[74] The first tier of the regime is composed of general, age-generic GDPR provisions which are specifically relevant to children and their online activities: the right to erasure; the right to data portability; obligations of data protection by design and by default; data protection impact assessments; requirements for awareness raising; and the provision of transparent information. The second tier refers to two provisions specifically applying to children as data subjects: restrictions on the profiling and marketing activities of data controllers, especially the prohibition of automated decisions that produce legal effects or similarly significantly affect the child (Recitals 38 and 71 GDPR) and the parental consent requirement (art 8).

The latter is the most significant, albeit controversial, child-specific provision in the GDPR. It imposes specific conditions for a child's consent in relation to online services. Where the

---

[68] 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, 11 February 2009).

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Article 29 Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013), *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010).

[73] 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) *OJ L 119*, 1–88.

[74] Milda Mačėnaitė, 'From Universal Towards Child-specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19(5) *New Media & Society* 765.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

child is below the age of 16, personal data collection and further processing is only lawful 'if and to the extent that consent is given or authorised by the holder of parental responsibility over the child' (art 8(1) GDPR). The age limit of 16 has not, however, become a uniform standard for digital consent in Europe, as the GDPR has afforded a margin of manoeuvre for individual EU Member States to lower the age to 13 in their national data protection laws. Many Member States have selected different age thresholds within the 13–16 range,[75] undermining the much-expected harmonization effect of the GDPR and maintaining significant challenges for companies that provide cross-border services.

The process of adopting Article 8 has been long, inconsistent and not grounded in evidence. The initial effort to closely mimic the US COPPA standards was unexpectedly challenged by calls for different age limits without any clear justification.[76] Even more controversially, the EU missed an opportunity to re-affirm its commitment to protect the rights of the child online in a systematic manner in other relevant regulations, e.g., the draft ePrivacy Regulation,[77] a *lex specialis* to the GDPR, neither addresses the distinction between adults and children as data subjects nor refers to the specific consent requirements.

At the same time, by explicitly acknowledging children as special data subjects and providing them with a wider set of rights, the GDPR sets a benchmark in Europe and beyond. Yet, at the current stage many questions still need to be clarified to ensure that its provisions, in particular Article 8, are clear and fully operationalized in practice. For example, although the GDPR requires parental consent under the specific age when data controllers provide information society services directly to children, the exact scope of this provision is still questionable. Although free commercial services are covered by the parental consent requirement, it is debatable whether online services for children provided by non-profit or educational organisations or certain online services that entail substantial offline components constitute an information society service.[78] In addition, it is still unclear to what extent online services created for adults but used by children are covered by the GDPR.[79] Cases brought before data

---

[75] 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.

[76] Milda Mačėnaitė and Eleni Kosta, 'Consent of Minors to their Online Personal Data Processing in the EU: Following in US Footsteps?' (2017) 26(2) *Information and Communications Technology Law* 146.

[77] 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).

[78] 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] OJ L 241, 1, art 1.1(b).

[79] 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, 10 April 2018) 25.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

protection authorities and courts will show how easy it will be to prove that the services are directed *de facto* to children and which of the factual evidence (e.g., the subject matter, the use of animated characters, advertising) will be given weight in the assessment. This clarification will be important in terms of actual protection as the terms of use of services often clearly exclude users below a certain age from the use of services but such users are present there in substantive numbers.

The GDPR also does not set out practical ways to obtain parental consent or to verify that a particular individual has a right to consent on child's behalf. The Article 29 Working Party has recommended a proportionate approach to data collection when obtaining and verifying consent, according to the principle of data minimisation.[80] However, it is still unclear whether and when parental consent verification can be based on a simple email exchange between a service provider and a parent and when the service provider requires additional proof. The Article 29 Working Party seems to accept in principle that in some cases an email to a parent would suffice to acquire parental consent, but the concrete application of this method alone in practice needs to be carefully assessed in specific cases. According to the Article 29 Working Party:

> What is reasonable efforts, when verifying that a person providing consent on behalf of a child is a holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology. In low-risk cases, verification of parental responsibility via email may be sufficient. Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information pursuant to Article 7(1) GDPR.[81]

In this regard, EU data controllers could look to the nuanced risk-based requirements for parental consent that have been developed under COPPA in the US.

Although the GDPR does not explicitly refer to the obligation to verify the age of the child, it is implicitly required in some cases. For example, if a child consents without being old enough to do so, the data processing would be considered unlawful in this case.[82] Therefore, according to the Article 29 Working Party '(w)hen providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities'.[83] If the child indicates that he or she is below the age of consent, the controller can accept this statement on face value but must then take steps to obtain parental consent, including steps to verify that the person consenting is the person with parental authority over the child.[84] In both cases, verification should not involve disproportionate data processing, but it is yet to be seen if data controllers will favour the least intrusive age verification methods, such as anonymous credentials and attributes, over more data-intensive options.

In keeping with the child's need for both protection and participation, Recital 30 of the GDPR states that consent by a parent or guardian is not required in the context of preventive

---

[80] Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 10 April 2018).

[81] Ibid., 25–26.

[82] Ibid.

[83] Ibid, 25.

[84] Ibid.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

or counselling services offered directly to a child. The rationale for such an exemption is the understanding that children may need to access certain services designed to help them and parental consent could create a barrier to such access. For example, online helplines for victims of sexual abuse would be able to obtain counselling if their parents are closely linked to the problem. In practical terms this exception means that the data controllers operating helplines or providing other preventive or counselling services online to a child (e.g., an online chat service to report abuse or violence) should not require prior parental consent from children.

V. CONCLUSION

Certainly, as a growing number of online services collect and monetize children's data, it is difficult to ensure that young people understand how information about them is being collected, used and disclosed. Bright line age restrictions underscore how problematic it is to place the burden of managing the risks on the shoulders of young children. However parental consent requirements are not a complete corrective, especially when viewed through the lens of the CRC. Many scholars are concerned that the various consent rules fail to fully take the best interests of children and their need for autonomy into account, either because they focus too much on protection or on the needs of online commerce.[85] It has also been suggested that strict parental consent requirement can negatively impact children's rights to freedom of expression and access to information.[86]

The Australian combined model, has an advantage of being both flexible and able to account for the developing cognitive capacity, autonomy and participation of children, but at the same time to remain operational in practice.[87] At a first glance, it seems to stand in stark contrast to the regulatory model introduced by the COPPA in the US or the GDPR in the EU, both of which entirely exclude the individual assessment element and rely on a bright line rule, presuming that from a certain age all children are able to provide their consent. However, when applied in practice both the Australian and the European models are likely to lead to a similar, if not an identical, outcome. The EU parental consent requirement applies only in the context of the information society services, i.e., to the online environment, where individual assessment is hardly possible. The GDPR does not exclude the individual assessment possibility when personal data of children is processed offline, which is not explicitly addressed in its text. Before the GDPR, EU data protection authorities have previously emphasized the importance of a case-by-case assessment when asking for consent from minors.[88] Yet, discretion to assess the actual capacity of each child or each age group is an attractive option from a child rights perspective, which is difficult to implement in law as opposed to non-binding

---

[85] Mačėnaitė (n 74) van der Hof (n 48). Valerie Verdoodt and Eva Lievens, 'Targeting Children with Personalised Advertising: How to Reconcile the (Best) Interests of Children and Advertisers' in Gert Vermeulen and Eva Lievens (eds) *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance and Big Data* (Maklu-Publishers 2017).

[86] Mačėnaitė, ibid.

[87] 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) 2287.

[88] 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, 11 February 2009).

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

guidelines, which needs to set clear and precise standards and obligations for data controllers who risk being imposed huge fines for non-compliance like in the GDPR and COPPA.

In an attempt to balance the competing pressures of online commerce and child rights, many data protection regimes also impose a social responsibility on online services directed towards children; certainly, early efforts at legislation such as COPPA called for transparent privacy policies written in plain language to better support informed consent. The EU has equally emphasized transparency and accountability of data controllers and the role of codes of conduct in its GDPR. However, studies indicate that privacy statements are often written in language well above young people's reading abilities,[89] and that compliance rates with the legislation are low.[90] In light of this, privacy by design and data protection impact assessments could significantly strengthen protection of children's personal data.[91]

It is also important to take the needs and perspectives of young people into account. Multiple research projects report that the mere fact that young people disclose information about themselves online does not mean that they have abandoned their interest in privacy.[92] Emerging work also suggests that they use different devices for different things, relying on texting, instant messaging and ephemeral technologies like SnapChat for more personal and intimate interactions;[93] however, the information infrastructures that govern the collection, use and disclosure of information on those platforms mirrors the structures on more 'public' platforms like Instagram and Twitter. This means that, even when young people put up barriers between their intended audiences in an attempt to protect their privacy, the information they share is collected, collated and used to shape their online behaviours and sense of self.[94]

But perhaps the most important way to evaluate the effectiveness of current approaches to protecting children's online privacy is to ask whether or not it limits the collection of children's data in the first place. A study of the top 50 websites visited by Canadian children suggests that commercial collection by these services is rampant: 96 per cent of them used an average of five trackers to continually collect data from children and, although 80 per cent had privacy settings, only 12 per cent were set to private by default.[95] This suggests that data

---

[89] Anca Micheti, Jacquelyn Burkell and Valerie Steeves, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand' (2010) 30(2) *Bulletin of Science, Technology & Society* 130.

[90] 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 and Serge Egelman, 'Won't Somebody Think of the Children?: Examining COPPA Compliance at Scale' (2018) 3 *Proceedings on Privacy Enhancing Technologies* 63.

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

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

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

[94] Ibid.

[95] Steeves, 'Terra Cognita: Surveillance of Young People's Favourite Websites' in Tonya Rooney and Emmeline Taylor (n 28). See also Irwin Reyes et al., 'Won't Somebody Think of the Children?:

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

protection authorities have more work to do to ensure that regulatory frameworks provide the kinds of privacy protections children deserve.

REFERENCES

Primary sources: Regulation and policy documents

30th International Conference of Data Protection and Privacy Commissioners, 'Resolution on Children's Online Privacy' (Strasbourg, 17 October 2008) para 2.

38th International Conference of Data Protection and Privacy Commissioners, 'Resolution for the Adoption of an International Competency Framework on Privacy Education' (Marrakesh, 18 October 2016).

Article 29 Working Party, *Guidelines on Consent under Regulation 2016/679* (WP 259, 10 April 2018).

Article 29 Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013).

Article 29 Working Party, *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010).

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, 11 February 2009).

Article 7, the Charter of Fundamental Rights of the European Union ([2000] OJ C364/1)

Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol 3, 2008) 2287.

Belgian Privacy Commission, *Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet* (2002).

Charter of Fundamental Rights of the European Union [2000] OJ C364/1, art. 24.

Commission (EC), 'European Strategy for a Better Internet for Children' (Communication) COM/2012/0196 final, 2 May 2012.

Commission (EC), 'An EU Agenda for the Rights of the Child' (Communication) COM/2011/0060 final, 15 February 2011.

Commonwealth of Australia, *Parliamentary Debates,* Senate, 30 November 2006, 20302 (N Bolkus). The amendment was supported by the Australian Democrats: *Commonwealth of Australia*, Parliamentary Debates, Senate, 29 November 2000, 20162 (N Stott Despoja), 20165.

Council of Europe, Strategy for the Rights of the Child 2016–2021 (March 2016).

Federal Trade Commission, 'Complying with COPPA: Frequently asked questions' (20 March 2015) https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions accessed 10 January 2019.

Global Privacy Enforcement Network, '2015 GPEN Sweep – Children's Privacy' (Final results, 2015).

Italian Data Protection Code (Legislative Decree no. 196 of 30 June 2003) section 50 and 52.5. Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities [1998] OJ 179, section 7.

Law no. 2016-1321 of October 7, 2016 for a Digital Republic ('French Digital Law'), art 40, art 58.

Office of the Australian Information Commissioner (OAIC),'Proposed changes to Facebook Data Use Policy and Statement of Rights and Responsibilities - OAIC letter to Facebook' (12 September 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; Statements on Facebook and Cambridge Analytica, 'Investigation into Facebook opened' (5 April 2018) https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica#investigation-into-facebook-opened accessed 10 January 2019.

Examining COPPA Compliance at Scale' (2018) 3 *Proceedings on Privacy Enhancing Technologies* 63 and Global Privacy Enforcement Network, '2015 GPEN Sweep – Children's Privacy' (Final results, 2015).

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines*: *Privacy Act 1988* (31 March 2015) 12–13.
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.
Privacy Commissioner of Canada Investigation, 'Social networking site for youth, Nexopia, breached Canadian privacy law' PIPEDA Report of Findings #2012-001.
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).
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) *OJ L 119*, 1–88.
UK Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (January 2017).
UK Data Protection Act 1998, section 66.
UK House of Lords Committee on Communications, 'Growing up with the internet' (2nd Report of Session 2016–17, March 2017).
UK Information Commissioner's Office, *Personal information online* (Code of Practice, 2010).
UN 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).
United States Electronic Code of Federal Regulations, Title 16 Chapter 1, Subchapter C, Part 312, as per 6502 (b)(1)(A).
Williams D (Attorney-General), 'First Meeting of Consultative Group on Children's Privacy' (Press Release, 4 June 2001). Cited in Australian Law Reform Commission, *Australian Privacy Law and Practice* (Report 108, Vol 3, 2008) 2254.

Secondary literature

Baker McKenzie, *Global Privacy and Information Management Handbook* (Baker McKenzie, 2017).
Grimes S.M. and L. Regan Shade, 'Neopian Economics of Play: Children's Cyberpets and Online Communities as Immersive Advertising in Neopets.com' (2005) 1 *International Journal of Media & Cultural Politics* 181.
Hughes K. 'The Child's Right to Privacy and Article 8 European Convention on Human Rights' in Michael Freeman (eds), *Current Legal Issues: Law and Childhood Studies, Vol. 14* (OUP 2012).
Johnson M., V. Steeves, L. Shade and G. Foran, *To Share or Not to Share: How Teens Make Privacy Decisions about Photos on Social Media* (Ottawa: MediaSmarts 2017).
Lievens E. 'Children's Rights and Media: Imperfect But Inspirational', in E. Brems, W. Vandenhole and E. Desmet (eds), *Children's Rights Law in the Global Human Rights Landscape: Isolation, Inspiration, Integration?* (Routledge 2017).
Livingstone S. 'Children: A Special Case for Privacy?' (2008) 46(2) *Intermedia* 18.
Mačėnaitė M. and E. Kosta, 'Consent of Minors to their Online Personal Data Processing in the EU: Following in US Footsteps?' (2017) 26(2) *Information and Communications Technology Law* 146.
Mačėnaitė M. 'From Universal Towards Child-specific Protection of the Right To Privacy Online: Dilemmas in the EU General Data Protection Regulation' (2017) 19(5) *New Media & Society* 765.
Marwick A.E. and d. boyd, 'Networked privacy: How teenagers negotiate context in social media' (2015) 16 *New Media and Society* 1051.
Micheti A, J. Burkell and V Steeves, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand' (2010) 30(2) *Bulletin of Science, Technology & Society* 130.
Montgomery K. *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (2007 MIT Press).
Montgomery K. 'Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications' (2015) 39 *Telecommunications Policy* 771.

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa

Peter J. and P.M. Valkenburg, 'Adolescents' Online Privacy: Toward a Developmental Perspective' in Sabine Trepte and Leonard Reinecke (eds), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (Springer 2011).

Preston C.B. and B.T. Crowther, 'Legal Osmosis: The Role of Brain Science in Protecting Adolescents' (2014) *Hofstra Law Review* 447.

Quennerstedt A. 'Children, But Not Really Humans? Critical Reflections on the Hampering Effect of the "3 p's"' (2010) 18 *IJCR* 619.

Reyes, I., P. Wijesekera, J. Readon, A. Elaxai Bar On, a. Razaghpanah, N. Vallina-Rodriguez and S Egelman, 'Won't Somebody Think of the Children?: Examining COPPA Compliance at Scale' (2018) 3 *Proceedings on Privacy Enhancing Technologies* 63.

Steeves V. 'It's Not Child's Play: The Online Invasion of Children's Privacy' (2006) 3 *UOLTJ* 169.

Steeves V. 'Privacy, Sociality and the Failure of Regulation: Lessons Learned from Young Canadians' Online Experiences' in B Roessler and D Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (Cambridge University Press 2015).

Steeves V. 'Terra Cognita: Surveillance of Young People's Favourite Websites' in Tonya Rooney and Emmeline Taylor (eds), *Surveillance Futures: Social and Ethical Implications of New Technologies of and Children and Young People* (Routledge 2016).

Steeves V., 'Snoops, Bullies and Hucksters: What Rights Do Young People Have in a Networked Environment?' in N.A. Jennings and S.R. Mazzarella (eds.), *20 Questions About Youth and Media* (2nd edn, 2017 New York: Peter Lang).

Steijn W.M.P. and A. Vedder, 'Privacy under Construction: A Developmental Perspective on Privacy Perception' (2015) 40(4) *Science, Technology, & Human Values* 615.

Vachman K. 'FTC restricts behavioural targeting of kids: New rules go into effect next July' (Ad Week,19 December 2012) http://www.adweek.com/digital/ftc-restricts-behavioral-targeting-kids-146108/ accessed 10 January 2019.

Van der Hof S. 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World' (2017) 34(2) *Wis. Int'l L.J.* 409.

Van der Hof S. and E. Lievens, 'The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR' (2018) 23(1) *Communications Law* 33.

Verdoodt V. and E. Lievens, 'Targeting Children with Personalised Advertising: How to Reconcile the (Best) Interests of Children and Advertisers in Gert Vermeulen and Eva Lievens (eds) *Data Protection and Privacy under Pressure: Transatlantic Tensions, EU Surveillance and Big Data* (Maklu-Publishers 2017).

Valerie Steeves and Milda Mačėnaitė - 9781786438515
Downloaded from PubFactory at 12/07/2022 03:48:01PM
via University of Ottawa