EJLT European Journal of Law and Technology

Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?

Cansu Caglar[1]

Abstract

Technology and the Internet have become significant and irreversible elements of modern life. Young people are particularly active users of digital services. In recent years, the number of young Internet users has grown significantly. They tend to stay online for longer periods and they are starting younger. While these technologies offer great opportunities and can improve daily life, every major beneficial development also has downsides. Many concerns have been raised over the emergence of internet-connected toys and wearables along with other smart devices and applications that were not necessarily developed for children's use. Leaving aside the visible risks such as sexual abuse, insomnia, obesity, low self-esteem or addiction, there are other hidden risks such as privacy invasions and data protection violations. These occur because children using the Internet, in effect, data subjects whose information is shared collected and processed, without their knowledge of or any understanding of potential consequences. Parents may be equally unaware of the privacy and security compromises their children are making and of all the possible impacts of data processing, data linkage, and data aggregation that may affect their rights and freedoms.

Children are exposed to these privacy-invasive digital risks partly because of the increasingly commercialised nature of information society services and the age of Big Data. The European Union has given special attention to data protection concerns arising from digital services offered to children, incorporating specific provisions into the General Data

[1] Law School, Aston University, Birmingham

Protection Regulation (GDPR). This article examines the newly incorporated requirements and concepts relating to child's consent under the GDPR and analyses whether its protection is adequate or reflects the cognitive appraisal of a child compared to an adult.

In addition, it sets out the requirements for obtaining valid consent for data processing from the child or parent and then briefly addresses the challenges this process encounters in practice. Given the complexities in implementing and enforcing these provisions, the article asks whether these requirements are sufficient to ensure children's rights and freedoms are protected. It evaluates whether the Regulation and its principles are failing to keep pace with the changing nature of technology.

Keywords: Data Protection, Privacy, Consent, Child's Consent, Parental Consent.

1. Introduction

In today's digital world, many of our everyday actions generate data, whether or not we know at the time. Alongside the information we choose to disclose, other data is gathered through sensors or is inferred through the use of sophisticated algorithms. The huge impact of this merging of the physical and digital worlds is undeniable. This situation creates a complicated relationship between online data processing and rights that are intended to preserve privacy and protect personal data.[2]

Children are increasingly becoming the subjects of data collection and processing. Alongside the direct challenges posed by their online activities, there is growing contention over how children are affected by the Internet of Things, connected home appliances, wearable technologies, augmented and virtual reality, and other new devices and applications.[3] Without conducting any further research, it is easy to see how these advances in technology have changed childhood experience. Digital technologies, which are the main components of this evolutionary process, significantly impact multiple areas of their lives including their learning, education, and safety.[4]

The debate continues on whether digital access is a beneficial game-changer for children or can ruin children's development and have other adverse effects. Initial research in this

[2] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review' (2019) London School of Economics and Political Science 3 <http://eprints.lse.ac.uk/id/eprint/101283> accessed 5 February 2020.
[3] Ingrida Milkaite and Eva Lievens 'The Internet of Toys: Playing Games with Children's Data?' in Giovanna Mascheroni and Donell Holloway (eds) *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Smart Play* (Springer 2019) 285; Sonia Livingstone, Giovanna Mascheroni and Elisabeth Staksrud, 'European Research on Children's Internet Use: Assessing the Past and Anticipating the Future' (2017) New Media and Society 2.
[4] Stephane Chaudron, Rosanna Di Gioia and Monica Gemo, 'Young Children (0-8) and Digital Technology: A Qualitative Study Across Europe' (JRC Science of Policy Report 2018) 24.

area indicates that digital technologies have positive impacts such as offering '*great educational benefits for young children's learning of literacy and numeracy skills*' via connected toys,[5] as well as negative impacts such as manipulating children by using profiling techniques.[6] As Simone van der Hof and others noted as technology becomes less and less visible to children, a world that embraces fun and playful activities seems to come to the fore. However, behind these enjoyable activities lie highly advanced business revenue models whose dangers cannot easily be foreseen either by children or the wider community. A hidden world of sophisticated algorithms and self-learning mechanisms fed by children's own personal data profiles them and offers them personalised advertisements and content, including the manipulative acts of hiding advertisements or nudging children to buy through play mechanisms.[7]

Children are particularly targeted because their personal data is so valuable for business operators. Children have increasingly more money to spend, can influence how their parents spend their budget, and will be future customers.[8] The more businesses know about their customers, the more tailor-made products and services they can provide for their consumers.

Digital marketing is blended into children's daily experiences, including their most private spheres, such as social and personal relationships.[9] As children enjoy learning, self-expressing, socialising, playing, and creating through new technologies, they also disclose a tremendous amount of personal information while using these technologies.[10] For that, the European Union (EU) incorporated specific provisions to protect children while benefiting from information communication technologies. Its goal was to protect children by ensuring data controllers and processors would find new, better-equipped solutions that respected their right to privacy and data protection.[11]

---

[5] COST Action IS 1410/EECERA Digital Childhoods SIG, 'Digital Literacy and Young Children: Towards Better Understandings of the Benefits and Challenges of Digital Technologies in Homes and Early Years Settings' (August 2018) 4 <http://digilitey.eu/wp-content/uploads/2018/08/DigiLitEY-and-EECERA-Digital-Childhoods-Policy-Brief.pdf> accessed 15 February 2020.

[6] Simone van der Hof, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, Ton Liefaard, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28(4) The International Journal of Children's Rights 833.

[7] Simone van der Hof, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, Ton Liefaard, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28(4) The International Journal of Children's Rights 833,835.

[8] 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) Wisconsin International Law Journal 101,107.

[9] ibid 108.

[10] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 146.

[11] Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679 [2017] 17/EN WP259, 3.

In order for the collection and processing of data from various devices to be lawful, it must meet the conditions set in Article 6(1) of the General Data Protection Regulation (GDPR).[12] Under Article 6(1)(a), consent is one of the six lawful bases for the processing of personal data.[13] While the EU's previous measure the Data Protection Directive[14] did not distinguish between children's and adults' consent in relation to data processing, the GDPR builds another layer to protect children and separately regulates the processing of their personal data since by nature they are considered more vulnerable.[15]

In light of the above, this article examines the parameters imposed by the GDPR for processing children's personal data. It briefly examines the notion of consent, before analysing in detail the specific conditions that need to be fulfilled for this processing to be lawful, including the area of parental authorisation for under-age children. This analysis sheds light on whether these provisions are sufficient to protect children or whether they could even inadvertently increase their risks either immediately or in the long term. The article's main objective is to evaluate the concept of *''consent''* as altered and adapted to children, which was originally adopted to the structure of technology intended for adults' use. Furthermore, this article also seeks to analyse whether the requirements for obtaining children's consent can actually protect those who have not developed the capacity to make an informed decision. These requirements are assessed in comparison to those in force for adults, with a detailed exploration of the implications for users who are not yet mature enough to understand and/or negotiate the content presented via information communication technologies.

2. Setting the Scene – Data Processing and its Impact

As briefly mentioned in the introduction, new devices and applications provide seemingly endless opportunities for children, whether they are used for entertainment, enjoyment, educational or self-development purposes.

Internet access has expanded so rapidly, by 2016, nearly 99% of UK households with children had an Internet connection in the UK while across the EU 93% of individuals aged 16-19 years use the Internet every day.[16] The highest computer use rate on a daily basis among children in the EU is found in Czechia, Estonia (90 %), followed by Poland and

[12] 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 [2016] L 119/1.
[13] Article 6 of the General Data Protection Regulation.
[14] 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 (The Data Protection Directive).
[15] Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679 [2017] 17/EN WP259, 23.
[16] Eurostat Statistics Explained, 'Being Young in Europe Today – Digital World' (July 2020) <https://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world#Youth_online:_a_way_of_life> accessed 5 August 2020.

Slovakia (89 %).[17] Globally, as per UNICEF, 175,000 children access Internet for the first time every day. One in three Internet users is a child.[18] As more children go online and disclose information at an increasing rate, the risks of privacy invasions and violations of data protection rise enormously.

As children increasingly have access to the Internet, it is easier for firms to interact with them, collect information about them or present them specific information (including advertisements). Before the digital revolution, it was impossible to target children with personalised advertisements via traditional media sources, and children were unlikely to disclose sensitive information unintentionally while lacking without adult supervision.[19] However, right now, especially due to hybrid ownership of devices such as smart dolls, companies can collect and process information while influencing children by controlling the doll, as it was the case for the smart doll Hello Barbie.[20]

The relationship between buyer and business does not end once the device is purchased because of the hybrid ownership of smart devices. Although the buyer might own the physical device, seller can still control it because of its network connection and interactive features. Despite resembling traditional toys, smart toys are digitally connected devices capable of collecting information from the child (or any other person) and sending it over for analysis.[21] Smart toys can be designed to generate information, such as detecting developmental delays or disorders in children. Although the appearance of the toy itself might have remained the same, unprecedented results can be obtained because of their potential to collect and process data.[22]

Another example is smart home assistants, which stay in stand-by-mode until they are activated via specific commands to help the person who is interacting with them. Although they may not be intended for use by children, many children use these devices.[23] Such

---

[17] ibid.

[18] UNICEF, 'The State of the World's Children 2017 – Children in a Digital World' (Germain Ake and Ernest Califra December 2017) <https://www.unicef.org/sowc2017/?utm_campaign=SOWC+English+&utm_medium=bitly&utm_source=Media> accessed 6 March 2020.

[19] Ingrid Lambrecht, Valerie Verdoodt and Jasper Bellon, 'Platforms and Commercial Communications Aimed at Children: A Playground Under Legislative Reform?' (2018) 32(1) International Review of Law, Computers & Technology 58,59.

[20] Esther Keymolen and Simone van der Hof, 'Can I Still Trust You, My Dear Doll? A Philosophical and Legal Exploration of Smart Toys and Trust' (2019) 4(2) Journal of Cyber Policy 143.

[21] ibid 144.

[22] Diego Rivera, Antonio Garcia, Bernardo Alarcos, Juan R Velasco, Jose Eugenio Ortega and Isaias Martinez-Yelmo, 'Smart Toys Designed for Detecting Developmental Delays' (2016) 16(11) Sensors (Basel). A study has been conducted to determine developmental delays in children using smart toys by observing 'the motion pattern while the child was moving the smart cubes'. Variables such as time of activity, speed, shaking data, accuracy of the alignment of smart cubes in the tower were processed to generate an outcome regarding developmental delays in children.

[23] Ingrida Milkaite and Eva Lievens 'The Internet of Toys: Playing Games with Children's Data?' in Giovanna Mascheroni and Donell Holloway (eds) *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Smart Play* (Springer 2019) 292.

devices can listen and record voices and conversations, collect users' location and gather other types of metadata.

Of course, it is right to celebrate the positive aspects of smart devices. They offer children a flexible learning environment,[24] access to information about diverse subjects from health to education, and access to employment opportunities.[25] However, to gain these unquestionable benefits from both private and public organisations, children disclose information about themselves. This may be done intentionally or unintentionally and the data may be personal or non-personal but few will have any real awareness of the process or the implications. With the merging of the physical and digital environment, the world has become *'data-intensive, hyperconnected and commercial'*.[26] Even people who do not knowingly use online service are frequently connected to the Internet through smart devices that constantly gather information of all kinds. The real value of data collected on this vast scale lies in the analysis of different types of data and the developed decision-making systems based on sophisticated algorithms.[27]

Very broadly speaking, personal data of high social, economic and political value[28] can be grouped under three broad categories[29]:

(i) data given: the data directly provided by individuals such as responses to a survey (for example when users fill in their name, age or address on forms or surveys).
(ii) data observed: the data generally unknowingly recorded using tracking technologies or sensors (behavioural data, such as cookies, facial recognition, location tracking application).
(iii) data derived or inferred: the data generated from analysis of data given and data observed. It can be possibly linked with various other data sets.

---

[24] ibid 285-286.
[25] Urs Gasser and Sandra Cortesi, 'Children's Rights and Digital Technologies: Introduction to the Discourse and Some Meta-Observation' in M. Ruck, M. Peterson-Badali & M. Freeman (eds) *Handbook of Children's Rights: Global and Multidisciplinary Perspectives* (Taylor & Francis Berkman Center Research Publication No. 2016-7) 7 (forthcoming).
[26] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review' (2019) London School of Economics and Political Science 16 <http://eprints.lse.ac.uk/id/eprint/101283> accessed 5 February 2020.
[27] Sarah Eskens, Jelte Timmer, Linda Kool and Rinie van Est, 'Beyond Control: Exploratory Study on the Discourse in Silicon Valley About Consumer Privacy in the Internet of Things' (Den Haag: Rathenau Instituut 2016) 20.
[28] Simone van der Hof, *Children and Data Protection From the Perspective of Children's Rights – Some Difficult Dilemmas Under the General Data Protection Regulation* (Wolters Kluwer 2018) 1.
[29] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' [2017] 17/EN (WP251rev.01, 6 February 2018) 8.

> The outcome is usually generated by complex algorithms and profiling techniques (such as credit scores).[30]

As technologies and processing techniques develop, data observed and derived has become the norm rather than the exception. Indeed, analysis of inferred data and the use of profiling techniques '*now constitute the core business model of many digital companies*'.[31] Profiling, also known as classification, is among the most effective methods for dealing with information overload. This is a key technique for finding correlations in data sets in order to identify and/or represent an individual or a particular group. It can individuate an individual, or classify them as a member of a virtually created group.[32] Although data is collected for a purpose, it is processed to classify and categorise people beyond purpose limitation principle to intervene in their future.[33]

Most users remain unaware of scale on which data is now being collected, processed and analysed. It is also hard for individuals and especially for children to understand the risks posed by data harvesting and profiling. Predicting the possible outcome is virtually impossible given the number of data sets being analysed and the complexity of the process. For instance, Facebook's news feed (where it shares pictures, links and updates about other member friends of the user) uses close to 100,000 individual weights[34] simply to decide on behalf of users which content the user will see. Various factors, including affinity, weights, and time decay, are used to determine an individual's news feed ranking[35] and to algorithmically determine the best posts from a large story pool to show a particular user.[36]

---

[30] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review' (2019) London School of Economics and Political Science 16 <http://eprints.lse.ac.uk/id/eprint/101283> accessed 5 February 2020.

[31] Mariya Stoilva, Rishita Nandagiri and Sonia Livingstone, 'Children's Understanding of Personal Data and Privacy Online – A systematic Evidence Mapping' [2019] Information. Communication & Society.

[32] Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' (2016) 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728717&download=yes> 3 February 2017; Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt 2013).

[33] Council of Europe Parliamentary Assembly, 'Committee on Culture, Science, Education and Media, 'Technological Convergence, Artificial Intelligence and Human Rights' Doc 14432 19 October 2017, 9.

[34] Lars Backstorm's statement, who is the engineering manager for news feed raking at Facebook: Matt McGee, 'Edge Rank is Dead: Facebook's News Feed Algorithm Now has Close to 100K Weights Factor' (*Marketing Land,* 16 August 2013) <https://marketingland.com/edgerank-is-dead-facebooks-news-feed-algorithm-now-has-close-to-100k-weight-factors-55908> accessed 1 May 2017.

[35] Matt McGee, 'Edge Rank is Dead: Facebook's News Feed Algorithm Now has Close to 100K Weights Factor' (*Marketing Land,* 16 August 2013) < https://marketingland.com/edgerank-is-dead-facebooks-news-feed-algorithm-now-has-close-to-100k-weight-factors-55908 > accessed 1 May 2017.

[36] Motahhare Eslami and others, 'I Always Assumed that I wasn't Really that Close to [Her]': Reasoning about Invisible Algorithms in News Feeds' (Conference: 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, April 2015) 153, 154.

The overall picture grows ever more complicated[37] as information has gone largely unrecorded over the course of many years is recorded, analysed and linked via Big Data and algorithms increasingly with the use of artificial intelligence and machine learning. By this means, data is monetised and has an economic value.[38] Equally concerning is that opting out of the collection of a specific type of data does not prevent companies trying to find the missing information using data aggregation and data linkage methods. For instance, people's intimate traits, like their sexual preferences, could also be identified by algorithms using facial images even if the data subject did not disclose his/her sexual orientation.

In one study, an algorithm shown a single image of a person was able to identify homosexual and heterosexual men with 81% and 71% accuracy for women, rising to 91% and 83% respectively, when five images were given for each person.[39] Another study looking at the use in smartphones of accelerometers, which measure speed, bumps, movement and vibration, found that if one user in the vehicle disclosed his/her location information, the identical pattern of the movements could disclose the location of a second user who had chosen to keep this information private. In other words, linking and combining both users' datasets would unintentionally disclose the second user's location data since they would have the same measures.[40] Certain sensitive information can also be revealed via the consent of other people in the same artificial group, potentially rendering them open to discrimination. Thus, even if an individual does not disclose a specific type of information, data processing techniques may be able to infer based on other information and fill in that blank that has been intentionally left out.

It is also hugely concerning that inferred data may be inaccurate because such data is based on correlations[41] and yet in most cases remains unavailable to data subjects. This combination of circumstances potentially leaves individuals unable to exercise their rights, even if they suffer unfair and discriminatory consequences. It is important to understand *'the power of algorithmic processing comes not from efficiencies, but rather the emergent*

---

[37] Matt McGee, 'Edge Rank is Dead: Facebook's News Feed Algorithm Now has Close to 100K Weights Factor' (*Marketing Land,* 16 August 2013) <https://marketingland.com/edgerank-is-dead-facebooks-news-feed-algorithm-now-has-close-to-100k-weight-factors-55908> accessed 1 May 2017.

[38] Mariya Stoilva, Rishita Nandagiri and Sonia Livingstone, 'Children's Understanding of Personal Data and Privacy Online – A systematic Evidence Mapping' [2019] Information. Communication & Society.

[39] Yilun Wang and Michal Kosinski, 'Deep Neural Networks are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images' (2018) 114(2) Innovations in Social Psychology 246,246.

[40] Scott R. Peppet, 'Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85,131.

[41] Simone van der Hof, *Children and Data Protection From the Perspective of Children's Rights – Some Difficult Dilemmas Under the General Data Protection Regulation* (Wolters Kluwer 2018) 6-7.

results that the system provides.''[42] In that regard, children could be at greater risk with respect to how their data is being used rather than if their personal data is being collected.

Profiling children by collecting and processing their personal data may also undermine their freedom to explore through *''play''* since play data are personal data that can be linked with their physio-physical state[43] and can be recorded, for instance through smart toys. This can critically affect the way they interact and make decisions.[44]

Indeed, profiling and automated decision-making can have permanent far-reaching negative effects on children[45] since they can be used to blacklist them, or to offer them or withhold them from certain products or services.[46] Children are very unlikely to be aware that specific data, whether disclosed or tracked by the data controller could place them in certain groups. For instance, few would suspect that hypothetically clicking 'like' on a particular product such as on curly fries on a social media platform would be used by data processors to indicate their intelligence or race.[47]

Although data subjects – in theory at least – are given information on the purpose of processing for over data collection practices, most of the time they cannot foresee the final outcomes, given the nonintuitive link between the input data and the outcome of processing once Big Data analytics and technologies like AI have come into play.[48] Even the most innocent groupings such as dog ownership can have harmful consequences that

---

[42] LSE, 'The Limits of Parental Consent in an Algorithmic World' (28 November 2016) <https://blogs.lse.ac.uk/medialse/2016/11/28/the-limits-of-parental-consent-in-an-algorithmic-world/> accessed 7 March 2020.

[43] Stéphane Chaudron Rosanna Di Gioia Monica Gemo, Donell Holloway Jackie Marsh Giovanna Mascheroni Jochen Peter, Dylan Yamada-Rice, 'Kaleidoscope on the Internet of Toys' (European Commission JRC Technical Reports 2017) 11-12; Article 31 of the UNCRC; Plat data 'refers to unstructured, informal activities of children that are not controlled by adults'. Further information can be found at: Simone van der Hof, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, Ton Liefaard, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28(4) The International Journal of Children's Rights 833,836

[44] Valerie Verdoodt, 'Children's Rights and Advertising Literacy in the Digital Era: Towards and Empowering Regulatory Framework for Commercial Communication' (PhD Thesis KU Leuven 2018) 102.

[45] Simone van der Hof, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, Ton Liefaard, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28(4) The International Journal of Children's Rights 833,834-836.

[46] ibid 836.

[47] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 146,188.

[48] Sandra Wachter, 'Artificial Intelligence: GDPR and Beyond – Dr Sandra Wachter, University of Oxford' (3 April 2018) <https://www.youtube.com/watch?v=7pibisWRncY> accessed 9 March 2019; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 75.

cannot be foreseen.[49] People who own dogs could be categorised in a way that could restrict them being offered certain services. In other cases, the sophisticated, real-time, data processing methods used for profiling open a window to individuals' deeper selves that even they might not be aware of.[50]

3. Children's Rights to Privacy and Data Protection at International and EU Level

The large-scale collection, processing and analysis of personal data clearly has serious implications for the human rights of data subjects of all ages. While, human rights are universal, applying equally to adults and children, children merit special protection because of their particular characteristics, and as a result they hold specific rights that apply only to them.[51] Children concurrently require special attention and protection because, they are born in a biological state of dependence on their parents unable to survive unless they are cared for. Secondly, at the beginning of their lives, they cannot make informed decisions for themselves due to their lack of capacity. Nevertheless, their cognitive performance generally evolves, and their capacity matures. Indeed, the opportunity to practice decision-making is a key part of their successful transition to adulthood.[52]

European law governing the rights of the children is '*largely based on the United Nations Convention on the Rights of the Child (UNCRC)*'.[53] The UNCRC is an inspiring document that establishes the minimum standards all children should experience[54] and whose principles bear great importance in the EU. The UNCRC defines child as '*every human being below the age of 18 years unless under the law applicable to the child, majority is attained earlier*'.[55]

---

[49] Sandra Watcher, 'Algorithms Drive Online Discrimination, Academic Warns' (Financial Times 12 December 2019) < https://www.ft.com/content/bc959e8c-1b67-11ea-97df-cc63de1d73f4> accessed 9 March 2020.

[50] Simone van der Hof had explained in one of her conference that once her Facebook data was processed, the outcome had shown that she had a high score for openness and extraversion. Although falling under these categories could sound pleasant, this outcome may also indicate potential risk-taking behaviour in her career decision, which might affect her hiring process. Simone van der Hof, '2015 Identity Conference' (YouTube, 31 May 2015) <https://www.youtube.com/watch?v=UtuwvgafAYk> accessed 25 January 2021.

[51] UNICEF, 'The Rights of Every Child' <https://www.unicef.org.uk/child-rights-partners/wp-content/uploads/sites/3/2016/08/CRC_summary_leaflet_Child_Rights_Partners_web_final.pdf> accessed 4 February 2020.

[52] Simone van der Hof, Eva Lievens, Ingrida Milkaite, Valerie Verdoodt, Thijs Hannema, Ton Liefaard, 'The Child's Right to Protection Against Economic Exploitation in the Digital World' (2020) 28(4) The International Journal of Children's Rights 833,846.

[53] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Law Relating to the Rights of the Child* (June 2015) 26 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2015-handbook-european-law-rights-of-the-child_en.pdf> accessed 16 February 2020.

[54] Children and Young People's Commissioner Scotland, 'Incorporating Children's Digital Rights into the UNCRC' <https://www.cypcs.org.uk/ufiles/Incorporating-Digital-Rights.pdf> accessed 3 January 2020.

[55] UN General Assembly, Convention on the Rights of the Child, 20 November 1989, United Nations, Treaty Series Vol. 1577 Article 1.

The UNCRC has four guiding principles that should be taken into consideration when interpreting and implementing it. The four guiding principles of the UNCRC are:

(i) non-discrimination (Article 2),
(ii) the best interests of the child (Article 3),
(iii) survival/right to life and development (Article 6) and
(iv) participation/inclusion (Article 12).[56]

The UNCRC recognises that all children should be treated with dignity; and be protected so they can reach their full potential.[57] It also lays emphasis on the responsibility of adults to act in the best interests of children by taking all necessary measures to protect them from possible harm and ensure their rights are respected.[58]

Clearly, the Convention's overarching objective is to protect children from harm on the basis of their needs. However, its adoption indicates a move from '*a needs-based approach to a rights-based approach*'.[59] The Convention marks a paradigm shift in how society should view children and take responsibility for protecting them[60] seeing them not as mere objects of protection afforded special protection due to their characteristics but as holders of human rights.[61]

In that respect, the UNCRC merges different dimensions recognising on one hand that children are human beings who require protection against harm and special care during their development while stressing on the other the importance of their emancipation and

[56] Child Rights Mainstreaming in Programme and Project Cycle Management, 'CRC and its Four Guiding Principles' <https://europa.eu/capacity4dev/sites/default/files/learning/Child-rights/2.7.html> accessed 7 January 2020.
[57] UNICEF, 'The Rights of Every Child' <https://www.unicef.org.uk/child-rights-partners/wp-content/uploads/sites/3/2016/08/CRC_summary_leaflet_Child_Rights_Partners_web_final.pdf> accessed 4 February 2020.
[58] Janice Richardson, Elizabeth Milovidov and Martin Schmalzried 'Internet Literacy Handbook' (Council of Europe, 2017) 142.
[59] 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) Wisconsin International Law Journal 101.121; A child rights-based approach is underpinned by dignity, non-discrimination, safety, participation, the best interest of the child, interdependence and indivisibility, transparency and accountability.
[60] Council of Europe Strategy for the Rights of the Child (2016-2021), 'Children's Human Rights' (Council of Europe 2016) 7 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8> accessed 9 January 2020; UNICEF, 'Child Rights Partners – Putting Children's Rights at the Heart of Public Services' (Council of Europe 2014) <https://www.unicef.org.uk/child-rights-partners/wp-content/uploads/sites/3/2016/11/Unicef-UK_CRP-information-booklet_14.11.16.pdf> accessed 29 January 2020.
[61] European Union Agency for Fundamental Rights, 'Handbook on European Law Relating to the Rights of the Child' (2015) 17 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2015-handbook-european-law-rights-of-the-child_en.pdf> accessed 25 August 2020.

participation in society if they grow and become independent individuals.[62] It lays emphasis on respecting children's ability to use their rights and freedoms. Furthermore, the UNCRC also requires them to be provided with the necessary instruments to develop themselves[63] physically, emotionally and socially.[64]

The fact that all the Member States of the EU and Council of Europe (CoE) are parties to the UNCRC, gives it a strong foundation. It has become the cornerstone of children's rights and has played a significant role in the development of European law on children's rights.[65] Regulations regarding children are often accompanied by either explicit or implicit reference to the principles of the UNCRC.[66] However, despite the UNCRC's clear intentions to protect children, its principles continue to be challenged and violated every day.[67]

The UNCRC is a shield to protect children and their rights in the physical and virtual world. When the UNCRC was adopted in 1989 and entered into force in 1990, the Internet and online services were not widely used as today. In that regard, the UNCRC has no specific provisions regarding digital services.[68] Nevertheless, its principles apply in the virtual as well as the real world. The resolution adopted by the UN affirmed this stating explicitly, *'… rights that people have offline must also be protected online*'.[69]

This leaves no room for doubt that the UNCRC should be used to interpret regulations in a way that protects children in the collecting, processing and use of their data and that its principles and pillars should guide the stakeholders when implementing relevant laws. This

---

[62] For example, rights in relation to privacy (Article 16), freedom of information and expression (Article 13), play (Article 35), association (Article 15), right to be heard (Article 12). For more detail: Simone van der Hof, *Children and Data Protection From the Perspective of Children's Rights – Some Difficult Dilemmas Under the General Data Protection Regulation* (Wolters Kluwer 2018) 11.

[63] For example, the right to education and development (Article 6 and 28).

[64] Simone van der Hof, *Children and Data Protection From the Perspective of Children's Rights – Some Difficult Dilemmas Under the General Data Protection Regulation* (Wolters Kluwer 2018) 11.

[65] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Law Relating to the Rights of the Child* (June 2015) 26 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-ecthr-2015-handbook-european-law-rights-of-the-child_en.pdf> accessed 16 February 2020.

[66] ibid 27.

[67] Council of Europe Strategy for the Rights of the Child (2016-2021), 'Children's Human Rights' (Council of Europe 2016) 7. 'Not being able to enjoy education, play and share leisure time with others, or being bullied because of one's ethnic origin, sexual orientation or other status' could be given as an example.

[68] Ingrida Milkaite and Eva Lievens, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10(1) European Journal of Law and Technology 2.

[69] United Nation, General Assembly Human Rights Council Thirty-eighth Session' (A/HRC/38/L.10/Rev.1 4 July 2018) <http://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_38_L10_rev1.docx> accessed 24 November 2020; UNESCO, 'Internet Universality R-O-A-M Principles' (09 July 2020) <https://en.unesco.org/news/unesco-welcomes-new-unhrc-resolution-highlighting-online-freedom-expression-and-noting-unesco> accessed 12 January 2020.

holistic approach should also be adopted when implementing if it is to reach its full potential.

In terms of measures specific to Europe, the CoE and the European Union have adopted important tools to ensure that the right to privacy of individuals are protected. The CoE regulates the right to privacy of individuals under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Convention 108 Modernised Convention for the Protection of Individuals with Regard to the Automatic Processing of Individuals Data). The European Union regulates the rights to privacy under Article 7 and personal data protection under Article 8 of the EU Charter of Fundamental Rights (CFREU). Article 24 of the CFREU on the rights of the child also recognises a child's rights to protection and care as necessary for their well-being stating that their best interests must be considered in all actions taken by public and private authorities in relation to them.[70]

The European Union has also adopted a specific provision in the GDPR to address concerns about the processing of children's data, which defines the rights, data processing responsibilities and adequate tools to be applied to personal data processing which are analysed in detail below.[71] However, even before the enforcement of the GDPR, the Article 29 Working Party[72] provided an opinion in 2009 on the protection of children's personal data, aiming to strengthen children's fundamental rights in the area of data protection since the Data Protection Directive – the GDPR's forerunner, which was in force at the time – lacked any special provisions on protecting children's personal data.[73] Its objective was to strengthen the fundamental rights of the children in regards to data protection.

It is interesting to note that in the US, the Children Privacy Protection Act (COPPA) goes into far greater detail than the GDPR on the subject. It provides specific examples and methods for obtaining valid consent.[74] While, the GDPR now offers robust measures to strengthen children's privacy and data protection, it still needs improvement to increase

---

[70] Ingrida Milkaite and Eva Lievens 'The Internet of Toys: Playing Games with Children's Data?' in Giovanna Mascheroni and Donell Holloway (eds) *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Smart Play* (Springer 2019) 287-288.

[71] Ingrida Milkaite and Eva Lievens 'The Internet of Toys: Playing Games with Children's Data?' in Giovanna Mascheroni and Donell Holloway (eds) *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Smart Play* (Springer 2019) 288.

[72] Article 29 Working Party was an independent authority established under the previous Data Protection Directive. It had issued many recommendations and guidelines in relation to privacy and data protection matters until 25 May 2018. Although the documents issued by the Article 29 Working Party were not binding and only had advisory status, they greatly influenced regulators and stakeholders. The relevant recommendations and guidelines have shed light on how to implement the Directive's provisions.

[73] Article 29 Data Protection Working Party Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools [2009] 17/EN 398/09/EN WP 160, 3.

[74] Valeria Verdoodt, Damian Clifford, Eva Lievens, 'Toying with Children's Emotions, the New Game in Town? The legality of Advergames in the EU' (2016) 32(4) Computer Law & Security Review 599, 609-612.

transparency and provide control over personal information, creating an opportunity to reflect and recalibrate the current principles and their implementation in practice.

4. The Notion of Consent for Data Collection and Data Processing

Consent is a crucial mechanism in today's hyper-connected world. Its ultimate goal is to entitle individuals to maintain control over their personal information and therefore over their digital selves.[75] The basic notion behind consent is that individual users control the collection and processing of their own personal data, deciding what type of data can be collected and how it can be used. Consent cements the principle that people are autonomous individuals who should have control over their own lives.[76] As Simone van der Hof argues, allowing individuals to determine their own destiny by making their own decisions marks a shift from a paternalistic approach to a rights-based approach.[77]

Article 8 of the European Convention of Human Rights and Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union underlines the crucial role of consent.[78] Consent is among the most widely used methods to ensure data processing is lawful. It has a significant role in our society. However, whether it fulfils its purpose is questionable. All too often, mechanisms intended to provide meaningful control over personal information has become hollow tick box exercises. New technology and processing techniques that do not rely on direct consent only increase this risk. Due to the contradicting nature of law and technology, data subjects who already show inconsistency between their privacy and actual behaviour are expected to have control through consent mechanisms without understanding the vast number of uses to which it can be put – and certainly unable to imagine how it could potentially be used against them in future.

The effectiveness of informed consent mechanisms has been challenged from technological,[79] legal, social, and behavioural perspectives. The process fails for several reasons, including people's lack of awareness of the data processing itself, or its risks; a lack of choice being clearly offered; user's failure to understand long, vague or technically

---

[75] 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) Wisconsin International Law Journal 101,128.
[76] 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) Wisconsin International Law Journal 101,110.
[77] ibid.
[78] Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679 [2017] 17/EN WP259, 3.
[79] Hidden placement of tags that collect and process personal data; no interactive screen or adequate user interface to permit consent to be given; sharing same connected device such as Alexa or Nest; multi-layered structure of the IoT can be given as examples. Ricardo Neisse, Gianmarco Baldini, Gary Steri and Vincent Mahieu, 'Informed Consent in Internet of Things: The Case Study of Cooperative Intelligent Transport Systems' (23rd International Conference on Telecommunications, Ispra, Italy, 2016) 1,41-42; The Future of Privacy Forum, Christopher Wolf and Jules Polonetsky, 'An Updated Privacy Paradigm for the 'Internet of Things'' <https://fpf.org/wp-content/uploads/Wolfand-Polonetsky-An-Updated-Privacy-Paradigm-for-the-'Internet-of-Things'-11-19-2013.pdf> accessed 27 January 2018.

worded privacy policies; and manipulation by designers that encourages users to complete their primary task, for example by habituating users to granting quick approval.[80]

As per Article 4(11) of the GDPR consent is defined as *'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'*[81] The basic notion behind consent is that we control the collection and processing of our own personal data. It means that we decide what type of data can be collected and for what specific purpose it is permitted to be processed. This approach has been supported by the right to *'self-determination'*, which has been discussed under the Population Census decision in 1983 and influenced the data protection laws in the European Union.[82] Although steps have been taken to strengthen the rights of the individuals and to force developers to ensure new technologies adhere to privacy and data protection principles, the idea that individuals are still in control of their personal data in an age of surveillance capitalism is still considered an illusion.[83] This is due in part to the amount of data now being collected especially by smart devices and the use of sophisticated algorithms (that are considered as black boxes).

Although a detailed analysis of consent mechanism as envisaged under the GDPR is beyond the scope of this article, it is worth noting that consent is considered valid only if the sub-principles of consent[84] along with the data protection principles, are fulfilled during the data collection and throughout the life cycle of data processing.

5. Children's Legal Capacity to Consent

International treaties, the Charter, and EU secondary laws and national laws entitle individuals with certain rights and obligations. However, children are not always entitled to the same rights. Most of the time they are dependent on the decisions of their parents.[85] By this means, the law aims to protect children and ensure that the decisions given on their behalf are made taking into consideration their best interest. Individuals need to reach a minimum age to be entitled to exercise certain rights, such as the right to marry or to seek

[80] Rainer Bohme and Stefan Kopsell, 'Trained to Accept? A Field Experiment on Consent Dialogs' (2010) 4 Conference on Human Factors in Computing Systems – Proceedings 2403,2403.
[81] Article 4 of the General Data Protection Regulation
[82] Simone van der Hof, *Children and Data Protection From the Perspective of Children's Rights – Some Difficult Dilemmas Under the General Data Protection Regulation* (Wolters Kluwer 2018) 11-12.
[83] ibid.
[84] In order to ensure compliance, each component stipulated under the definition of consent should be analysed in light of the factual basis of each case of processing. The definition of consent as set out in the GDPR can be divided into four concepts. It must be: (i) freely given; (ii) specific; (iii) informed; and (iv) an unambiguous indication of data subject's wishes. Further information can be found at EDPB, 'Guidelines 05/2020h on Consent under Regulation 2016/679 (Version 1.1, 4May 2020).
[85] European Union Agency For Fundamental Rights 'Mapping Minimum Age Requirements with respect to the Rights of the Child in the EU' <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/background-information> accessed 9 January 2020.

employment.[86] According to the classic and contemporary literature on cognitive process and development, age is a variable often used to explain changes and shifts in children's understanding.[87] However, children's evolving capacities shall be taken into consideration when setting a minimum age for the acquisition of certain rights and loss of certain protections as adopted under the UNCRC.[88]

It is not easy to determine the legal capacity of children to consent to data processing. Similar challenges have been faced in other areas of law as well, such as consumer law or contract law. However, what is unique in this new digital era is that it is even more challenging to know the subjective capacity and the maturity of a child behind the black screen or a device.

From a legal perspective, as explained by Eva Lievens and others *'children (for the most part) defined in terms of chronological age – – and the age threshold selected varies depending on the purpose of the law or policy in question (e.g., consent to sexual activity, consumption of alcohol and tobacco, army enlistment, or leaving school)*'.[89] Participating in the digital world has become a central element in the children's world today. In connection with this new world, defining what a child means and setting a minimum age requirement are crucial for their development and protection. However, taking chronological age to determine the capacity of the child on the basis of the Piagetian Theory that determines the cognitive development of the child would oversimplify the persuasive process. It would also fail to address the risks posed by the advancement of technology and the way it affects our daily lives.[90]

In order to resolve this matter, data protection regulations in the European Union have adopted a flexible age to guide data controllers regarding obtainment of children's consent. As per Article 8(1) of the General Data Protection Regulation, in cases where consent is chosen as the most appropriate mechanism to lawfully process data in relation to information society services offered directly to a child, the processing of personal data of a child is lawful where the child is at least 16 years old. However, Member States may

---

[86] ibid.

[87] Piagetian Theory: Zheng Yan, 'Limited Knowledge and Limited Resources: Children's and Adolescents' Understanding of the Internet' (2009) 30 Journal of Applied Developmental Psychology 103,113; Zheng Yan, 'Age Differences in Children's Understanding of the Complexity of the Internet' (2005) 26(4) Journal of Applied Developmental Psychology 385.

[88] Eva Lievens, Sonia Livingstone, Sharon McLaughlin, Brian O'Neill, and Valerie Verdoodt, 'Children's Rights and Digital Technologies' in Ton Liefaard, and Ursula Kilkelly (eds.) *International Human Rights of Children - International Human Rights* (Springer 2019) 487-491.

[89] Eva Lievens, Sonia Livingstone, Sharon McLaughlin, Brian O'Neill, and Valerie Verdoodt, 'Children's Rights and Digital Technologies' in Ton Liefaard, and Ursula Kilkelly (eds.) *International Human Rights of Children - International Human Rights* (Springer 2019) 487-491.

[90] Kathryn C Montgomery, Jeff Chester, Tijana Milosevic, 'Children's Privacy in the Big Data Era: Research Opportunities' (2017) 140(2) Pediatrics 117,119-120.

provide a lower age threshold provided that the lower age limit is not below the age of 13.[91]

6. Child's Consent under the GDPR

Before the advent of the GDPR, the EU Data Protection Directive 95/46/EC had no specific provisions on processing children's personal data, partly because information communication technology (ICT) was at a much earlier stage of development when the Directive came into force. The Internet was still not widely used at homes, and not many people and especially children had access to it.[92] However, *'in 2018, just over three quarters (76 %) of the EU adult population (aged 16-74 years) used the internet on a daily basis (during the three months before being surveyed)'*.[93]

This rapid shift left the Directive lacking sufficient public protection, including in areas of social interaction and technological innovations.[94] Furthermore, when the Directive was negotiated, the focus was more on achieving economic goals and the free flow of information. It was a secondary goal of the regulator to ensure the protection of fundamental human rights along with children's rights.[95] However, as technology developed and many households including children started having regular access to the ICTs, the regulator had to respond. The eventual outcome was Article 8 of the GDPR, which strengthens children's rights and protection when using digital technologies.

Children have only limited legal autonomy[96] perhaps because they may not be fully aware of the possible risks and consequences of data collection and processing.[97] They have specific rights and protections until they reach a certain maturity. Recital 38 of the GDPR also acknowledges this by stating '*children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data*'.

---

[91] Article 8 of the General Data Protection Regulation.
[92] Lina Jasmontaite and Paul de Hert, 'The EU, Children Under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet' (2014) 5(1) International Data Privacy Law 1,3.
[93] Eurostat Statistics Explained, 'Digital Economy and Digital Society Statistics at Regional Level' (2019) <https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_digital_society_statistics_at_regional_level#Internet_use_and_activities> accessed 20 March 2020.
[94] Chiara Bortot, 'Children and Data Protection: Awareness and Effectiveness in a Connected World' (LLM Dissertation, Tilburg University 2018) 6.
[95] Lina Jasmontaite and Paul de Hert, 'The EU, Children Under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet' (2014) 5(1) International Data Privacy Law 3.
[96] ibid 2.
[97] ICO, Children and the GDPR 1 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection themes/children/> accessed 27 February 2020.

It is important to note that while the GDPR sets an age threshold for obtaining consent from children for the collection and processing of their personal data, it does not define what is meant by a *'child*'. Consequently, it is not clear up to when children are entitled to benefit from this unique safeguard mentioned under the GDPR (especially the Recital 38 regarding profiling).[98] It is essential to understand to what extent children are competent or able to understand, process information and make an informed choice. Vivian Hamilton argues that *'general cognitive capacity—i.e., the abilities to process information, understand and reason from facts, and assess and appreciate the nature of a given situation—improves into mid- adolescence''.*[99]

Generally speaking, by the age of sixteen, children's basic cognitive abilities have developed and matured to a certain degree.[100] However, studies have shown that in certain contexts, children are still more likely than adults to misjudge the risks and consequences of their decisions and to engage in risky behaviours[101] – mainly because children put more weight on the benefits they will gain than on the risks they are taking. Moreover, the hidden harmful effects of data collection and processing tend to occur some time after consent is given, weighing the balance of decision in favour of the instant benefits of the service being accessed.

Other evidence can also be found of the complexity of setting age limits in the digital world. One study found that children aged 11-12 had adultlike technical understanding, but a lower level of understanding of societal issues.[102] Even if children do develop both technical and social understanding, studies have also concluded that *'teenagers are inclined to behave impulsively and often do not think about the consequences of their actions before taking them, even in situations involving considerable risk'*.[103] Individuals aged between 13-17 are more likely to take online risks. Craig Andrews and others explain that this could happen possibly because the prefrontal cortex and the necessary skills required to control urges are not fully developed until later on during puberty, which can lead adolescents to make risky decisions.[104]

---

[98] Eva Lievens Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34(2) Computer Law and Security Review 269,271.

[99] Vivian E. Hamilton, 'Immature Citizens and the State' (2010) 2010(4) The Brigham Young University Law Review 1055, 1109.

[100] 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) Wisconsin International Law Journal 101,126.

[101] ibid 126.

Zheng Yan, 'Limited Knowledge and Limited Resources: Children's and Adolescents' Understanding of the Internet' (2009) 30 Journal of Applied Developmental Psychology 103,112-113.

[103] Kathryn C Montgomery, Jeff Chester, Tijana Milosevic, 'Children's Privacy in the Big Data Era: Research Opportunities' (2017) 140(2) Pediatrics 117,119-120.

[104] J Craig Andrews, Kristen L. Walker, and Jeremy Kees, 'Children and Online Privacy Protection: Empowerment from Cognitive Defence Strategies' (2020) 39(2) Journal of Public Policy & Marketing 205,207.

As a result, even children who have developed sufficient technical and social understanding to make appropriate and informed decisions may be vulnerable to making poor choices owing to the unique characteristics of this period of impulsivity. The protection and empowerment of children should be balanced taking into consideration their evolving capacities.[105] Milda Macenaite and Eleni Kosta note that, *'the complexity of setting an age specific competence threshold stems from conceptions of childhood, including the ideas about children's needs and capacities and how they can change with growth, as well as national historical, cultural and social heritage of a particular country and legal system.'*[106]

In order to set an age threshold, regulators must know how children understand privacy, data protection, and the concept of consent in the digital environment. Unfortunately, as stated by Better Internet for Kids (a platform incorporated on behalf of the European Commission to share resources, services and practices for service providers), there is insufficient evidence on '*how children understand consent and when they are able to give it*' meaningfully.[107] Most prior research on consent has focused on medical procedures and health-related matters. However, in these cases, consent is very individual[108] and how it is communicated to children is very different from digital platforms where children often lack a one-on-one relationship with the digital service providers.

Tangentially, it is asserted that more research is needed on the psychology of children in decision-making processes. The multidimensional and complex structure of these processes has to be understood before a fixed age threshold can be agreed.[109] Questions such as how children's understanding of privacy varies depending on their age and maturity level and what is the appropriate age for children to acquire certain rights in the digital environment must be answered before regulators and other relevant stakeholders establish an age threshold in information society services.

Although some studies have focused on children aged of 12-18, not much attention has been given to younger cohorts. Given the lack of robust evidence, Sonia Livingstone and others highlight the difficulties posed in deciding how children of different ages should be

---

[105] Valerie Verdoodt, 'Children's Rights and Advertising Literacy in the Digital Era: Towards and Empowering Regulatory Framework for Commercial Communication' (PhD Thesis KU Leuven 2018) 11-12.

[106] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 146,151.

[107] Better Internet for Kids, 'The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society' (Brussels 2017) 14 <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> accessed 25 April 2020.

[108] ibid.

[109] Better Internet for Kids, 'The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society' (Brussels 2017) 14 <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> accessed 25 April 2020.

grouped, disaggregated, and identified, based on their specific understanding and development. Their study did map the development of children's understanding of privacy[110] concluding that children of different ages had different maturity and understanding levels, again highlighting the complexities in the idea that children can be neatly placed into groups.

There is no magic age when children can be said to have crossed a threshold into full capacity and maturity. Instead, in line with the developments in psychology and as urged by the UN, children should be treated as individuals, taking into consideration their circumstances and evolving capacities as stipulated under the UNCRC.[111]

Given the varying ages at which children mature, it could be even argued that a fixed age threshold is ultimately, arbitrary and subjective. On the other hand, a flexible age threshold would cause vagueness and problems both for businesses and law enforcement officers. Firms cannot be expected to evaluate each child operating a device or computer remotely and decide their capacity on a case by case basis. Ultimately, flexible rules seeking to treat children as individuals by considering their specific understanding level could undermine child protection effort to create genuine problems for business owners seeking to comply.[112]

Nonetheless, in order to comply with the rights-based approach of the UNCRC, businesses should adapt their services to different age groups. This requires them to conduct a balancing act between an overly paternalistic approach that imposes too many restrictions, and an under-regulated approach that offers too little protection. In addition, an empowerment approach could be used to ensure compliance with other rights such as self-determination and the right to development.

Although the GDPR does not explicitly define what a child means, it still enforces special protection for children under the age threshold, which also includes everyone under the age of 18, in line with the UNCRC definition. This problem is not new. Setting a fixed age from which young children will have a legal capacity has been an issue in many areas of law. A fixed age provides legal certainty for stakeholders, which strengthens the laws.[113] Yet, the GDPR has a fixed age for young children to provide consent for information society services at the age of 16.

However, as stated, Member States are allowed to lower this threshold. For instance, in the UK, if a business operator is relying on consent mechanism as a lawful basis for

---

[110] Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri, 'Children's Data and Privacy Online: Growing up in a Digital Age. An Evidence Review' (2019) London School of Economics and Political Science 18 <http://eprints.lse.ac.uk/id/eprint/101283> accessed 5 February 2020.

[111] ibid.

[112] Julia Hornle, Ian Walden, John Angel, *Research Report, Marketing to Children and the Internet Data Collection From Children by Website Operators* (The Institute of Computer and Communications Law) 11.

[113] ibid 12.

processing, children need to be 13 years or over. For younger children, the consent of the holder of the parental responsibility is required, unless the business operator provides a preventative or counselling service.[114] Nevertheless, the age threshold applies if the sub-principles of the provision are present in each case. Each criterion is analysed in detail below.

7. Information Society Services

The Article 8(1) of the GDPR on child's consent states that if one of the conditions laid down under Article 6(1) applies as a lawful basis for processing in relation to the offer of *'information society services'* offered *'directly to a child'*, processing on this basis is deemed lawful only if the child is at least 16 years old. The term *'information society services'* covers 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.[115] As stated by the Information Commissioner's Office (ICO), most online services are information society services. Websites, applications, search engines, online contents such as on-demand video services and music, online games, and connected toys can be given as examples of information society services. Broadcasts or radio transmissions offered through general broadcast instead of on-demand is excluded[116] even if the channel is available online, as it is being shared with a general audience.[117] While payment is frequently involved it is not required for the services to fall within the scope of Article 8(1) of the GDPR. Services financed by advertising are also considered as information society services[118] although, it is questionable whether those provided by non-profit or educational organisations are included.[119]

The European Court of Justice has evaluated the scope of remuneration in several cases. For example, in *Belgium v Humbel* case the court noted *'the essential characteristic of remuneration thus lies in the fact that it constitutes consideration for the service in question, and is normally agreed upon between the provider and the recipient of the*

[114] ICO, Children and the GDPR 1 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 27 February 2020.
[115] 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 [2015] OJ L 241/1.
[116] ICO, Children and the GDPR 1 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 27 February 2020.
[117] ICO, 'Age Appropriate Design: A Code of Practice for Online Services. Consultation Document' (2 September 2020) 17.
[118] Valerie Verdoodt, 'Children's Rights and Advertising Literacy in the Digital Era: Towards and Empowering Regulatory Framework for Commercial Communication' (PhD Thesis KU Leuven 2018) 178-179.
[119] Eva Lievens Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34(2) Computer Law and Security Review 269,272; Valerie Verdoodt, 'Children's Rights and Advertising Literacy in the Digital Era: Towards and Empowering Regulatory Framework for Commercial Communication' (PhD Thesis KU Leuven 2018) 178-179.

service'.[120] However, in another case, the Court of Justice held that remuneration could come from a third party rather than the recipient of the service. The Court stated that it was enough that the advertisers paid broadcasters for the service.[121] Moreover, the Court of Justice has also ruled that even non-profit organisations fall under the abovementioned definition *'when there is an 'element of chance' inherent in return or when the service is of recreational or sporting nature, within this interpretation'*.[122] Given this wide definition of remuneration, the meaning of information society services has also been interpreted very broadly, drawing in a wide range of activities and online services.[123]

8. Services Offered Directly to Children

The second essential principle of Article 8(1) of the GDPR is that the information society service has been offered directly to children. If an information society service is offered to children through an intermediary, such as education centres/schools, then it does not fall within the scope of services *'offered directly to children.'* In that case, the said article does not apply. All other services that clearly indicates that they are for children or are targeted at children are deemed to being offered directly to children and therefore fall within its scope.[124]

The question then arises about services that are not specifically targeted at any age group, and the problems this poses for enforcement officers trying to decide whether a child is being targeted. YouTube provides a good example of this complexity: does the article apply only to YouTube Kids, which specifically targets children; or does it cover YouTube content which has a general audience but is heavily used by children?[125] Eva Lievens and Valerie Verdoodt highlighted the need to consider the protection that Article 8(1) of the GDPR was designed to offer, arguing that this would be undermined if children's daily use of digital services was excluded.[126]

The ICO considers that business operators are targeting children if their services are available to everyone without any age limit, or if any age limit that is in place allows access to children aged under 18.[127] All firms, regardless of their intended target audience should evaluate whether their online services will appeal to children and are likely to be accessed

---

[120] Case 263/86 *Belgian State v René Humbel and Marie-Thérèse Edel* [1988] ECLI 5383 para 17.
[121] Case 352/85 *Bond van Adverteerders and others v The Netherlands State Case* [1988] ECLI 2124 para 16.
[122] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 146,171.
[123] ibid.
[124] ICO, Children and the GDPR 24 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 27 February 2020.
[125] Eva Lievens Valerie Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation' (2018) 34(2) Computer Law and Security Review 269,272.
[126] ibid 272.
[127] ICO, Children and the GDPR 24 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 27 February 2020.

by them, if necessary by conducting market research or assessing user behaviour. This information will guide them in whether they need to comply with the relevant provisions on the processing children's personal data. If the initial evaluation indicates an absence of interest or access by children, but subsequent evidence shows this has changed, firms must still comply with the law – even if the number of children involved represents a small proportion of their overall audience.[128] Returning to the YouTube example, while the site considers itself to be aimed at general audience, several channel owners have informed YouTube they would prepare content specifically for children and YouTube's classification system identifies some content as intended for children. Furthermore, YouTube has shown to be among most popular websites among children aged between 2-12.[129]

Clearly, exempting general audience websites from the provisions relating to children undermines the protective aims of the GDPR. Similar concerns exist about smart devices that are not specifically intended for children, but collect their data regardless – either when children interact with them or through background functions. In 2019, Amazon was sued in the US over child recordings made during performing tasks such as playing music, telling jokes, or, helping with maths questions: no valid consent had been gained either from the child or the parent.[130]

If a business genuinely believes that only adults are likely to access its services, the articles regarding children will not apply. However, the business owner will need to be able to demonstrate the facts on which this evaluation is based. As the ICO suggests, operators could rely on market surveys, the content of their service, or tailored solutions that prevent children from accessing their services.[131]

9. Territorial Application of Age-Limit

Another essential question regarding the application and scope of Article 8(1) of the GDPR is the age limit that companies have to comply with when designing their products and services. Do data controllers only need to take into account laws of the Member State where their company is established or should they comply with the differing national laws in each Member States?

---

[128] ICO, 'Age Appropriate Design: A Code of Practice for Online Services. Consultation Document' (2 September 2020) 13-14.
[129] FTC, 'Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law' (4 September 2019) <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> accessed 10 February 2021.
[130] Zak Doffman, 'Amazon Slammed for Putting Kids at Risk with 'Blatant Violation of Privacy Laws' (*Forbes*, 9 May 2019) <https://www.forbes.com/sites/zakdoffman/2019/05/09/amazons-echo-dot-kids-accused-of-violating-privacy-laws-and-putting-kids-at-risk/?sh=322ead4a7e5a> accessed 25 January 2021; Ingrida Milkaite and Eva Lievens, 'Child-Friendly Transparency of Data Processing in the EU: from Legal Requirements to Platform Policies' (2020) 14(1) Journal of Children and Media 5,6.
[131] ICO, 'Age Appropriate Design: A Code of Practice for Online Services. Consultation Document' (2 September 2020) 14.

Although the GDPR aims for harmonisation among the Member States when providing cross-border services, each Member State is free to set lower age than 16 provided that it is not lower than 13. Determination of the age of consent is closely related to the civil law rules of each national jurisdiction. Therefore, Member States were given the flexibility to determine the age of capacity to consent to data processing.[132] However, the specific reasoning behind each national decision is not supported by evidence-based data.

To add the complexity of the debate, the GDPR's own age threshold of 16 does not take into account the individual level of maturity of the child.[133] Children have different capacities and reach key developmental stages at different ages because of factors such as differing levels of education, access to technology, or wealth,[134] but the digital realm has little scope for assessing them individually. It is not realistic or feasible to expect data controllers and processors to make such individual assessments when they cannot have one-to-one relationships with the subjects. However, service providers should still take into consideration the different age groups they are targeting, so they can ensure they implement appropriate measures and safeguards for children of that age group.

Despite the acceptance of differences in the maturity level of individual children of the same age, it is still not possible to explain the reasons for wide differences in the legal age of consent in different EU countries.[135] For instance – children in Denmark and the Netherlands have three years' difference between the age of legal capacity. This patchwork of ages and national laws means the businesses must be aware of the age limit in each country and determine whether they need to comply with each of them. Nevertheless, according to the Article 29 Working Party, Member States shall consider the best interest of the child while determining which national law to be complied with.[136]

Member States have adopted different age limits under their national laws for the age of digital consent. Belgium, Denmark, Latvia, Estonia, Finland, Malta, Portugal, Sweden and the UK have adopted the age of 13 as the age of consent. Austria, Bulgaria, Cyprus, Italy, Lithuania and Spain have adopted the age of 14 as the age of consent. The age limit is set as 15 in Czech Republic, France, Greece and Slovenia whereas children in Croatia, Germany,

---

[132] Better Internet for Kids, 'The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society' (Brussels 2017) <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> accessed 25 July 2020.

[133] Eva Lievens, Sonia Livingstone, Sharon McLaughlin, Brian O'Neill, and Valerie Verdoodt, 'Children's Rights and Digital Technologies' in Ton Liefaard, and Ursula Kilkelly (eds.) *International Human Rights of Children - International Human Rights* (Springer 2019) 487-494.

[134] Wouter Vandenhole, 'Children's Rights and Sustainable Development from a 'Law and Development' Perspective in Claire Fenton-Glynn (ed) *Children's Rights and Sustainable Development: Interpreting the UNCRC for Future Generations* (Cambridge 2019) 12.

[135] Eva Lievens and Simone van der Hof, '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 33,34.

[136] Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679 [2017] 17/EN WP259, 25.

Hungary, Ireland, Slovakia, Poland, Netherlands, Luxemburg and Romania have to wait until they are 16 to be able to give consent.[137]

As Karolina Mojzesowicz explains, several potential options are on the table to solve the problem of territorial application.

- Country of Establishment: Data controller would have to apply the age threshold that the company was established. In practice, this would mean data controller established in Member States X where the digital age of consent is 13 and providing services to children located in Member State Y, where the age limit is 14, would apply the threshold of 13 based on the country of establishment principle. Germany and the Netherlands have indicated that this is their preferred solution.[138]
- Sole Purpose of Circumventing: If a business has been incorporated in Member State X to deliberately avoid the age limit of the other Member State Y, which the company specifically targets the residents of that Member State Y, the age threshold envisaged under the regulations of Member State Y should apply.
- Country of Residence: Some Member States require their own age threshold to be applied when targeting children of that Member State. For example, a service provider established in Member State X but targeting children in Member State Y would be expected to comply with the laws of Member State Y.[139] The UK[140] expects service providers established anywhere in the EU and around the world to comply with the UK age limit when they collect and process the personal information of UK residents.[141] This approach may require service providers ask children using their services to declare which country they are in.[142]

Moreover, it is acknowledged in the recent Communication of the European Commission published in June 2020, that an approach on providing room for manoeuvre when

---

[137] Ingrida Milkaite and Eva Lievens, 'The GDPR Child's Age of Consent for Data Processing Across the EU-One Year Later' (Better Internet for Kids, July 2019).

[138] Better Internet for Kids, 'The General Data Protection Regulation and Children's Rights: Questions and Answers for Legislators, DPAs, Industry, Education, Stakeholders and Civil Society' (Brussels 2017) 9 <https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf> accessed 25 April 2020.

[139] ibid.

[140] Although the EU GDPR does no longer applies in the UK due to Brexit, the GDPR has been incorporated into UK data protection law as the UK GDPR. The UK GDPR sits along with the Data Protection Act 2018, which continues to apply. There is only little change in practice, but the core data protection principles, rights and obligations remain the same. Further information available at: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/#doesthe.

[141] ICO, Children and the GDPR 24 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/> accessed 27 February 2020.

[142] ibid.

determining children's legal capacity to consent creates *''uncertainty to children and their parents as to the application of their data protection rights in the Single Market'*.[143] It creates further challenges in conducting business with other states. Therefore, the Commission will explore whether harmonisation of the age child can consent could be achieved.[144]

10. Parental Consent

According to Article 8(1) of the GDPR, if the child is below the age threshold, processing the data of a child will be deemed lawful provided that consent has been given by the holder of parental responsibility. As it is the case under the civil law matters, parental consent or authorisation is a tool used to '*remedy children's lack of legal capacity to enter into a contract*'.[145] When children reach the specific age threshold set by law, the service provider is no longer obliged to obtain parental consent, since this is replaced by the direct consent of the child.

The holder of parental responsibility is not defined under the GDPR; instead this has to be determined by individual Member States.[146] We have to refer to the family law of the relevant Member State in order to determine the holder of parental responsibility. The concept of parental responsibility includes ensuring that children have shelter, food, clothes and access to legal representation if needed, and that decisions about them should take their best interests into account.[147] In most cases, these areas of responsibility rest with children's parents.

However, if parents are deceased or incapable of carrying them out, a guardian may be appointed by the court.[148] If this definition of the holder of parental responsibility is accepted without any limitation, only parents or the legal guardians can authorise the processing of children's personal data. However, this may not always be feasible. Service providers who need parental consent need to take all necessary measures to ensure this comes from the parent or guardian rather than the child. It will not usually be deemed valid

---

[143] Commission, 'Communication from the Commission to the European Parliament and the Council: Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' COM (2020) 264 final 7.
[144] ibid 15.
[145] Lina Jasmontaite and Paul de Hert, 'The EU, Children Under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet' (2014) 5(1) International Data Privacy Law 5.
[146] Rosemary Jay, *Guide to the General Data Protection Regulation* (Sweet & Maxwell 2017) 92.
[147] Children Act 1989.
[148] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 146,176.

if the child can simply click to confirm their parents have agreed to the data to be collected and processed.[149]

A separate issue relates to parents' and guardians' own lack of information. While they are responsible for protecting their children and taking into consideration their best interests[150] they may find it hard in the digital era, to make informed decisions about giving consent for processing of personal data or maintaining control over their children's personal information. For these reasons, most parents either avoid using these services [151] or give consent to each data processing without being aware of the consequences. Although restricting children's access to Internet could protect them from online harms, at the same time it also prevents opportunities by undermining children's self-determination. Restricting them in the digital platforms could also raise issues about the development of their evolving capacities.[152]

It is also important to consider whether parental authorisation is an optimal way to ensure a child's best interest. Parents do not always have a better understanding than their children of how information society services work. They may have greater difficulty than their offspring in understanding new advertising and marketing techniques based on processed data. Complex algorithmic designs and data processing practices may not always make sense to adults either. In that respect, depending on the child's age and level of maturity, adults are not always in a better position and more empowered than children to protect their freedoms and rights.[153]

Indeed, adults face similar issues when it comes to understanding privacy policies and making informed decisions. The understanding level of privacy policies is so low that: *'as Chris Hoofnagle and others found out in their research, 75% of 974 participants of the survey answered correctly 2 or less out of 5 basic questions concerning online privacy knowledge*'.[154] As a result, adults will not necessarily make better-informed decisions than their children. It can be equally tricky for them to understand what kind of data is being collected, how that is being carried out, how it will be processed and used and with whom and for what purpose it will be shared. Thus, relying on parents to ensure children's privacy

[149] Julia Hornle, Ian Walden, John Angel, *Research Report, Marketing to Children and the Internet Data Collection from Children by Website Operators* (The Institute of Computer and Communications Law) 60.
[150] ICO, 'Age Appropriate Design: A Code of Practice for Online Services. Consultation Document' (2 September 2020) 6.
[151] ibid 6.
[152] Valeria Verdoodt, Damian Clifford, Eva Lievens, 'Toying with Children's Emotions, the New Game in Town? The legality of Advergames in the EU' (2016) 32(4) Computer Law & Security Review 599, 612.
[153] Valerie Verdoodt, 'Children's Rights and Advertising Literacy in the Digital Era: Towards and Empowering Regulatory Framework for Commercial Communication' (PhD Thesis KU Leuven 2018) 81.
[154] Jakub Misek, 'Consent to Personal Data Processing' (2014) 8(1) Masaryk University Journal of Law and Technology 69, 77.

and data protection is questionable. There is no evidence that parental authorisation reduces children's exposure to risks in relation to information society services.[155]

11. Reasonable Efforts

As per the second paragraph of Article 8 of the GDPR, service providers are obliged to make reasonable efforts to verify that consent has been given by children or authorised by the holder of parental responsibility, taking into consideration the available technology.[156] Although the GDPR offers no further guidance on what constitutes reasonable efforts in this content, the introduction of COPPA in the US which has been introduced more than 15 years ago, sheds some light on possible ways of considering this matter.

Both the GDPR and COPPA require parental authorisation for processing of the personal data of children below a certain age. The GDPR envisages this limit to be 16 years of age, whereas COPPA requires parental consent to be applied for children below the age of 13.[157] Although COPPA differs from the GDPR, its guidelines and recommendations are useful, as these have been elaborated since it came to force in 1998.

COPPA also regulates online services that are directly offered to children or general audience sites that knowingly collect and process children's personal data.[158] It also lays down specific guidelines and recommendations in relation to putting reasonable efforts into verifying a child's consent and parental authorisation. In this respect, the GDPR could benefit from the existing studies and research conducted in relation to *''reasonable effort''* and adapt them as necessary to match its own principles.

The FTC provides several methods of verifiable consent as follows:

- Providing a form that can be printed, signed and sent back to the business via post, fax or scan
- Requiring the parent to insert a credit card or details of another payment method
- Maintaining a free telephone number
- Operating a video-conference to connect to the parent
- Verifying the identity details of the parent via government-issued ID

---

[155] Sonia Livingstone and Brian O'Neill, 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions' in Simone van der Hof, Bibi van den Berg, Bart Schermer (eds) Minding Minors Wandering the Web: Regulating Online Child Safety (Springer 2014) 19, 30-33.

[156] Ingrida Milkaite and Eva Lievens, 'Children's Rights to Privacy and Data Protection Around the World: Challenges in the Digital Realm' (2019) 10(1) European Journal of Law and Technology.

[157] FTC Jule Brill, 'Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation Ghostery/Hogan Lovells Data Privacy Day' (21 January 2016) 6 <https://www.ftc.gov/system/files/documents/public_statements/910663/160121hoganghostery_dpd.pdf> accessed 6 March 2020.

[158] Commission Implementing Decision EU (2016/1250) of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) 207/1.

- Using facial recognition technology to verify the parent with a photo ID and a second photo submitted by the parent
- Requiring the parent to answer a series of knowledge-based challenging questions that would require the knowledge of a parent to be answered.[159]

Although these ideas are useful, this is not an exhaustive list from which business operators must choose. Instead, the FTC also allows business operators to submit their own method of parental consent for approval.[160] This encourages the development of more advanced solutions that are more effective and in compliance with the relevant laws.[161] In accordance with the dynamics of each product or service, the business operator shall choose or develop the best method to obtain verifiable consent and should be able to demonstrate that reasonable efforts have been made.

Despite the GDPR's lack of a definition of *''reasonable efforts''* it is expected that data protection authorities will provide more guidance and explain to firms to the extent to which their efforts are considered reasonable.[162] Again, this raises fresh complexities. On the one hand, age verification and verifiable parental authorisation are considered as additional layers of protection for children. On the other hand, collecting the data required for age verification and processing excessive personal data of children and their parents itself raises questions about privacy, anonymity, and, freedom of speech.[163] Additionally, this process should be balanced with the principles of data protection regulations such as the purpose limitation principle and data minimisation.

It is also unclear whether a data controller who made reasonable efforts, but nevertheless was fooled by the data subject, resulting in invalid consent, has violated the provisions. Conversely, it also remains uncertain whether a data controller who did not make reasonable efforts but did gain valid consent would be in breach of this provision.[164]

12. Conclusion

Technology and the Internet are great tools that enable children to learn, communicate, socialise and enjoy their spare time.[165] However, technology and the Internet expose

---

[159] FTC, 'Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for your Business' <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#chart> accessed 9 March 2020.

[160] FTC, Complying with COPPA: Frequently Asked Questions <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Verifiable%20Parental> accessed 9 March 2020.

[161] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) 26(2) Information and Communications Technology Law 146,179.

[162] ibid 171.

[163] ibid 179.

[164] Rosemary Jay, *Guide to the General Data Protection Regulation* (Sweet & Maxwell 2017).

[165] Council of Europe, User Rights <https://www.coe.int/en/web/freedom-expression/internet-users-rights> accessed 16 March 2020.

children to '*unknown and unprecedented dangers*'.[166] Although certain assumptions can be made about the impact of technology on individuals and the community as a whole, it is hard to make definite predictions on how children's futures will be shaped when self-surveillance is normalised.[167]

Laws and regulations drafted on the assumption that only adults use the Internet, have proved inadequate to protect young users.[168] It is impossible to lay all the responsibility and decisions on children and their parents when their data management choices are designed and shaped by the business operators. Their control is steered in certain directions by the limited options the business operators offer them.

The new Regulation – the GDPR – takes into consideration the special protection needed for children in the digital world, incorporating an additional layer to safeguard them from harm or abuse. However, although the GDPR represents a significant step forward, it still needs improvement to tackle the challenges faced in practice, especially when implementing the articles regarding the obtainment of consent. Partial progress has been made towards protecting children's right to privacy and data protection when they access information society services.

It is encouraging that a number of new studies are being conducted in an effort to provide further guidelines and tools that support the implementation of articles on the protection of children. In light of the above, the age of consent should be justified on evidence-based data.[169] It is also good practice to include children's views when designing a product since this helps to ensure that risks are identified, the level of understanding required is assessed, privacy policies are altered if necessary and all necessary safeguards are implemented.[170]

It is equally important that stakeholders and businesses ensure that provisions such as privacy by design, privacy by default, and data protection impact assessment, which do not explicitly mention children but have crucial importance to their protection should be applied to the processing of children's personal data. Appropriate measures that overcome practical barriers and target evidence-based risks should be identified and evaluated before, during, and after the data collection and processing.

---

[166] Sonia Livingstone, Daniel Kardefelt Winther and Marium Saeed, 'Global Kids Online, Comparative Report' (UNICEF November 2019) 6.

[167] LSE, 'The Internet of Toys Comment' (27 January 2017) <https://blogs.lse.ac.uk/parenting4digitalfuture/2017/01/27/the-internet-of-toys/> accessed 17 March 2020.

[168] Report of the 2014 Day of General Discussion, Digital Media and Children's Rights (Committee on the Rights of the Child 2014) 8-9.

[169] Eva Lievens, Sonia Livingstone, Sharon McLaughlin, Brian O'Neill, and Valerie Verdoodt, 'Children's Rights and Digital Technologies' in Ton Liefaard, and Ursula Kilkelly (eds.) *International Human Rights of Children - International Human Rights* (Springer 2019) 487-491.

[170] ICO, Children and the GDPR 13 <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection themes/children/> accessed 27 February 2020.

Further interdisciplinary research is crucial in this field. The GDPR itself also needs to be improved to reflect the changing nature of technology, especially in relation to obtaining valid consent as it does not yet overcome the barriers that stakeholders face as technology advances. Many topics remain unexplored, such as gaining the informed consent of non-user data subjects, and balancing the opportunities presented by technology with the rising ethical, privacy, and security-based concerns. Finally, it is important to step beyond a simplistic binary view of technology as exclusively evil or purely good. Humanity's overall interests will perhaps be best served if a shared mindset is developed that considers all the economic, social, and, ethical aspects of this ever-expanding technology – and celebrates its benefits while mitigating its harms.