Mario Viola de Azevedo Cunha

December 2017

unicef
Office of Research-Innocenti

Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy

Innocenti Discussion Paper 2017-03

unicef
for every child

THE UNICEF OFFICE OF RESEARCH – INNOCENTI

The Office of Research – Innocenti is UNICEF's dedicated research centre. It undertakes research on emerging or current issues in order to inform the strategic directions, policies and programmes of UNICEF and its partners, shape global debates on child rights and development, and inform the global research and policy agenda for all children, and particularly for the most vulnerable.

Publications produced by the Office are contributions to a global debate on children and may not necessarily reflect UNICEF policies or approaches. The views expressed are those of the authors.

The Office of Research – Innocenti receives financial support from the Government of Italy, while funding for specific projects is also provided by other governments, international institutions and private sources, including UNICEF National Committees.

For further information and to download or order this and other publications, please visit the website at: www.unicef-irc.org.

INNOCENTI DISCUSSION PAPERS

Discussion Papers are signed pieces by experts and researchers on current topics in social and economic policy and the realization of children's rights. The aim is to encourage reflection and stimulate wide-ranging discussion.

This is a peer reviewed series.

For readers wishing to cite this document we suggest the following form: Viola de Azevedo Cunha, M. Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy. *Innocenti Discussion Paper* 2017-03. UNICEF Office of Research - Innocenti

Correspondence should be addressed to:

UNICEF Office of Research – Innocenti
Piazza SS. Annunziata, 12
50122 Florence, Italy
Tel: (+39) 055 20 330
Fax: (+39) 055 2033 220
florence@unicef.org
www.unicef-irc.org
@UNICEFInnocenti
facebook.com/UnicefOfficeofResearchInnocenti

CHILD PRIVACY IN THE AGE OF WEB 2.0 AND 3.0: CHALLENGES AND OPPORTUNITIES FOR POLICY

Mario Viola de Azevedo Cunha
Senior Research Fellow, UNICEF Office of Research - Innocenti; Research Associate, Centre for Media Pluralism and Media Freedom, European University Institute; and Member of the Institute for Technology and Society of Rio de Janeiro, Brazil.

Corresponding author: mario.cunha@eui.eu

ABSTRACT

We live in an information society, where the flow of information in the virtual environment is unprecedented. Web 2.0 platforms – and recently Web 3.0 platforms and the Internet of Things (IoT) – represent an important step forward in enhancing the lives of both adults and children everywhere, by combining greater efficiencies with a wide availability of new tools that can boost individual creativity and collective production. This new environment has exposed adults and children to fresh challenges that deserve special attention, especially those surrounding privacy. The main objective of this paper is to address the challenges posed to child privacy online and the impact that these challenges might have on other rights such as freedom of expression, access to information and public participation. To do this, the paper first analyses the current (and foreseen) threats to child privacy online and the various approaches adopted by government and/or the private sector to tackle this issue. The paper also examines whether children's perspectives and needs are considered in international debates on technology regulation, including in regard to the so-called 'right to be forgotten'. It then contextualizes the protection of privacy (and data protection) in relation to other fundamental rights in the online environment, arguing that in most cases this interaction is rather positive, with the enforcement of the right to privacy serving to protect other rights. The paper concludes by proposing some policy recommendations on how to better address the protection of children's online privacy. These objectives are achieved through literature review and analysis of legal instruments.

KEYWORDS: web, Internet of Things, privacy, data protection, children

ACKNOWLEDGMENTS

The author thanks Sarah Cook (UNICEF Innocenti), Jasmina Byrne (UNICEF Innocenti), Maria Grazia Porcedda (University of Leeds) and Danilo Doneda (Rio de Janeiro State University) for their useful insights and review of this paper.

GLOSSARY

Age of Capacity: Age at which a person attains legal capacity (Business Dictionary online).

Algorithm: "A step-by-step procedure for solving a problem or accomplishing some end especially by a computer" (Merriam-Webster Dictionary Online).

Article 29 Working Party: An independent advisory body composed of representatives of the national data protection authorities of all European Union (EU) member States, a representative of the European Commission and a representative of the European Data Protection Supervisor, which provides advice to the European Commission and supports EU member States in the harmonization of data protection rules and policies.

Blockchain: A technology that allows the creation of a robust, secure, transparent and distributed value recording and transfer system (Axon, 2015).

Bulk interception: A form of data collection via which government agencies tap the high capacity fibre-optic cables that carry the world's Internet communications (Kim, 2016).

Data subject rights: A set of rights related to the processing of personal data that usually includes the rights of access, rectification, blocking and erasure, and the right to object to a data processing activity (European Data Protection Supervisor, 2014).

Internet of Things (IoT): The network of objects that communicate and interact in an autonomous way through the Internet (McKinsey Global Institute, 2015).

Privacy by default: "Intrinsically designing privacy into all innovations before information management capabilities are added" (Cavoukian and Popa, 2016).

Privacy by design: "A multifaceted concept, involving various technological and organisational components, which implement privacy and data protection principles in systems and services" (European Union Agency for Network and Information Security website).

Privacy enhancing technologies (PETs): "Any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights" (Information Commissioner's Office, 2007)

Public participation: "Any process that directly engages the public in decision-making and gives full consideration to public input in making that decision" (United States Environmental Protection Agency website).

Sharenting: "A term used to describe the overuse of social media by parents to share content based on their children. It is related to the concept of 'too much information'" (Berman and Albright, 2017).

Web 2.0: "The second stage of development of the Internet, characterized especially by the change from static web pages to dynamic or user-generated content and the growth of social media" (Oxford Dictionaries online).

Web 3.0: "Refers to a supposed third generation of Internet-based services that collectively comprise what might be called 'the intelligent Web' – which uses technologies like semantic web, microformats, natural language search, data-mining, machine learning, recommendation agents, and artificial intelligence technologies – which emphasize machine-facilitated understanding of information in order to provide a more productive and intuitive user experience" (Spivack, 2007).

TABLE OF CONTENTS

1. Introduction . . . 6

2. Emerging challenges and risks to children's privacy . . . 6
- 2.1 Children's lack of knowledge . . . 6
- 2.2 Online surveillance . . . 8
- 2.3 Biometrics, Internet of Things-enabled devices and blockchain . . . 8
- 2.4 Pre-existing risks acquire a new dimension . . . 9

3. The protection of children's privacy: Regulatory mechanisms . . . 11
- 3.1 National Regimes. . . . 11
- 3.2 Regional Regimes. . . . 12
- 3.3 International Regimes . . . 14

4. Children's online rights, parental consent and the right to be forgotten: Impacts on privacy, freedom of expression and access to information . . . 14

5. Conclusions and policy recommendations: Why and how to address child privacy online . . . 17

6. References . . . 19

INTRODUCTION

We live in an information society, where the flow of information in the virtual environment is unprecedented. Web 2.0 and Web 3.0 platforms as well as the Internet of Things (IoT) represent important steps forward in enhancing the lives of both adults and children[1] everywhere, by combining greater efficiencies with a wide availability of new tools that can boost individual creativity and collective production.

The virtual environment has become a place where individuals can express ideas and opinions, build a public image or just interact with other people, either by sharing information and knowledge or by participating in cultural, social and/or political activities (Sartor and Viola, 2010). Children, who represent one third of all Internet users (Livingstone, Carr and Byrne, 2016), are increasingly exposed to this virtual environment and to all the benefits and hazards that come with it.

Several structures and systems are used to enable users' web activities, which range from the sharing of content (photos, videos and information), to the creation of blogs and participation in social networks, to the production of collective intellectual content. Moreover, in this new reality, e-commerce has added a further dimension, with platforms like Amazon and Alibaba, which transcend the physical boundaries of countries (UNICEF, 2017), enabling products to be purchased even in countries where the manufacturer has no local distribution network. Social networks such as Instagram and Snapchat, which now represent an important tool for children's social activity and are even seen as part of their identity (WHO, 2016), also operate beyond national borders.

These web platforms represent an important step forward both in terms of users' engagement in the public sphere and in enabling access to information available online. Indeed, such platforms facilitate public participation, making the Internet a user-friendly space for adults and children alike. Today, creating a blog – or even posting videos online – does not require a thorough knowledge of computer science. 'Plug and play' is the order of the day, and the ease with which new platforms can be acquired and used allows millions of people to participate in the virtual environment, whether by expressing views on issues, posting news, disseminating scientific and literary works, sharing photos and videos, or even developing open access computer systems (Sartor and Viola, 2010). The availability of new and easy-to-use technological tools therefore opens new opportunities for children, their development and how they can express themselves and engage in civic debates (Omar, 2014).

Taking this into account, the main objective of this paper is to address the challenges posed to child privacy online and the impact that this might have on other (human) rights such as freedom of expression, access to information and public participation. To do this, the paper first analyses the current (and foreseen) threats to child privacy online and the various approaches adopted by government and/or the private sector to tackle this issue. The paper also examines whether children's perspectives and needs are considered (or not) in international debates on technology regulation. It then contextualizes the protection of privacy (and data protection) in relation to other fundamental rights in the online environment, arguing that in most cases this interaction is rather positive, with the enforcement of the right to privacy serving to protect other rights. The paper concludes by proposing some policy recommendations on how to better address the protection of children's online privacy.

1 "For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier." (Convention on the Rights of the Child, article 1).

It is important to note that this paper deals exclusively with children's privacy online. It does not address other online risks for children such as bullying, abuse, sexual exploitation, sexting, online grooming, and the promotion of self-harm.

2. EMERGING CHALLENGES AND RISKS TO CHILDREN'S PRIVACY

The processing of huge amounts of personal data using data mining techniques has become a topic of interest because of the impact that it can have on children's right to privacy. Debate in this area currently focuses on issues such as children's lack of knowledge in regard to the processing of personal data; online surveillance techniques used by governments; the use of biometrics, including in combination with other technologies, and how this relates to children; and the pre-existing risks for children that acquired a new dimension with the advent of the web.

2.1 Children's lack of knowledge

The processing of data that we make available – or which is collected from us – online affects all internet users. It is of special relevance to vulnerable groups and especially minors, as they do not comprehend the risks and consequences related to the processing of their personal data (Shin and Kang, 2016). A Global Privacy Enforcement Network (GPEN) survey conducted in 2015 in response to concerns over children's apps and websites found that two thirds of the 1,494 websites[2] and apps surveyed had no protective controls to enable children (or their parents) to limit the disclosure of personal data (GPEN, 2015). A 2016 GPEN survey focusing on the IoT verified that 59 per cent of the IoT devices surveyed did not provide proper information on how they collect, use and disclose users' personal information (GPEN, 2016). Furthermore, a 2016 World Health Organization report on online food advertisements aimed at children concluded that parents were unaware of both the profiling techniques used to target children and the related risks (WHO, 2016).

These examples show that children (and their parents) are usually neither very knowledgeable about the risks they are exposed to online, nor aware of how information they post online may be used (Livingstone, Carr and Byrne, 2016; Byrne et al., 2016) and how this might jeopardize their privacy, safety and future careers (Jasmontaite and De Hert, 2015). These examples also demonstrate that children (and their parents) lack the skills and tools necessary to keep track of their data and exercise their rights as data subjects.

The fact that children "often lack the awareness and the capacity to foresee possible consequences (e.g. disclosure of personal information online can potentially make it universally accessible)" (OECD, 2012) makes them even more vulnerable to these risks. In this sense, there are cases where young adults have been rejected for jobs as a consequence of what they have posted online when in school or at college (OECD, 2012). Moreover, the disclosure of personal information online can lead, in extreme cases, to more serious consequences, such as the case of a young Italian woman who committed suicide after fighting (unsuccessfully) for months to have a video of a sexual nature removed from the Internet (Ambrosoli and Sideri, 2017). This raises some questions about the so-called 'right to be forgotten', which will be discussed later in this paper (see Section 4).

2 See: https://www.dataprotection.ie/docs/04-09-2015-Concerns-overchildrens-apps-and-websites-/1485.htm

2.2 Online surveillance

Another issue of concern relates to the growing use by some governments of mass surveillance techniques – authorized by recent laws (Nyst, 2017) – which capture the personal data of Internet users across the globe, including young children (Kim, 2016). Through the use of techniques such as bulk interception, the Internet traffic transiting fibre-optic cables that land in a specific country is monitored, and huge amounts of data – including personal data pertaining to children – are collected and analysed. On the one hand, the web provides new tools that allow children to investigate the world around them; on the other, it opens new avenues for governments and companies "to track, store, and analyse children's actions with a level of detail previously unattainable" (Brown and Pecora, 2014).

Mass online surveillance not only affects privacy rights, but also other rights such as freedom of expression. The processing of personal data without a specific purpose (e.g. to monitor an individual under investigation) – as is done for thousands or even millions of people – is a violation of privacy rights. Freedom of expression is also curtailed by online surveillance, as many people would refrain from expressing their views online if they knew that a certain government could monitor their activity, even in a third country. A report commissioned by UNICEF has highlighted how online surveillance could be even more dangerous for children growing up today, as the mass collection of data "would allow authorities to build and maintain records of children's entire digital existence" if linked to individual profiles – something that many experts suggest is already possible (Nyst, 2017).

2.3 Biometrics, Internet of Things-enabled devices and blockchain

The use of biometrics is a third example of how today's technologies can affect child privacy online – and also offline. Biometric authentication is largely used for identification purposes in the area of migration (Lodinová, 2016), mostly to identify and register undocumented immigrants and refugees (UNHCR, 2015). The technology is also being used for the identification of children in countries that lack effective birth registration systems (Gelb and Clark, 2013). If we consider that some 230 million children under the age of 5 worldwide were not registered at birth (UNICEF, 2013), we see that biometric authentication could be a good substitute for traditional birth registration systems[3] where these do not work properly. Identification using biometrics would allow children to claim services and protection that they are entitled to but which they do not currently receive, since claiming them is usually reliant upon birth registration (UNICEF, 2015).

Biometrics are now being combined with online technologies such as social networks, IoT-enabled devices and the blockchain.[4] For example, some social media platforms have integrated facial recognition technologies with 'tagging' functionality, enabling the identification of children in photos (Nyst, 2017). In a similar vein, some IoT-enabled devices and toys have voice recognition features that allow them to identify and recognize children as well as to communicate with them and record their voices (Nyst, 2017).

Blockchain technology, in turn, is being used to ensure that biometric data are stored in an environment that ensures the security and integrity of such information (Mordini, 2016). This is

3 "Biometrics can be used for two identity-related purposes: 1) *identifying* an individual within a large population to determine if she is unique (one-to-many or 1:N matching), and 2) *authenticating* an individual against a record to determine if she is who she claims to be (one to one or 1:1 matching)." Gelb and Clark, 2013.

4 For a brief explanation of blockchain technology, see Axon, 2015.

made possible by the blockchain decentralized model combined with the use of cryptography (Axon, 2015).

Privacy advocates have raised considerable concern over these new applications of biometrics, over and above the pre-existing risks that relate to identity theft and misuse of personal information. They consider the use of biometric data invasive, and highlight how errors and inaccuracies in the authentication process could restrict individuals' access to services and products (Nyst, 2017).

Such risks arise largely because biometric data are permanently associated with an individual (e.g. once data have been stored in a blockchain, they cannot be excluded). Thus, if stored biometric data contain an error or inaccuracy, or if such data are lost or stolen, it is incredibly difficult to modify or replace the biometric data (Cimato, Sassi and Scotti, 2008). It is not by chance that European data protection authorities recommend that biometric technologies "should only be used for the strictly limited purpose to verify the user's consent and should therefore be deleted immediately after" (Article 29 Working Party, 2012).[5]

It is not that biometrics have no positive applications – in fact, it is just the opposite. The technology can be really useful, as outlined in the above example that uses biometrics as a substitute for birth registration. A proper framework must be put in place, however, to protect children's privacy against the eventual misuse of biometric technologies and the processing of personal data through them. At the very least, the principles of privacy by design and privacy by default should be applied when designing any biometrics based system or application, and corresponding privacy enhancing technologies put in place.

2.4 Pre-existing risks acquire a new dimension

The risks highlighted above mostly relate to the web and to the development of new technologies. There are also other risks that are similar to offline risks in existence since before the advent of the Internet,[6] but which have gained a new dimension online. These risks "include, but are not limited to, cyberbullying, online stalking, identity theft, and exposure to unwanted or inappropriate advertising content" (Shin and Kang, 2016).

One such pre-existing risk relates to advertising directed at children. Companies see children and adolescents as an important market, since they influence the consumer decisions made by families (Doneda and Rossini, 2015). Information about children's online habits and behaviour is thus commercially attractive, as it helps companies to develop effective business strategies to reach this important share of the online market. As highlighted by some authors, spending time online is one of children's main activities today, and children represent a very important consumer segment (Shin and Kang, 2016).

Children's private lives can thus be exploited by marketers, who can observe their online activity and even mimic those online environments that appeal to children and in which they feel safe (Steeves, 2006). This kind of behaviour not only affects children's privacy, but also other fundamental rights, like access to information, as by obtaining children's data, marketers can

5 Although this document focuses chiefly on facial recognition technologies, it fully applies to the use of biometrics in the web environment in general, since it relies on the "the particular risks involved with biometric data".

6 "Not all forms of ICT-facilitated child abuse and exploitation are necessarily new or fundamentally different from existing forms of child abuse and exploitation." UNODC, 2015, p. 8.

shape children's online experience and manipulate their online social environment (Casarosa, 2011). Paid partnerships between advertisers and YouTube video bloggers (vloggers) are one example of such manipulation, since the advertisers typically do not make it clear that the content is paid advertising rather than authentic vlogger-produced content (WHO, 2016). Recent research into advertising on YouTube channels for children confirmed that food and drink companies "use popular youtubers to pitch products and brands as non-commercial content in videos" (Araújo et al., 2017).

These are, however, just a few examples of the many and varied challenges regarding the protection of children privacy in the web environment.[7] The above-mentioned report commissioned by UNICEF summarizes the different threats to children's rights online under the following headings: i) corporate data collection, analysis and sale of children's browsing data; ii) use of biometrics; iii) age verification and mandatory use of identity; iv) encryption and device security; v) government surveillance; vi) use of parental controls; and vii) managing reputation online (Nyst, 2017).

Another new trend that poses a series of risks to children, especially those from certain ethnic or religious groups, is the everyday use of algorithms to make an increasing number of automated decisions online. If privacy and other ethical standards are not embedded in algorithms, their use can lead to discrimination against children based on their country of origin, ethnicity and/or religious status. Such discrimination can limit children's future opportunities in terms of education and career, and may even expose children to increased state surveillance – should they appear to correspond to a group that is more likely to exhibit criminal behaviour in future. Discrimination can occur because algorithms are 'fuelled' by data: if the data contain any bias, the analysis conducted by the algorithm will follow the same pattern. For example, a recruitment system algorithm that relies on historical hiring data, without embedding any data protection or ethical principles, will likely give preference to job applicants living close to the workplace, because such candidates have historically had better retention rates. Such results will automatically exclude from the recruitment process applicants who live far from the workplace – often those living in low-income areas – which may discriminate against certain groups (Marshall, 2016). Another real example of discrimination resulting from an algorithm concerns the Compas software program used in the United States of America to determine the likelihood of a criminal defendant reoffending, which was found to be racially biased against individualsof African descent (Larson et al., 2016).

It is important to highlight that not all threats to children's privacy come from companies or governments: schools (ICO, 2012) and even parents can pose serious risks too. Parental breech of their children's privacy, for example, can have another dimension in the digital age. Cases of 'sharenting' – where a parent shares a child's personal information and/or images without her/his consent – have become quite common (Steinberg, 2017) and can affect a child's reputation and her/his privacy more broadly, for example, by enabling the misuse of personal information. (Steinberg, 2017). Before consenting to the processing of a child's personal data by social media, or personally disclosing a child's personal information online, parents should first ask the child whether she/he agrees to this, taking into account her/his age of capacity (Steinberg, 2017).

7 For an idea of more traditional examples of the privacy risks to which children and teenagers are exposed online, see Powell, 2010.

Despite all of this, existing laws generally do not sufficiently safeguard children's privacy online (OECD, 2012). The situation becomes even more worrying as new identification tools based on biometrics technology are developed, including facial recognition systems, and we see the widespread use of identity verification tools such as those mentioned above (see Section 2.3).

3. PROTECTION OF CHILDREN'S PRIVACY: REGULATORY MECHANISMS

In analysing the various national, regional and international instruments that aim to protect children's privacy and their personal information, it is important to note that the adoption of such norms pre-dates the advent of the Internet.

3.1 National Regimes

In 1974, the United States adopted the Family Educational Rights and Privacy Act (FERPA) to protect children's privacy and family privacy. This federal law – which remains in force today – prohibits educational institutions in receipt of federal funding from releasing educational records[8] to unauthorized persons (Topelson et al., 2013). In regard to students under the age of 18, FERPA relies mainly on the notion of parental consent – as do all subsequent laws and international instruments adopted around the world to address the issue of child privacy. One interesting requirement under FERPA is the obligation for schools to send students and their parents (where appropriate) an annual notice to inform them of their rights in relation to the processing of personal data (Topelson et al., 2013).

Another US law, the Children's Online Privacy Protection Act (COPPA), and its related Children's Online Privacy Protection Rule (known as the COPPA Rule),[9] adopt the same approach based on parental consent. These norms apply to online service providers (OSPs) that offer services designed to target children under the age of 13 or which knowingly collect data from them (Topelson et al., 2013). According to the COPPA Rule, an OSP must "obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children."[10]

Other countries to have adopted similar provisions requiring parental consent prior to the processing of children's personal data include South Africa[11] and Spain (AEPD, 2008). The age threshold differs in each case, however. While in the US, COPPA applies to children under the age of 13, the age threshold for the equivalent provision in Spain is 14 years and in South Africa 18 years. In the UK, although there is no legal requirement for OSPs to obtain parental consent, the Information Commissioner's Office recommends they do so for children under the age of 12 (ICO, 2010).

Some other countries simply restrict the processing of children's personal data. For example, Ghana's Data Protection Act, 2012[12] classifies data relating to a child as a special category of

8 According to FERPA, "educational records" include the name of a student or a student's family member, the address of a student or student's family member, personal identifiers, indirect identifiers and other information that "would allow a 'reasonable person in the school community' to identify the student with reasonable certainty". (Topelson et al., 2013, p. 3.)

9 <www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites>, accessed on 17 November 2017.

10 United States of America, Federal Trade Commission, Children's Online Privacy Protection Rule 2013.

11 Republic of South Africa, Protection of Personal Information Bill, 2009. Available at: <www.up.ac.za/media/shared/9/HumPdf docs/Postgrad Research Docs/protection-of-personal-information-2009.zp53213.pdf>, accessed 20 January 2017.

12 Ghana's Data Protection Act, 2012. Available at: <www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf>,>, accessed 17 November 2017.

data (sensitive data), which should be processed under specific conditions, one of them being the consent of the data subject (or person legally responsible for the child). Other countries like Brazil just rely on the general rules on legal capacity, instead of specific ones for the processing of children's personal data.[13]

3.2. Regional Regimes

At a regional level, the new EU General Data Protection Regulation (GDPR) will enter into force in May 2018. This regional instrument "explicitly recognizes that children deserve their personal data to be specifically protected, 'as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data' (Recital 38)" (Maceinate, 2016). Again, the GDPR relies on the requirement to obtain parental consent, in the context of an offer of an information service provided online directly to a child, establishing an age threshold of 16 years.[14] This provision has been criticized, in part because it may lead to confusion and to different legal standards of protection, since it allows member States to set different age thresholds (WHO, 2016).[15] The chief criticisms of the provision requiring parental consent, however, are that it is too inclusive and overprotective, because "it risks limiting all children in their online activities and restricting their opportunities" (Maceinate, 2016). Moreover, it also implies that parents know more than their children about protecting privacy – an idea already challenged in this paper (see Section 2.1) – and that no specific protection is required for children above the age threshold (WHO, 2016).[16] It is important to highlight that the GDPR does not require parental consent to be obtained "in the context of preventive or counselling services offered directly to a child".[17] This seems to be a good step forward in terms of recognizing the best interests of the child, as provided for by article 3 of the Convention on the Rights of the Child.

Even taking into account its critics, the GDPR nevertheless marks a great change for the EU, as its current data protection framework (Data Protection Directive 95/46/EC and Privacy and Electronic Communications Directive 2002/58/EC) contains no specific provisions for children.[18] According to the Data Protection Directive, "The processing of both children's and adults' personal data is lawful if unambiguous consent of the data subject is provided or if the processing of personal data is necessary in a particular situation" (Jasmontaite and De Hert, 2015).

Another regional initiative that tackles that issue of data protection is the African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014.[19] This seems to go in the same direction as the GDPR, although it does not expressly provide for the requirement to obtain parental consent. Article 1 of the Convention defines "consent of the data

13 Bill 5276/2016, presented to the National Congress by the President of Brazil on 13 May 2016, after two rounds of public consultation. See: <www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>, accessed 20 January 2017.

14 The GDPR, however, leaves it open to member States to establish, by law, "a lower age for those purposes provided that such lower age is not below 13 years". Regulation (EU) 2016/679 (General Data Protection Regulation), 2016, art. 8(1).

15 The minimum age threshold authorized by the GDPR is 13 years.

16 Actually, many surveys have shown that millions of children under the age of 13 are active users of social networks, which demonstrates that the age controls put in place by such web platforms are ineffective. See, for instance, Montgomery, 2015.

17 Recital 38 of the GDPR.

18 This is not unusual: most data protection laws do not take into account the age of the data subject. See, for instance, the laws of Argentina (Protección de Datos Personales, Ley 25.326), Canada (Privacy Act 1985; Personal Information Protection and Electronic Documents Act 2000), Japan (Act on the Protection of Personal Information, Act No. 57 of 2003) and Uruguay (Ley de Protección de Datos Personales y Acción de "Habeas Data", Ley No. 18.331).

19 At the time of writing, only nine African countries had signed the Convention and just one country, Senegal, had ratified it. See: <www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf>, accessed 22 September 2017.

subject" as "any manifestation of express, unequivocal, free, specific and informed will" given by the data subject or by her/his legal representative.[20]

Requiring parental consent represents progress to a certain extent, because without such a requirement "neither [Internet service providers] nor website operators (ie. data controllers) are required to take into account the age of the users when they notify that the processing of personal data is taking place or when they request users' consent" (Jasmontaite and De Hert, 2015). What this means in effect is that children are required to provide consent in the same way as adults (Jasmontaite and De Hert, 2015). Age is thus a crucial issue to address in Internet governance and data protection debates (Livingstone, Carr and Byrne, 2016).

Nevertheless, privacy and child safety advocates criticize approaches that rely exclusively on the requirement to obtain parental consent. They correctly suggest other, more effective measures to protect child privacy online, including education initiatives aimed at children and parents and web platforms making changes to their default privacy settings (Jasmontaite and De Hert, 2015). Moreover, relying solely on parental consent can have an impact not only on children's right to privacy, but also on their rights to freedom of expression, access to information and public participation, as will be discussed in Section 4.

Governments should therefore adopt legislation or put in place policies that require Internet service providers, search engines, social media networks and other providers of Internet-enabled content and services to provide children with proper information – adapted to their capacities – about the processing of their personal data and their rights as data subjects. Such providers should also be required to ensure greater transparency of the personal data processing that they carry out. A good example in the right direction is the GDPR, article 12(1) of which requires all companies and public authorities that collect and process personal data to provide information to data subjects (i.e. users) "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child" (GDPR, 2016). Moreover, government agendas should also focus on promoting digital literacy among children and parents, as although both children and parents may be aware of basic privacy settings, they face increasing difficulties due to the new challenges mentioned discussed in Section 2 (Berman and Albright, 2017).

The worst case scenario, however, is a total lack of data protection laws – which most often occurs in low-income or lower-middle-income countries[21] – because personal data from both children and adults can then be processed without any safeguards in place. Relying on parental consent is thus already an important step towards ensuring child privacy online, although, as discussed in Section 2.1, parents also lack a proper understanding of online privacy challenges and must be better educated in this respect.

20 The full text of the Convention is available at: <www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>, accessed 20 January 2017.

21 There is a tendency, however, to adopt data protection laws even in low-income countries, for example, low-income African nations. See, for instance, Technology Law Dispatch, 'New Data Protection Laws in Africa', <www.technologylawdispatch.com/2015/02/data-cyber-security/new-data-protection-laws-in-africa/>, accessed 23 January 2017.

3.3 International Regimes

At the international level, the situation is even worse – despite growing discussion of the importance of protecting child privacy online, international documents adopted in the field of online privacy do not usually refer specifically to child privacy. For example, child privacy is mentioned by neither the United Nations General Assembly resolution on online privacy[22] nor the first report of the first United Nations Special Rapporteur on the right to privacy[23] (child privacy is not among the Special Rapporteur's mandate priorities).[24] Similarly, recently adopted national instruments intended to regulate rights online, like Brazil's Civil Rights Framework for the Internet (Marco Civil da Internet)[25] and Italy's Declaration of Internet Rights,[26] make no provision for the protection of child privacy.[27] An exception to this rule is the United Nations Human Rights Council resolution on the right to privacy in the digital age, adopted in 2017. This explicitly mentions the Convention on the Rights of the Child as a guiding human rights instrument, and also recognizes that violations of the right to privacy online can have particular effects on children.[28]

It is crucial to remember, however: "Implementation of child rights in the digital age requires not only adherence to human rights and values, but also empowerment and participation of child users that fosters their creativity, innovation and societal engagement" (Livingstone, Carr and Byrne, 2016). The protection of privacy plays a critical role in this respect (OECD, 2012; Nyst, 2017).[29]

4. CHILDREN'S ONLINE RIGHTS, PARENTAL CONSENT AND THE RIGHT TO BE FORGOTTEN: IMPACTS ON PRIVACY, FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION

It is apparent that most regulatory solutions to address child privacy online rely mainly on the requirement to obtain parental consent before processing the personal data of children up to a certain age. Such a restriction may impact on other child rights, however. A recent paper published by UNICEF acknowledges that "Requiring parental involvement and consent for the use of widely available online services, for instance, can impede children's freedom of expression, access to information and development of digital literacy" (Nyst, 2017)[30].
The situation is more complex for a number of reasons. First of all, relying on parental involvement does not take into account the empirical evidence that shows that children are as aware as their parents of the privacy risks to which they are exposed online (Jasmontaite and De Hert, 2015). Moreover, children can exercise agency in line with their evolving capacities,

22 United Nations General Assembly Resolution 68/167, adopted on 18 December 2013.

23 Cannataci, Joseph A., Report of the Special Rapporteur on the right to privacy, A/HRC/31/64, advance unedited version, 8 March 2016. Available at: <www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc>, accessed 15 January 2017.

24 United Nations Human Rights Office of the High Commissioner, 'Planned Thematic Reports and call for consultations', <www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx>, accessed 22 January 2017.

25 An unofficial English version can be found in De Souza, Viola and Lemos, 2015.

26 Declaration of Internet Rights (official English version) is available at: <www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf>, accessed 6 September 2016.

27 Though article 29 of Brazil's Civil Rights Framework for the Internet does recognize the potential for parents to exercise parental control over children's online activities using parental control software programs. See De Souza, Viola and Lemos, 2015.

28 United Nations Human Rights Council Resolution A/HRC/34/L.7/Rev.1, 22 March 2017, preamble and Section 5.g.

29 A recommendation of the Organisation for Economic Co-operation and Development Council on the Protection of Children Online suggests that "Policies to protect children online should be consistent with fundamental values of democratic societies as they apply to all individuals including children. In particular, they should support freedom of expression, privacy protection and the free flow of information." OECD, 2012. A recently published UNICEF discussion paper makes the same argument in a similar way (Nyst, 2017).

30 Nyst, 2017, p. 9.

as provided for by article 12 of the Convention on the Rights of the Child (Robin, 2014). Indeed, a recent UNICEF Innocenti study shows that while most older children know how to manage online privacy settings, only a few younger children report that they can do so (Byrne et al., 2016). Furthermore, threats to children's privacy come not only from governments and private companies, but also from parents. Since "it is now commonplace for parents to share information about their children online, most children are not in a position to either scrutinize the information or object to its posting" (Nyst, 2017). This so-called sharenting can affect a child's privacy and reputation.

The idea of relying solely on parental intervention "opposes the idea of children's participation in the decision-making process that concerns them – an idea that is anchored in the UN Convention of the Rights of Children" (Jasmontaite and De Hert, 2015). To consent to the processing of their children's personal data, parents must intervene in their children's private online spaces (e.g. gaming accounts, social network accounts). As a result, children's access to information and potential to express themselves become both limited and dependent on their parents. Children may even consider such control by their parents an invasion of their private lives, as children are often unwilling to share their online experiences with their parents. Relying mainly on parental consent to protect children's privacy thus reduces children's autonomy and freedom online (Shin and Kang, 2016). Children have the right to express their views on all matters that affect them, and can express their views independently from their parents on matters that affect them, even when such opinons defer from those of of their parents. However, as stated in the Committee on the Rights of the Child General Comment No. 20 (2016).[31] This includes receiving guidance on how to exercise their rights and protect their privacy - even within the family.

Ensuring child privacy online has, in most cases, a positive impact on the exercise of the other aforementioned child rights. Careful consideration should be given to how privacy initiatives can help to guarantee the full exercise of these other rights and ensure that such initiatives are "consistent with the evolving capacities of the child [and provide] appropriate ... guidance in the exercise by the child of the rights" (Jasmontaite and De Hert, 2015), as provided for by article 5 of the Convention on the Rights of the Child. In fact, Member States "shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child" (Jasmontaite and De Hert, 2015).

The Memorandum on the protection of personal data and privacy in Internet social networks, specifically in regard to children and adolescents (the Memorandum of Montevideo)[32] is considered a landmark instrument and contains recommendations for the protection of children online (Elder et al., 2013; UNICEF, 2011). The Memorandum suggests that a ban on the processing of children's personal data should be considered and that parental control mechanisms should be put in place to protect adolescents' data.[33] Such an approach still does not seem to properly address the problem, however: banning the handling of children's personal

31 United Nations, Committee on the Rights of the Child, General Comment No. 20 (2016) on the implementation of the rights of the child during adolescence, CRC/C/GC/20, United Nations, 6 December 2016.

32 The Memorandum of Montevideo was drafted in 2009 by a team of Latin American experts and includes recommendations for states, public bodies, industry and educational institutions. Memorandum on the protection of personal data and privacy in Internet social networks, specifically in regard to children and adolescents (Memorandum of Montevideo), Montevideo, 28 July 2009. Available at: <www.iijusticia.org/docs/MemoMVD_En.pdf>, accessed 22 January 2017.

33 One of the weaknesses of the Memorandum is that it does not establish the differences between 'children' and 'adolescents', leaving it instead to states to make this distinction.

data would end up restricting children's access to the web; and putting in place parental control mechanisms for adolescents does not take into account adolescents' evolving capacities, instead making them entirely dependent on their parents' consent.

Another debate that has gained a lot of attention since 2014, and which affects children's privacy online revolves around the so-called 'right to be forgotten'. The idea of such a right achieved international prominence following the case brought before the European Court of Justice by Mario Costeja González.[34] In its decision, the Court concluded that a search engine provider, at the request of an individual, should remove from search results (following on a search for the individual's name) links to any third party web pages containing personal information about the individual, even where there is no proof of harm.

This 'right to delist' – as recognized by the European Court of Justice – is just one online aspect of the so-called right to be forgotten (Viola and Itagiba, 2016). The other is the deletion of content on web pages – or even in social network posts – which contains personal information about the individual in question. This 'right', in fact, works much more as a means to protect other rights, such as privacy and reputation, than as a right in itself. In this respect, such a 'remedy' could ensure that children do not suffer serious long-term consequences simply because they lack a full understanding of the risks involved in posting personal information online. For example, children may post images of themselves in embarrassing situations, or their parents may post images without the children's 'consent', which may result in serious reputational damage. As children grow into adults, the consequences of being unable to erase regrettable content from the Internet and thus from public view can be severe, as in the cases mentioned in Section 2.4 of the young adults rejected for jobs and the tragic suicide of the young Italian woman.

As Macenaite highlights, however, the application of the right to be forgotten to children "may be more problematic than to adults, demanding a dynamic perspective: with time, an unknown child may become a public figure, and his or her data may therefore change status from private (worth deleting) to something worth public interest (worth preserving)" (Macenaite, 2016).

Nonetheless, there have already been some attempts to regulate the right to be forgotten by applying a child protection approach. The first such attempt was made by the State of California, which recognized such a right specifically in relation to children, in a law that applies to information posted by the minor her/himself (rather than by a third party). This law enables a minor (under 18 years) who is a registered user of a "website, online service, online application, or mobile application" to request that the relevant provider removes the content or information she/he has posted on a particular website, online service, or online or mobile application.[35] The new EU GDPR adopts a similar approach.[36] It acknowledges that children are usually not fully aware of the risks related to the processing of their personal data and recognizes the possibility of an individual requesting the removal of specific personal data even if she/he is no longer a child. The GDPR also sets out criteria for how to assess if there is a case for applying the right to be forgotten, and it will be for OSPs to conduct this assessment exercise.[37]

34 European Court of Justice, Case C–131/12, judgment, 13 May 2014.

35 See California Legislative Information, 'Business and Professions Code, Division 8. Special Business Regulations, Chapter 22.1 Privacy Rights for California Minors in the Digital World,' <http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22580>, accessed 26 July 2017.

36 Recital 68 of the GDPR.

37 Article 17 of the GDPR.

The debate on the right to be forgotten has also sparked great controversy, with some groups that advocate for freedom of expression arguing against the right to be forgotten, and others which advocate for privacy rallying in favour of such a right (Singleton, 2015). Courts around the world adopt one or other stance. But, again, when talking about children, this 'right' could be used not as a right in itself – that is, to delete any information from the web – but as a tool to protect children when their privacy, reputation or other rights are violated and no better solution exists to stop the violation. It is important to say that there is no final word on how such a right should be exercised: in some countries (e.g. Japan) a court should balance the interests involved; in others (e.g. member States of the European Union) the OSPs themselves are required to balance the competing interests (Neville, 2017).

5. CONCLUSIONS AND POLICY RECOMMENDATIONS: WHY AND HOW TO ADDRESS CHILD PRIVACY ONLINE

There are various reasons why it is necessary to address online privacy differently in relation to children as compared to adults. As mentioned above, children represent one third of web users worldwide. This proportion is far greater if we focus only on the Global South, which has a larger population of children and adolescents than the Global North (Livingstone, Carr and Byrne, 2016).

Some authors rightly say "it is timely to translate the [Convention on the Rights of the Child] into a clear set of standards and guidelines and a programme of action that addresses children's rights in the digital age." (Livingstone, Carr and Byrne, 2016) considering "children's needs and rights in global and national internet policy, provision and governance" (Byrne et al., 2016).

Taking into account these concerns, the following recommendations are proposed:

- Any legislation in the field of online privacy should be 'technologically neutral',[38] so that it is also able to regulate new technologies developed following its adoption, without the need for revision.

- Business models pursued by OSPs, and regulatory frameworks applicable to them, should include "transparency in methods of data collection and clear explanations of how the resulting data will be used" (Brown and Pecora, 2014). They should also be adapted to meet children's information needs and understanding.

- The idea of requiring OSPs to send an annual notice – similar to those sent by schools in the United States under FERPA – to inform children and their parents about the possibility of reviewing/accessing their personal data and seeking correction (among other rights) seems to be a good measure to ensure the protection of child privacy online.

- The adoption of privacy policies with a "clear and easy to understand" (Topelson et al., 2013) wording, as provided for by COPPA and the GDPR[39], will help to ensure that children and their parents have a better understanding of what OSPs do with children's data.

38 'Technological neutrality' means that "the same regulatory principles should apply regardless of the technology used" (Maxwell and Bourreau, 2015). Various international and regional forums are discussing the idea of technological neutrality as a means to ensure that legislation drafted now will cover future technological developments without the need for amendments.

39 Recital 58 of the GDPR requires that "any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

- Rules on consent for the processing of children's personal data should consider their age and should take into account developmental differences and special vulnerabilities (OECD, 2012). For instance, parental consent may be required to process the personal data of children below a certain age (e.g. 13 years); above this age threshold, parental intervention may be replaced by specific safeguards that reflect children's age of capacity (EDPS, 2012;[40] Article 29 Working Party, 2008).[41]

- The particular rights and needs of children should be considered in the design of Internet governance rules (Livingstone, Carr and Byrne, 2016) as well as in the international debate about online (and offline) privacy.

As recognized by the Oslo Challenge, issued in 1999 – by which time Internet use was already widespread – the web can play an important role in allowing children to fully exercise their rights. Therefore the recommendations made almost 20 years ago – highlighting that policymakers should consider children's perspectives and needs when addressing policy issues, especially those related to (new) media, are still valid.[42] In addition to considering children's needs and perspectives, policy makers should give children a voice in the international debates on technology regulation. Laws and international instruments should be adopted with these ideas in mind, as a fundamental way of ensuring that children's perspectives and needs are considered and respected.

40 The European Data Protection Supervisor suggests, "It should be explored to what extent, and within which age group, parental consent would be required to validate a change of privacy settings." See EDPS, 2012, p. 7.

41 The Article 29 Working Party suggests that even consent should be adapted to the degree of majority of the child. See Article 29 Working Party, 2008, p. 6.

42 https://www.unicef.org/malaysia/Factsheet-CRC-Oslo-Challenge.pdf. Accessed 20 January 2017.

6. REFERENCES

Agencia Española de Protección de Datos, Safe Browsing: Guidelines on rights of children and duties of parents, AEPD, 2008. Available at: <www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/RECOMEND_MEN_MAY_eng.pdf>, accessed 13 November 2017.

Ambrosoli, Umberto, and Sideri, Massimo, *Diritto all'oblio, dovere della memoria*, Giunti, 2017.

Araújo, Camila S., et al., 'Characterizing Videos, Audience and Advertising in Youtube Channels for Kids', in Giovanni L. Ciampaglia, Afra Mashhadi and Taha Yasseri (eds.), 9th International Conference, SocInfo 2017, Oxford, 13–15 September 2017, Proceedings, Part I, pp. 341–359.

Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf>, accessed 13 November 2017.

Article 29 Working Party, Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools), adopted on 18 February 2008. Available at: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp147_en.pdf>, accessed 13 November 2017.

Axon, Louise, 'Privacy-awareness in blockchain-based PKI', CDT Technical Paper Series 21/15, Centre for Doctoral Training in Cyber Security, Oxford, 2015. Available at: <https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b>, accessed 13 November 2017.

Bansal, Komal, 'Effectiveness of Children Online Privacy Strategies', proceedings of the 16th Winona Computer Science Undergraduate Research Symposium, Winona State University, Minn., 27 April 2016.

Berman, Gabrielle, and Albright, Kerry, 'Children and the Data Cycle: Rights and Ethics in a Big Data World', *Innocenti Working Paper* 2017-05, UNICEF Office of Research - Innocenti, Florence, June 2017. Available at: <www.unicef-irc.org/publications/pdf/IWP_2017_05.pdf>, accessed 13 November 2017.

Brown, Duncan H., and Pecora, Norma, 'Online Data Privacy as a Children's Media Right: Toward Global Policy Principles', *Journal of Children and Media*, vol. 8, no. 2, 2014, pp. 201–207.

Byrne, Jasmina, et al., *Global Kids Online: Research synthesis 2015-2016*, UNICEF Office of Research Innocenti and London School of Economics and Political Science, 2016. Available at: <www.unicef-irc.org/research/270/>, accessed 13 November 2017.

Casarosa, Federica, 'Protection of minors online: available regulatory approaches', *Journal of Internet Law*, vol. 9, March 2011, pp. 25–35.

Cavoukian, Ann, and Popa, Claudiu, Embedding Privacy Into What's Next: Privacy by Design for the Internet of Things, Privacy and Big Data Institute, Ryerson University, Toronto, April 2016. Available at: <www.ryerson.ca/content/dam/pbdce/papers/Privacy-by-Design-for-the-Internet-of-Things.pdf>, accessed 13 November 2017.

Cimato, Stelvio, Sassi, Roberto, and Scotti, Fabio, 'Biometrics and Privacy', *Recent Patents on Computer Science*, vol. 1, 2008, pp. 98–109.

Data Protection Commissioner of Ireland, 'Global Privacy Enforcement Network (GPEN) Privacy Sweep 2015: Concerns over children's apps and websites', <www.dataprotection.ie/docs/04-09-2015-Concerns-overchildrens-apps-and-websites-/1485.htm>, accessed 13 November 2017

Doneda, Danilo, and Rossini, Carolina , *Proteção de dados de crianças e adolescentes na Internet*, TIC Kids Online Brasil 2014, Comitê Gestor da Internet no Brasil, São Paulo, 2015. *Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil,* edited by Alexandre F. Barbosa, Comitê Gestor da Internet no Brasil, São Paulo, 2015. Available at: <http://cetic.br/media/docs/publicacoes/2/TIC_Kids_2014_livro_eletronico.pdf>, accessed 13 November 2017.

Elder, Laurent, et al., eds., *Connecting ICTs to Development: The IDRC Experience*, Anthem Press, London and New York, 2013.

European Court of Justice, Case C–131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of the Court (Grand Chamber), 13 May 2014.

European Data Protection Supervisor, Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, EDPS, 2014. Available at: <https://edps.europa.eu/sites/edp/files/publication/14-02-25_gl_ds_rights_en.pdf>, accessed 13 November 2017.

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – 'European Strategy for a Better Internet for Children', EDPS, 2012. Available at: <https://edps.europa.eu/sites/edp/files/publication/12-07-17_better_iternet_children_en_0.pdf>, accessed 13 November 2017.

Gelb, Alan, and Clark, Julia, 'Identification for Development: The Biometrics Revolution', CGD Working Paper 315, Center for Global Development, Washington, D.C., January 2013.

Information Commissioner's Office, Data Protection Guidance Note: Privacy enhancing technologies (PETs), ICO, 2007. Available at: <www.acc.com/chapters/euro/upload/PRIVACY_ENHANCING_TECHNOLOGIES_V2-ashx.pdf>, accessed 13 November 2017.

Information Commissioner's Office, Personal information online code of practice, ICO, 2010. Available at: <https://ico.org.uk/media/1591/personal_information_online_cop.pdf>, accessed 13 November 2017.

Information Commissioner's Office, Report on the data protection guidance we gave schools in 2012, ICO, September 2012. Available at: <https://ico.org.uk/media/for-organisations/documents/1132/report_dp_guidance_for_schools.pdf>, accessed 13 November 2017.

Jasmontaite, Lina, and De Hert, Paul, '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', *International Data Privacy Law*, vol. 5, no. 1, 2015, pp. 20–33.

Kim, Scarlet, 'How Bulk Interception Works', Privacy International, September 2016, <https://medium.com/privacy-international/how-bulk-interception-works-d645440ff6bd>, accessed 13 November 2017.

Larson, Jeff, et al., 'How We Analyzed the COMPAS Recidivism Algorithm', ProPublica, May 2016, <www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm/>, accessed 13 November 2017.

Livingstone, Sonia, Carr, John, and Byrne, Jasmina, 'One in Three: Internet Governance and Children's Rights', Innocenti Discussion Paper No. 2016-01, UNICEF Office of Research - Innocenti, Florence, 2016. Available at: <www.unicef-irc.org/publications/pdf/idp_2016_01.pdf>, accessed 13 November 2017.

Lodinová, Anna, 'Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy', *Development, Environment and Foresight*, vol. 2, no. 2, November 2016, pp. 91–100.

Macenaite, Milda, 'From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation', *New Media and Society*, vol. 19, no. 5, May 2017, pp. 767–779.

Marshall, P., 'Issue: Technology and Business Ethics Short Article: Algorithms Can Mask Biases in Hiring', 2016. Available at: http://businessresearcher.sagepub.com/sbr-1775-98200-2717795/20160215/algorithms-can-mask-biases-in-hiring

Maxwell, Winston, and Bourreau, Marc, 'Technology neutrality in Internet, telecoms and data protection regulation', *Computer and Telecommunications Law Review*, vol. 1, January 2015, pp. 1–4.

McKinsey Global Institute, The Internet of things: Mapping the value beyond the hype, McKinsey & Company, June 2015. Available at: <www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>, accessed 13 November 2017.

Montgomery, Kathryn C., 'Youth and surveillance in the Facebook era: Policy interventions and social implications', *Telecommunications Policy*, vol. 39, no. 9, 2015, pp. 771–786.

Mordini, Emilio, 'Biometric identifiers for refugees: Political context and ethical challenges', *Keesing Journal of Documents & Identity*, October 2016.

Neville, Andrew, 'Is it a Human Right to be Forgotten? Conceptualizing the World View,' *Santa Clara Journal of International Law*, vol. 15, no. 2, 2017, pp. 157–172.

Nyst, Carly, 'Privacy, protection of personal information and reputation rights,' *Children's Rights and Business in a Digital World Discussion Paper Series*, United Nations Children's Fund, March 2017.

Office of the Privacy Commissioner of Canada, 'Results of the 2016 Global Privacy Enforcement Network Sweep', <www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_160922/>, accessed 13 November 2017.

Office of the United Nations High Commissioner for Human Rights, 'Planned Thematic Reports and call for consultations', <www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx>, accessed 13 November 2017.

Omar, Siti Z., et al., 'Children Internet Usage: Opportunities for Self Development', *Procedia - Social and Behavioral Sciences*, vol. 155, November 2014, pp. 75–80.

Organisation for Economic Co-operation and Development, Recommendation of the Council on the Protection of Children Online, C(2011)155, OECD, 16 February 2012.

Powell, Anastasia, 'Configuring Consent: Emerging Technologies, Unauthorized Sexual Images and Sexual Assault', *Australian and New Zealand Journal of Criminology*, vol. 43, no. 1, April 2010, pp. 76–90.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, 4 May 2016.

Resolution adopted by the United Nations General Assembly, The right to privacy in the digital age, A/RES/68/167, 18 December 2013. Available at: <www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167>, accessed 13 November 2017.

Robin, Pierrine, 'The Participation of Children in Care in the Assessment Process', ch. 10 in *Children's Rights and the Capability Approach: Challenges and Prospects*, edited by Daniel Stoecklin and Jean-Michel Bonvin, Springer, Dordrecht, 2014.

Sartor, Giovanni, and Viola de Azevedo Cunha, Mario, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents', *International Journal of Law and Information Technology*, vol. 18, no. 4, December 2010, pp. 356–378.

Shin, Wonsun, and Kang, Hyunjin, 'Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet,' *Computers in Human Behavior*, vol. 54, January 2016, pp. 114–123.

Singleton, Shaniqua, 'Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD', *Georgia Journal of International and Comparative Law*, vol. 44, no. 1, 2015, pp. 165–193. Available at: <http://digitalcommons.law.uga.edu/gjicl/vol44/iss1/6>, accessed 13 November 2017.

De Souza, Carlos, Pereira, Affonso, Viola, Mario and Lemos, Ronaldo, *Understanding Brazil's Internet Bill of Rights*, 1st ed., Instituto de Tecnologia e Sociedade do Rio de Janeiro, Rio de Janeiro, 2015. Available at: <http://itsrio.org/wp-content/uploads/2015/11/Understanding-Brazils-Internet-Bill-of-Rights.pdf>, accessed 13 November 2017.

Spivack, Nova, 'Web 3.0: The Third Generation Web is Coming', Lifeboat Foundation, 2007, <https://lifeboat.com/ex/web.3.0>, accessed 13 November 2017.

Steeves, Valerie, 'It's Not Child's Play: The Online Invasion of Children's Privacy', *University of Ottawa Law & Technology Journal*, vol. 3, no. 1, July 2007, pp. 169–188.

Steinberg, Stacey B., 'Sharenting: Children's Privacy in the Age of Social Media,' *Emory Law Journal*, vol. 66, 2017, pp. 839–884.

Topelson, Dalia, et al., 'Privacy and Children's Data - An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act', Berkman Center Research Publication No. 23, November 2013. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354339>, accessed 13 November 2017.

United Nations Children's Fund, *Child Safety Online: Global challenges and strategies*, UNICEF Office of Research - Innocenti, Florence, 2011. Available at: <www.unicef-irc.org/publications/pdf/ict_eng.pdf>, accessed 13 November 2017.

United Nations Children's Fund, *Every Child's Birth Right: Inequities and trends in birth registration*, UNICEF, New York, December 2013. Available at: <www.un.org/ruleoflaw/files/Embargoed_11_Dec_Birth_Registration_report_low_res.pdf>, accessed 13 November 2017.

United Nations Children's Fund, *HORIZONS: Selected trends relevant for the wellbeing of children and UNICEF*, UNICEF, September 2017.

United Nations Children's Fund, 'Issue Brief: Protecting children from violence, exploitation and abuse', in *A Post-2015 World Fit for Children: An Agenda for #EVERYChild 2015*, UNICEF, November 2014.

United Nations Human Rights Council Resolution A/HRC/34/L.7/Rev.1, The right to privacy in the digital age, 22 March 2017. Available at: <www.un.org/ga/search/view_doc.asp?symbol=A/HRC/34/L.7/Rev.1, accessed 16 November 2017.

United Nations Office on Drugs and Crime, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, UNODC, Vienna, May 2015. Available at: www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf, accessed 17 November 2017.

United Nations High Commissioner for Refugees, 'Biometric Identity Management System: Enhancing Registration and Data Management', *Division of Programme Support and Management Key Initiatives series*, UNHCR, 2015. Available at: <www.unhcr.org/550c304c9.pdf>, accessed 17 November 2017.

United States Environmental Protection Agency, 'Public Participation Guide: Introduction to Public Participation', <www.epa.gov/international-cooperation/public-participation-guide-introduction-public-participation>, accessed 16 November 2017.

United States of America, Federal Trade Commission, Children's Online Privacy Protection Rule, 16 CFR Part 312, *Federal Register*, vol. 72, no. 12, 17 January 2013, Section 312.5. Available at: <www.ftc.gov/system/files/2012-31341.pdf>, accessed 17 November 2017.

Viola de Azevedo Cunha, Mario, and Itagiba, Gabriel, 'Between privacy, freedom of information and freedom of expression: Is there a right to be forgotten in Brazil?', *Computer Law & Security Review*, vol. 32, no. 4, August 2016, pp. 634–641.

Wetzling, Thorsten, 'Germany's intelligence reform: More surveillance, modest restraints and inefficient controls', policy brief, Stiftung Neue Verantwortung, June 2017. Available at: <www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf>, accessed 17 November 2017.

World Health Organization, *Tackling food marketing to children in a digital world: trans-disciplinary perspectives*, WHO Regional Office for Europe, Copenhagen, 2016. Available at: <www.euro.who.int/__data/assets/pdf_file/0017/322226/Tackling-food-marketing-children-digital-world-trans-disciplinary-perspectives-en.pdf?ua=1>, accessed 17 November 2017.

UNICEF Office of Research – Innocenti
Piazza SS. Annunziata, 12
50122 Florence, Italy
Tel: (+39) 055 20 330
Fax: (+39) 055 2033 220
florence@unicef.org

www.unicef-irc.org
@UNICEFInnocenti
facebook.com/UnicefOfficeofResearchInnocenti

unicef
Office of Research–Innocenti