DATA PROTECTION, PRIVACY AND EUROPEAN REGULATION IN THE DIGITAL AGE

EDITED BY
TOBIAS BRÄUTIGAM AND
SAMULI MIETTINEN

FORUM IURIS

Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut

ISBN 978-951-51-2530-9 (painettu)
ISBN 978-951-51-2531-6 (pdf)
ISSN 1456-842X (painettu)
ISSN 2342-8996 (verkkojulkaisu)

Unigrafia
Helsinki 2016

The general data protection regulation: a partial success for children on social network sites?

Karen Mc Cullagh*

I. INTRODUCTION

Almost 20 years ago, the first social networking site ("SNS") was launched in the U.S. Whilst developers originally intended for SNSs to be used by adults—which they are—they have also become an integral communication platform in the lives of many children in EU Member States. Sharing personal information on SNSs is now a routine activity for many children and, whilst they are computer literate in a way that their parents are often not, a number of concerns have emerged. One of these concerns is that children are vulnerable since they lack the capacity to consent to the terms of SNS membership agreements regarding the processing of their personal data. A further concern is that children's naïve confidence sometimes leads them to take risks—by sharing information about themselves—that adults would not take. This is particularly concerning as children may be ignorant about the fact that their profile and behavioural data is sold to data brokers who use that information to produce targeted adverts—and that these adverts may display age inappropriate content or even may not by recognised by the children as adverts.[1]

Directive 95/46/EC[2] regulates the processing of the personal data of EU citizens, including personal data posted on SNSs. Problematically, it was drafted in a pre-SNS era and neither makes reference to children nor considers them vulnerable data subjects whose personal data should be subject to more stringent processing rules. The absence of specific legal protection for children's data on SNSs sparked concerns that children were ignorantly disclosing personal data and being exposed to profiling and advertising without adequate privacy and data protection safeguards in place. In response to these concerns, provisions aimed at safeguarding children's privacy and data protection rights have been included in Regulation (EU)

* Dr. Karen Mc Cullagh, Lecturer in Law, University of East Anglia, k.mccullagh@uea.ac.uk. The author thanks the anonymous reviewers and editors for their helpful comments.

2016/679 (hereafter "GDPR"),[3] which will come into force on 25 May 2018.

This chapter provides a critical evaluation of the forthcoming measures to address a knowledge gap that exists because of the novelty of these provisions and the fact that scholarship in this area is currently underdeveloped.[4] It begins by providing an overview of SNSs and the problems posed by underage children's access to them. In this regard, it will illustrate that the biological and psychosocial developmental changes that children experience as they progress through their teenage years and develop their capacity for freedom of expression makes them vulnerable to impulsive personal information disclosures and privacy invasions. After this, an exploration of the current legal protections for children's privacy on SNSs from the perspective of privacy as information control will highlight deficiencies in Directive 95/46/EC. This leads to an analysis of the measures in the GDPR to determine whether they will, when introduced, realise the twin goals of legitimising the processing of children's personal data and, at the same time, protecting their fundamental privacy and data protection rights. The compatibility of measures in the GDPR with provisions in the United Nations Convention on the Rights of the Child (1989) ("the UNCRC") and the Charter of Fundamental Rights of the European Union (2000) ("the EU Charter") is considered as these provide a normative framework for evaluating children's legal rights. To comply with both legal frameworks, data protection measures in the GDPR governing children's activities on SNSs should recognise their evolving capacity for freedom of expression and privacy. This would allow them to express themselves with appropriate safeguards in place, ensuring that their best interests are protected and that they are not subject to economic exploitation through activities such as profiling and advertising without consent. Specifically, the analysis presents a critical evaluation of the introduction of an age threshold, below which children are deemed to lack capacity to consent to the processing of their personal data; the conceptual coherence of relying on parental consent for children under the threshold age; the practical implications of Member States being permitted to set the threshold age within a range of ages; and the practical challenges posed by relying on verified parental consent.

The chapter concludes that measures in the GDPR are compatible with provisions in the UNCRC and the EU Charter but that a number of practical challenges remain unsolved. For instance, allowing Member States to set the threshold age means that the goal of simplifying and harmonising the regulatory environment for SNSs operating on a transnational basis will not be fully realised. Equally, reliance on parental consent and the consent of children over the threshold age is conceptually coherent, but it is dependent on the introduction of low-cost age-verification mechanisms being integrated into SNSs. It is also dependent on child data subjects (or

their parents) being digitally literate enough to give unambiguous, specific consent to the processing of their personal data. Relatedly, whilst the GDPR includes measures to promote and increase the digital literacy of both parents and children, it remains to be seen how effective these will be in practice. For these reasons, the GDPR is an improvement on Directive 95/46/EC, but only a partial success.

II. OVERVIEW OF SOCIAL NETWORK SITES

Boyd and Ellison define SNSs as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[5] Members create profiles populated with their personal data (for example, their name, age, sex, location and marital status) alongside a picture and other details about themselves (for example, their favourite movie; which football team they support; which music and films they like; which events they will attend; where they work, or attend(ed) school; and their religious and political affiliations). They can also provide frequent status updates, broadcasting to those in their network what they are doing, how they are feeling, what they like and other personal details. By so doing, they can communicate with friends, and, if they choose, with individuals not personally known to them so that, over time, they become part of an online community of people with common interests.

The first social network site of this type, SixDegrees.com, launched in 1997. Since then, a huge number of social networks sites have emerged (*e.g.* Facebook, iWiW, Myvip, Nasza-klasa and Tuenti) and have attracted a huge number of members. As of July 2015, there were an estimated 2.3 bn. active SNS members.[6] Across the globe, one SNS dominates: Facebook, which has over 1.4 bn. registered members across the globe, of whom an estimated 7.5m. are children are younger than 13.[7] Indeed, a survey of European children aged 9–16 found that Facebook was the most popular SNS in 17 out of 25 EU Member States and the second-most popular in another 5 Member States surveyed.[8] The meteoric growth and popularity of SNSs across all age groups is attributable to the ease with which they facilitate self-expression and socialisation. By enabling members to share content that they have produced themselves and to receive content from others, SNSs encourage members to keep in touch with friends and relatives, to meet new people through interaction with friends of existing SNS friends, and join SNS groups with common interests.

A. CHILDREN'S "GROWING" PRESENCE ON SNSs

Children in EU Member States are using the internet 'at ever younger ages'[9] and join SNSs to be creative, communicate, play, and to establish and maintain friendship and relationship bonds.[10] Indeed, 26% of 9–10 year olds in the EU have an SNS profile[11] and participation increases as children progress through their teenage years—82% of 15–16 year olds in the EU have an SNS profile.[12]

Despite the development of SNSs that are specifically designed for and aimed at children (such as ClubPenguin, Dgamer, WebKinz and Whyville), SNSs such as Facebook—which were originally intended to be used by adults only (in Faceboook's case, membership was initially limited to Harvard University students)—have become popular amongst all age groups, including children. One reason for this is that these sites are more widely known whereas levels of awareness of child-specific SNSs are lower. Another pertinent explanation for children's presence on SNSs designed for adult members is that they offer greater functionality. For example, Club Penguin limits what members can say to a predefined menu of greetings, questions and statements, as well as emotes, actions and greeting cards, and blocks attempts to communicate a phone number or other personally identifiable information, whereas Facebook does not. During adolescence, teenagers frequently experiment with their identity as their sense of freedom of expression, selfhood and independence grows.[13] A profile on an SNS such as Facebook provides a platform for experimentation, in that it allows children to present their thoughts and personal images to a captive, interested audience. In selectively choosing what information to disclose to others, teenagers are able to influence how others perceive them and refine their own sense of identity. Such is the popularity of these sites that children fear social exclusion from their peer group if they are not members. Indeed, peer pressure from other children often results in parents being coerced by their children to give permission to join SNSs and, in some instances, to assist in the registration process, even though the child is underage (U.S.-owned SNSs such as Facebook have set the minimum membership age at 13 to comply with U.S. law[14] namely, the Children's Online Privacy Protection Act 1998, hereafter 'COPPA".). For instance, a U.K.-based IT law expert has confessed that "I found myself readily conspiring with the parent of a 10-year-old to find a way past a block on the child's access to Google Hangout, where it was clear that all her friends were already registered and that it would be 'the end of worthwhile life' if she did not get back on."[15] The combined effect of an individual child's desire to socialise through sharing personal information and the peer pressure to be socially present

means that sharing of personal information on SNSs has become a routine daily activity for many children in EU Member States.

B. SNSs—PRIVACY AS "INFORMATION CONTROL"

Before evaluating the adequacy of both the current and the forthcoming legal measures for protecting EU children's privacy, it is necessary to explain what is meant by privacy in the context of SNSs, since the act of posting personal information—including one's name, date of birth, relationship status, hobbies, and photos which reveal information either explicitly (*e.g.* gender) or implicitly (*e.g.* sexual orientation or religious affiliation)—may seem to conflict with notions of privacy. Privacy is a nebulous, contested, philosophical concept used to describe the legal protection afforded to variety of interests including "the right to be let alone";[16] limited access to the self;[17] secrecy (the concealment of certain matters from others);[18] personhood (the protection of one's personality, individuality, and dignity);[19] intimacy (the control over, or limited access to, one's intimate relationships or aspects of life);[20] and, in the context of data protection laws, the ability to exercise control over information about oneself. Accordingly, in this chapter, the protection of children's privacy interests on SNSs is considered from the perspective of privacy as "information control" or "informational self-determination".[21] Westin defined information control privacy as:

> "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others … [it is] the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others."[22]

Thus, children exercise both their freedom of expression[23] and privacy[24] rights when they decide what personal information to share, and with whom, on SNSs and only suffer a privacy invasion when they lose control over their information. In the context of SNSs, members control their personal data by giving or withholding consent to processing by SNSs and third parties.

III. INADEQUACIES OF DIRECTIVE 95/46/EC

Directive 95/46/EC was drafted before SNSs were invented so it neither anticipated nor provides for the particular privacy and data protection is-

sues caused by this technology. Whilst the UN had completed the UNCRC in 1989, not all EU Member States had ratified it by the time the text of Directive 95/46/EC was agreed, with the effect that children's rights were not fully fledged. As a result, Directive 95/46/EC neither makes reference to children nor considers them data subjects whose personal data should be subject to more stringent processing rules. However, in recent years, a number of child-specific privacy and data protection problems have emerged from SNSs, as set out below.

A. CONSENT—THE ABSENCE OF A "CAPACITY" ASSESSMENT

The processing of adult and child SNS members' personal data by SNSs, data brokers and advertisers is all permitted on the same basis—namely the Directive 95/46/EC, arts. 2(h) and 7 requirements that the data subject has unambiguously given consent. Accordingly, SNS members do not suffer a privacy invasion when their information is processed lawfully—that is, when they freely give specific and informed consent to the processing of their personal data.

For children to give unambiguous consent to personal data processing, they must, however, have the requisite capacity to understand the terms of service and privacy notices on SNS sites (Facebook, for example, refer to its terms of service as a "Statement of Rights and Responsibilities"[25]). Since SNSs were originally designed for adults, the language used in privacy notices and terms of service are typically too complex for children to understand.[26] Moreover, children who might naturally turn to their parents for assistance and explanation frequently cannot do so as Bonneau and Priebusch's analysis of multiple SNS privacy policies found "great diversity in the length and content of formal privacy policies"[27] and, significantly, that "almost all policies are not accessible to ordinary users due to obfuscating legal jargon".[28] In other words, they are usually written in such opaque, impenetrable legalese that most adults struggle to comprehend them. Worse than that, the lengthy and complex nature of these documents dissuades SNS members from reading them—a recent Eurobarometer survey of adults in EU Member States found that 56% of internet and online-platform users do not read terms and conditions and a further 18% read them but do not take them into account.[29] Clearly, if a parent has neither read, nor understood, nor taken into account an SNS's privacy policy, they cannot explain it to their child—arguably invalidating any purported consent given by the child. Equally, if a child cannot understand the complex terms in such notices then they cannot give unambiguous consent to the processing of their

personal data.[30] Relatedly, if a child lacks the knowledge or understanding of data protection rules then they are unlikely to appreciate that SNSs are processing their personal data when they post it online, nor are they likely to appreciate that some personal data is considered "sensitive" and should be subject to more stringent processing conditions (for example, if they upload a photo of a Hanukkah celebration).[31]

B. THE VERIFIABLE AGE PROBLEM

In an attempt to avoid the difficulties associated with establishing children's unambiguous consent to the processing of their personal data, SNS data controllers have sought to forbid children from accessing SNSs by setting minimum age requirements for membership. However, the minimum age set by SNSs varies across EU Member States because of the absence of child-specific provisions in Directive 95/46/EC. Only one EU Member State (Spain) used the leeway available to Member States when transposing the Directive's provisions into national law to include a minimum age—in this case, 14 years old, beyond which a child can validly consent to the processing of their personal data in national law.[32] As a result, the Spanish-owned SNS Tuenti has set the minimum membership age at 14 years old. No other Member State established such an age limit. Consequently, as EU-owned SNSs emerged, and U.S.-owned SNSs spread into EU Member States, variations in minimum ages arose, with 13 being the most common minimum age—reflecting the fact that the U.S.-owned SNS Facebook has set the minimum membership age at 13 to comply with COPPA.

Although SNSs stipulate that they forbid membership of underage users, they do not usually require age and identity verification or express parental consent as a precondition to the registration of an account by children. Rather, they rely on self-certification by children to prove that they are over the permitted age—*e.g.* through tick-boxes or date of birth entry boxes that reject under-age entries. Some sites never actually ask the user to confirm their birth date, relying instead on a statement in their terms and conditions: "You must be at least 13 years old to use the Service." SNSs such as Facebook have, however, admitted that current measures to identify and prevent access by underage users are not wholly successful because children lie about their age: "There are people who lie, there are people who are under 13 accessing Facebook. Facebook removes 20,000 people a day, people who are under-age."[33] Verifying the age of those under 18 also poses practical challenges:

> "[T]here are not really mechanisms in most Western societies to verify whether you are a kid; they are all geared towards verifying that you are an adult, whether with a driver's licence or some-

> thing else. So we do things like 'age gating', so that if you put in the wrong age once, a cookie on your machine will block you. We also, through algorithms, try to detect patterns of speech and things that look like you are not likely to be over 13, and we remove people. We also take complaints from teachers or other people in the network that you are involved in if you do not belong there, and we remove people."[34]

Unsurprisingly, a survey of European children aged 9–16 found that 38% of 9–12 year olds and 77% of 13–16 year olds have an SNS profile, despite the imposition of minimum age membership restrictions.[35] U.K. statistics confirmed a similar pattern with 72% of 10–18 year olds (and 49% of under-13 year olds) having a Facebook profile—and 78% of 10–12 year olds in the U.K. having a social media account of some kind.[36] Evidently, there are many underage children on SNSs whose lack of understanding of the terms of service and privacy notices means that they cannot lawfully consent to the processing of their personal data.

C. DATAFICATION OF RELATIONSHIPS, PROFILING & ADVERTISING

A further problem is that SNS members (both adults and children) who have either not read or not understood the terms and conditions or privacy policies tend to lack awareness that whilst SNSs are "free" in the sense that they typically do not have membership or subscription fees, they are advertisement-supported communication mediums that profit from the "datafication of relationships." "Datafication" refers to "the ability of networked platforms to render into data many aspects of the world that have never been quantified before—not just demographic or profiling data yielded by customers in (online) surveys, but automatically derived metadata from smart phones such as time stamps and GPS-inferred locations".[37] In other words, SNSs can collect, analyse and sell prodigious amounts of personal data generated by its members to data brokers and specialised data analytics and metrics companies who use the profile and behavioural data to produce personalised, targeted, adverts.[38]

A particularly problematic aspect of this business model is that it encourages SNSs and third parties to collect information using surreptitious techniques, *e.g.* through "likes" and quizzes. Children (and indeed most adults) are unlikely to be aware that inferences can be made from their disclosures—for instance, that "liking" curly fries on Facebook is indicative of high intelligence[39] or that "likes" can be used to predict race or sexual

orientation with a high degree of accuracy[40]—and that both disclosed and inferred information can be used to generate profiles and produce targeted adverts. The exposure of children to highly impactful personalised advertisements has heightened concerns about the "commercialisation" of childhood.[41]

Additionally, one of the ways in which advertisers operate on social network sites is through "advergames"—online video games created in order to promote a brand, product or organisation through an immersive marketing message within a game. For example, the Krave Krusader game was used to promote cereal to Facebook members.[42] Whilst advertisers do use measures such as adult verification schemes (also known as age gating) to try to prevent underage children from being exposed to age-inappropriate advergames, children who have provided false age details to SNSs are equally likely to have the wherewithal to fool age-gating mechanisms. This is problematic as research has confirmed that some children as old as 15 do not recognise advergames as advertisements, reinforcing persistent fears about children who lack capacity being unwittingly exposed to and influenced by highly impactful advertising.[43]

A related, but unintended, consequence of children being on SNSs intended for adults is that they are exposed to age-inappropriate advertisement content. For instance, a small-scale study by the U.K. Advertising Standards Authority found that age-restricted adverts (*e.g.* for alcohol) were viewed by under-18 SNS members despite the advertisers efforts to prevent this—primarily because children presented false age information to SNSs when registering for membership.[44] Similarly, a recent EU Commission sponsored study found that children were exposed to child-inappropriate (commercial) content, sexual content and alcohol-related advertisements.[45] This is problematic because research on adolescent psychological and neurobiological development indicates that many adolescents "look to advertising models to identify adult-only products and activities that will help them to project a more mature and positive self image and to boost their self esteem."[46] It has further confirmed that adolescents are more prone to making poor decisions when emotionally aroused. Since digital marketing "purposefully evokes high emotional arousal and urges adolescents to make consumption decisions under high arousal, it exacerbates this problem."[47]

The silence of Directive 95/46/EC on issues such as online behavioural advertising and profiling constitutes a threat to children's autonomy, dignity and ability to control their personal information. Thus, there was a need to introduce a Regulation to speak to and address these issues.

D. EFFECT OF LEGISLATIVE INADEQUACIES

In summary, Directive 95/46/EC and related national data protection laws were considered problematic because they did not provide adequate privacy and data protection safeguards for children on SNSs. Also, inconsistent transposition of the Directive's provisions into Member States national laws gave rise to multiple regulatory-compliance burdens for SNSs operating on a transnational basis, resulted in unevenly applied protection for children and undermined the EU's internal market goal of harmonised legislation. Consequently, there were calls for reform of Directive 95/46/EC and for it to be replaced by a Regulation to give individuals the operational means to ensure that they are fully informed about what happens to their personal data and enable them to exercise their rights more effectively, with specific additional provisions to safeguard the privacy and personal data of children.

IV. IMPETUS FOR THE INTRODUCTION OF THE GDPR

The GDPR seeks to realise the political and economic goals of "help[ing to] stimulate the Digital Single Market in the EU by fostering consumer trust in online services and legal certainty for businesses based on clear and uniform rules."[48] The European Commission recognised that personal data is a highly valuable economic asset—such is its value that it is sometimes referred to as the "oil of the internet and the new currency of the digital world."[49] For instance, the European Commission has confirmed that "the *value of European citizens' personal data* has the potential to grow to nearly *€1 trillion annually by 2020*."[50] [Emphasis in original.] Its increasing economic value means that personal data is fast becoming a valuable resource in the 21st century—one from which SNSs will seek to harvest and profit. The collection and processing of personal data for profiling and advertising purposes is already a hugely profitable business model. Facebook earned an estimated $8.3 bn. from advertising in 2015[51] and forecasts suggest that by 2017 global SNS advertisement spending will reach $35.98 bn.[52]

Despite the keenness to exploit the economic potential of personal data, in November 2011, the then EU Justice Commissioner, Viviane Reding, expressed concern about the growth of digital advertising and the lack of public understanding that it is contingent on the harvesting and analysis of personal information.[53] Thus, one of the chief concerns during the consultation process to replace Directive 95/46/EC with the GDPR was the growth of SNSs such as Facebook and how data protection rules applied to

them. The European Commission recognised that SNSs offer both economic opportunities for businesses and creative communication and expression opportunities for individuals. Any revision of Directive 95/46/EC should therefore seek to create an enabling environment for such activities that legitimises the processing of such personal data whilst also affording effective privacy and data protection to SNS members (including an exemption for individuals using social network sites in a personal capacity[54]).

In addition, there was support for the introduction of specific rules to strengthen the data protection measures available to children as a Eurobarometer survey of European citizens had confirmed that 95% of Europeans "believe that *under-age children should be specially protected* from the collection and disclosure of personal data" and 96% agreed that "*minors should be warned* of the consequences of collecting and disclosing personal data."[55] [Emphasis in original.]

The European Commission had also previously noted that children need special protection because research had confirmed that children may be "less aware of risks, consequences, safeguards and rights in relation to the processing of personal data."[56] Furthermore, self-regulatory initiatives such as the Safer Social Networking Principles for the EU and the Coalition To Make The Internet A Better Place For Kids have proven only partially successful.[57] These initiatives were developed in furtherance of the European Commission's European Strategy for a Better Internet for Children which aimed to give children greater protection from violations of their privacy and the potential abuse of their personal information.[58]

Moreover, although children's human rights were not fully fledged when Directive 95/46/EC was introduced, they have, in recent years, been integrated into the legal framework of Member States. For instance, all EU Member States have ratified the UNCRC, which grants all children a comprehensive set of rights in recognition of the fact that they are vulnerable and in need of protection from exploitation. By ratifying it, all EU Member States have agreed to make all laws, policy and practices compatible with it (although a child cannot bring legal proceedings relying only on the UNCRC, courts, tribunals, and other administrative bodies should refer it to it when making decisions that affect children).

The UNCRC defines a child as "every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier."[59] It recognises children as both "being" and "becoming" privacy rights holders.[60] The right to privacy for children is recognised in art. 16, and when art. 16 is read in conjunction with art. 3(1)—which stipulates that, in all actions concerning children, "the best interests of the child shall be a primary consideration"—or art. 5—which provides that parents are responsible for providing appropriate direction and guidance to children "in a manner consistent with the evolving capacities of the child"—it is clear

that children are also "becoming" rights holders in the sense that as they mature they develop the capacity to manage decisions relating to their right to privacy. This dual status was recognised by Sir Thomas Bingham M.R. in *In re S*[61] where he stated that a "judicious balance" had to be struck between recognising that "children are human beings in their own right" but that "a child is, after all, a child."[62] Other notable provisions in the UNCRC include art. 18(1), which obliges States to recognise that parents have the primary responsibility for the upbringing and development of children, and art. 18(2), which obliges States to provide appropriate assistance to parents. Also, art. 32 obliges States to "recognize the right of the child to be protected from economic exploitation" and must, under art. 32(c), provide for appropriate penalties or other sanctions. Collectively, these provisions seek to strike a delicate balance in recognising children as privacy rights holders who, in some circumstances, are also "becoming" rights holders and are in need of protection from harms like economic exploitation if they lack the capacity to give unambiguous consent to the processing of their personal data. The Court of Justice of the European Union has expressly recognised the need to respect children's rights and requires EU law to take due account of the UNCRC.[63]

Furthermore, in 2009, the EU Commission marked the 20th anniversary of the UNCRC by endorsing the promotion and protection of children's rights as a policy priority.[64] Indeed, the Lisbon Treaty imposes upon the EU, when exercising its competences, an obligation to promote the protection of the rights of the child.[65] The Lisbon Treaty introduced amendments to Article 6 of the Treaty on European Union, the effect of which is that the EU Charter of Fundamental Rights is now legally binding, having the same status as primary EU law.

The EU Charter enshrines certain political, social, and economic rights for EU citizens and residents into EU law. For instance, art. 7 sets out a right to privacy, art. 8 sets out a right to data protection and art. 11 provides a right to freedom of expression. Specifically in relation to children, the Charter, art. 24(1) states that children have the right to the protection and care necessary for their well-being and that their views shall be "taken into consideration on matters which concern them in accordance with their age and maturity". Meanwhile, art. 24(2) states that that "[i]n all actions relating to children … the child's best interests must be a primary consideration." Institutions of the EU and its Member States must legislate in compliance with the Charter and the EU's courts will strike down legislation adopted by the EU's institutions that contravenes it.

V. THE GDPR: INFLUENCE AND IMPACT OF LOBBYING

Important arguments have been, and are continuing to be, made regarding whether the decision to extend participation in the personal data economy is in children's best interests,[66] particularly as "the realization of children's rights is not an automatic consequence of economic growth and business enterprises can also negatively impact children's rights."[67] In this Part, the success of the GDPR is considered by assessing the extent to which it complies with the principles and provisions in the UNCRC and the EU Charter, as these provide a normative framework for evaluating children's legal rights. The discussion will illustrate that the GDPR is ambitious in that it the first EU legal instrument to afford specific privacy and data protection to children, whilst also legitimising the processing of their personal data so that data controllers and third parties can realise its economic value in furtherance of the goals of the Digital Single Market. The analysis below will, however, illustrate that measures concerning children in the GDPR were shaped, and arguably weakened, through intense lobbying by industry representatives who were keen to maintain the legal and business *status quo*, and further that EU lawmakers are, to an extent, responsible for allowing this to happen because they did not make use of available mechanisms, such as impact assessments, to inform the law-making process.

A. RECOGNITION OF CHILDREN'S VULNERABILITY AND EVOLVING CAPACITY TO CONSENT

In recognition of children's vulnerability due to their evolving capacity to understand and consent to the processing of their personal data, the first draft of the GDPR released by the European Commission in January 2012[68] observed, in recital 29, that "[c]hildren deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data." It further proposed to draw upon the UNCRC, art. 1 definition of a child of "every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier." The proposal triggered submissions from industry representatives, including the American Chamber of E-Commerce to the European Union[69] and Facebook,[70] that the age of a child be lowered from the age of 18 to 13 on the basis that "[a] threshold of 13 years of age for a child reflects more accurately the prevailing standard

in Europe (though there are some variations)."[71] In response, a revised draft of the GDPR published by the Council on 4 December 2015[72] removed reference to the UNCRC definition of children as those under 18 years of age. Lobbying by industry representatives to maintain the threshold age of 13 set by the dominant SNS provider, Facebook, was to be expected since raising the threshold age would increase their compliance burden and potentially reduce their membership base.

The first draft of the GDPR released by the European Commission in January 2012 further proposed in art. 8 that, "in relation to the offering of information society services directly to a child, *the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian.*" [Emphasis added.] A related Impact Assessment created as a Commission Staff Working Paper indicated that the proposal to set the age of consent at 13, below which parental authorisation would be required, took "inspiration for the age limit from the current US Child Online Privacy Protection Act of 1998 and are not expected to impose undue and unrealistic burden upon providers of online services and other controllers."[73] Industry representatives were naturally supportive of this proposal since a harmonised age would reduce the compliance burden for SNSs operating across multiple jurisdictions. For instance, the Advertising Education Forum reported that "[c]hildren should be defined as under 13, according to international and EU best practice."[74] Similarly, an article in Games Industry noted that an age limit of 13 would bring EU law into line with the age set in the U.S. under COPPA, stating that "[t]his will bring the EU's data protection regime more closely in line with the US's Children's Online Privacy Protection Act of 1998 which places similar requirements on any company that wishes to process any personal information relating to a child under the age of 13 years."[75]

Given that problems with age-related content provisions in COPPA 1998 are widely known,[76] the apparent willingness of EU legislators to adopt similar provisions without scrutinising whether they were appropriate and fit for purpose seems flawed. However, to the surprise of many, the revised draft of the GDPR published by the Council on 4 December 2015, art. 8 proposed to set the threshold age at a higher age of 16:

> "[I]n relation to the offering of information society services directly to a child, *the processing of personal data of a child below the age of 16 years shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child*." [Emphasis added.]

The proposed higher age limit drew a torrent of criticism from industry representatives and child protection experts such as Janice Richardson, former coordinator of European Safer Internet Network, on the basis that "moving

the requirement for parental consent from age 13 to age 16 would deprive young people of educational and social opportunities in a number of ways, yet would provide no more (and likely even less) protection."[77] Similarly, Larry Magid, chief executive of ConnectSafely.org, expressed concern that it would result in "banning a very significant percentage of youth and especially the most vulnerable ones who will be unable to obtain [parental] consent for a variety of reasons" from social network sites.[78]

The common theme of criticism from these child protection experts was that the proposed threshold age was too high, with the effect that some 16-year-old children who had the capacity to understand terms of service and consent to the processing of their personal data by SNSs would be denied the opportunity to do so because they were deemed in law to lack capacity—instead being forced to seek parental consent to join SNSs. Consequently, a further revised text was hastily issued and agreed upon by the European Parliament, the Council, and the Commission on 15 December 2015.[79] The revised text, in art. 8(1), appears, in response to the criticisms and complaints about the introduction of a threshold age of 16, to make a concession by setting the default threshold age at 16 but allowing individual member states to set their own limit, with 13 being the lowest option. The final text of the GDPR, art. 8(1) reads:

> "[I]n relation to the offer of information society services directly to a child, *the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*
>
> *Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*" [Emphasis added.]

Notably, and much to the disappointment of civil society and child protection experts,[80] neither the Commission nor the Council conducted an impact assessment to consider the implications of including or excluding an age-based definition of children in the GDPR 2016/679—or the merits of setting the threshold age at 13, 16 or any age in between those two ages. Instead, the threshold age of consent appears to have been influenced by the representations of industry lobbyists rather than fact-based, impact-assessment evidence. This is problematic as capacity to consent to data processing by SNSs should not vary on a country-by-country basis since there is no obvious reason why children should mature more or less quickly in different countries. The fact that there are differences in the age of consent is a reflection of differing historical and cultural attitudes to child maturity rather than a modern-day evidence-informed approach to capac-

ity—and it is an approach that EU Member States are being challenged to reconsider through ratification and adoption of the UNCRC principles. An opportunity to do so in the context of data protection laws has arguably been wasted due to the failure of the Commission or Council to seek an impact assessment on the merits and implications of setting a threshold age below 18. On a more positive note, recital 58 and art. 12 seek to address the problem of terms of service and privacy notice being written in complex legalese by requiring that information and communications regarding the processing of children's data "should be in such a clear and plain language that the child can easily understand" (recital 58). This will assist children who are over the default age of consent yet under 18 who might otherwise struggle to comprehend terms of services and privacy notices. It will also increase the likelihood that they will be in a position to form the requisite consent to the collection and use of their personal data by enabling them to understand and assess whether or not the perceived benefit of using the SNS is worth the privacy trade-off.

It remains to be seen whether individual lawmakers in Member States will conduct impact assessments and seek independent, research-informed evidence when setting the threshold age in their countries. As outlined above, research has already confirmed that some children under the age of 15 do not have the mental capacity to identify advergames as a form of advertisement,[81] providing a rationale for Member States to seek impact assessments on the merits of setting the default age of consent at 15 years of age or higher. It is to be hoped that individual Member States will conduct impact statements since doing so without an evidence-based rationale has the potential to result in the default age being set either set too low or too high to adequately reflect the capacity of children. If it is set too high, *e.g.* at 16, it may have the unintended consequence of creating a conflict of interest between parents and children by requiring parents to violate their children's privacy during the later adolescent years when they have a reasonable expectation of privacy from their parents. Equally, where the default age is set too low, *e.g.* at 13, when the child does not have the maturity and mental capacity to comprehend terms of service and privacy notices, then the child is likely to be exposed to privacy and data protection harms.

A threshold age of consent: individual assessment v age fixed in law

Through the introduction of a threshold age-of-consent requirement, the GDPR seeks to give effect to the "evolving capacities" model of "being" and "becoming" privacy rights holders set out in both the UNCRC and the EU Charter. Application of the evolving capacities model to consent to personal

data processing in the context of SNSs would result in a graduated approach to consent. Under this approach, very young children would be deemed to lack the capacity to consent to the processing of their personal data but parents (or those with parental responsibility) would be empowered to give consent on their behalf. As for older children, their capacity to consent to the processing of their personal data on SNSs would be determined on an individual basis by an independent body, *e.g.* a national regulator, psychologist or children's commissioner. During the negotiation phase of agreeing the text of the GDPR, calls were made by the European NGO Alliance for Child Safety Online ("eNACSO") and others[82] for children's consent to the processing to be determined on an individual basis because—

> "[i]t seems unlikely that fixing a single age for 'privacy maturity' in relation to everything that happens between childhood and adulthood is going to be the right answer to the online privacy challenge. Between the ages of 12 and 18 young people do a lot of growing up, and different privacy standards or parental consent standards should be applied to persons of different ages or in relation to different types of activity undertaken at different ages within that span."[83]

However, it would not be practical or feasible to require a court or independent regulator to assess a child's capacity each time a child subscribes to an SNS or other information society service that processed their personal data. eNACSO conceded that even if the SNS operators agreed to undertake the task of assessing capacity themselves, it would not prove politically acceptable nor would it provide a practical solution. The "evolving capacities" concept was developed when the working assumption was that every child could be seen and individually assessed by a person competent to make an informed decision about the child, but that does not reflect the reality of the internet:

> "In remote environments such as the internet for now and the foreseeable future that is a practical impossibility. And even if it was not, the ability of, say, private companies to make such intimate assessments would raise major concerns about how and where the information thus obtained might be stored, who might have access to it and for what purposes?"[84]

Accordingly, instead of requiring an independent body to assess the capacity of a child, the GDPR stipulates that children who have attained the threshold age, fixed in law by the Member State in which the child lives, have the capacity to consent to the processing of their personal data. Concomitantly, children below the threshold age are deemed to lack capacity to consent to the processing of their personal data and an *onus* is placed on those

with parental responsibility for children below that age to give or withhold consent to children accessing such sites. In so doing, the GDPR seeks to give effect to a modified but fit for purpose application of the "evolving capacities" model of "being" and "becoming" privacy rights holders set out in both the UNCRC and the EU Charter.

B. PARENTAL EXERCISE OF CONSENT—POTENTIAL CHALLENGES

The art. 8(1) requirement of parental consent for children under the threshold age also complies with the evolving "capacities concept" embodied in the UNCRC, art. 18(1), which obliges States to recognise that parents have the primary responsibility for the upbringing and development of children. Arguably, empowering parents in the GDPR, art. 8(1) to give or withhold consent to the processing of their children's data (when the child is below the threshold age) reflects the current practice of parents making decisions regarding the schooling or health care of their children that are in "the best interests of the child"[85] and "consistent with the evolving capacities of the child".[86] Thus, the requirement for parental consent to the processing of personal data of children deemed to lack capacity is merely an extension of the traditional parent/child relationship to the digital era. Theoretically, it constitutes an improvement on the current practice of children self-declaring or confirming their age to SNSs, since many underage children regularly flouted these rules to gain underage access to SNSs. However, two aspects of this provision are potentially problematic: low levels of parental digital literacy and the practical challenge of obtaining "verifiable" parental consent.

(i) Low levels of parental digital literacy

The appropriateness of parents, or those with parental responsibility, exercising consent to the processing of children's data depends on their digital literacy. Concern has been expressed that "this legislation is shaped by a romanticization of parent-child relationships and an assumption of parental knowledge that is laughable."[87] It is often the case that children are more "tech savvy" than their parents. Indeed, a U.K. survey found that "more than four in ten parents of a child aged 5–15 who goes online … agree with the statement: 'My child knows more about the Internet than I do.'"[88] Plus, as outlined above, most adults do not read privacy policies and those that do often struggle to understand them, so many parents are ignorant of the privacy risks posed and are arguably not best placed to supervise their

children's access to SNSs or give consent to the processing of children's personal data.[89]

Moreover, a new, SNS-related phenomenon—referred to as "sharenting"—has emerged in recent years. Sharenting is the use of social media by parents to over-share detailed information about their children's lives online, often without their children's knowledge or consent.[90] Arguably, parents who engage in "sharenting" are incapable of educating their children of the privacy and data protection implications of posting personal information on SNSs and therefore are not best placed to supervise their children's SNS activities.

However, whilst the problem of "sharenting" should not be minimised (a case of a teenager suing her parents for sharing embarrassing childhood photos on Facebook is ongoing in Austria[91]), it is important to remember that, in law, adults are expected to have the capacity to make informed decisions about their own freedom of expression and privacy choices. It would not be reasonable to expect lawmakers to establish tribunals to assess whether every adult exercising parental responsibility has the capacity to understand terms of service and privacy notices every time they, or a child under their care, wanted to sign up for a new website or post personal information on an SNS, in the same way that it would not be appropriate for a State to interfere with other parenting choices (*e.g.* bedtimes, food choices and leisure activities) that parents make for their children. Nevertheless, Member States and SNSs have a responsibility to support parents through the provision of information to increase their digital literacy, as, in 2013, the Committee on the Rights of the Child stated that whilst "there is no international legally binding instrument on the business sector's responsibilities … all businesses must meet their responsibilities regarding children's rights and States must ensure they do so."[92] Similarly, the UNCRC, art. 18(2) obliges states to provide appropriate assistance to parents.

The GDPR, art. 57(1)(b) attempts to address the digital literacy problem by obliging Member States' supervisory authorities to "promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing. *Activities addressed specifically to children shall receive specific attention*." [Emphasis added.] Additionally, the GDPR, art. 40 states that Member States, supervisory authorities, the European Data Protection Board and the Commission shall "encourage" the creation, by bodies representing data controllers, of codes of conduct specifying "the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained". The development of informative educational campaigns and codes of conduct will be key to increasing levels of parental digital literacy.

(ii) The practical challenge of obtaining "verifiable" consent

The provision that is likely to provide the greatest operational challenge is art. 8(2), which states that "[t]he controller shall make *reasonable efforts to verify* in such cases [where a child is under the age of consent] *that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology*." [Emphasis added.]

This provision poses two challenges for SNSs: first, how to reliably determine whether a child is over the default age of consent; and, secondly, in the case of a child under the default age, how to reliably determine that consent was given by a parent (or someone with parental responsibility). Problematically, at present, there is no effective framework for child age verification in operation across EU Member States,[93] nor is there political will for age verified databases to be compiled by either public authorities or private entities. Mechanisms that allow SNSs to confirm that the person who is claiming to be a parent, or to exercise parental responsibility, is over 18 do exist, but they cannot be used to confirm a parental responsibility link to a child. For instance, an adult could provide a copy of their passport or driving licence, or their name, address or credit card details to an SNS. These details could be checked against records held by official agencies (such as the passport office, the DVLA, the electoral register or credit reference agencies) to confirm that the details match an existing record for someone over the age of 18, but it could not be used to confirm a parental responsibility link with a child whose data the SNS seeks to process.

Thus, whilst parental permission may provide an appropriate and effective safeguard for younger children, the focus on parental consent for pre-teens and teenagers is likely to prove ineffective as the evidence above suggests that they are adept at falsifying age credentials and will have the technical wherewithal to falsify parental consent. Until these problems are resolved, this aspect of the GDPR will not be effective.

There is another, as yet unresolved, challenge: When the GDPR takes effect on 25 May 2018, this provision is also likely to generate confusion and conflict between parents and children in countries where the default age is raised from a currently lower age, since it is unclear whether it will oblige children who had previously been deemed to have the capacity to access SNSs to seek parental permission to do so going forward.

Given the widely known, and as yet unsolved, challenges regarding verification of children's ages and the associated problems of verifying that it is in fact a parent or person with parental responsibility who is giving consent to the processing of a child's data, law makers should have taken an alternative approach. It would have been better to encourage children to provide their true age to SNSs and require SNSs to offer alternative, child-friendly services. This could have been done, for example, by offering

platforms to facilitate expression and socialisation by children and permit SNSs to collect performance data from children without parental permission so as to enhance the service offered, but mandate that no profiling and tracking of children's data can be conducted for commercial purposes.

C. DATAFICATION OF RELATIONSHIPS, PROFILING & ADVERTISING REVISITED

On a positive note, the GDPR has attempted to address the problem of datafication of relationships through the inclusion of a right of erasure (also referred to as a right to be forgotten).[94] Notably, this right embodies the evolving capacities principle by recognising that as children reach maturity and develop a greater sense of privacy, they may wish to withdraw consent to some previous disclosures of personal information continuing to be available. The GDPR states that—

> "[t]hat right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child."[95]

Behavioural advertising and profiling of children are also prohibited in recital 38—which states that "specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child"—and recital 71—which states that children should not be the subject of profiling. This accords with an opinion issued by the Article 29 Working Party that children should not be exposed to behavioural advertising and profiling.[96] Whilst the prohibition on online behavioural advertising and profiling are welcome developments, further steps will have to be taken to ensure their success. For instance, clear policy guidelines will need to be issued and enforcement mechanisms will need to be used. Given the lack of effective age-verification measures, ensuring that children under the threshold age are not exposed to age inappropriate advertisements or subject to profiling will not be an easy task. It will require close, on-going, co-operation between SNSs and third party advertisers.

VI. CONCLUDING REMARKS

In conclusion, the GDPR is a positive development, in that it is the first EU legal measure that seeks to afford specific privacy and data protection to children whilst also legitimising the processing of their personal data so that data controllers and third parties can realise its economic value in furtherance of the goals of the Digital Single Market. However, the result is an inherent and unresolvable tension between fostering economic objectives and ensuring that fundamental rights are not eroded.

The GDPR provides a legal and regulatory framework that is conceptually compatible with UNCRC and the EU Charter. Specifically, it recognises children as both being and becoming rights holders, and seeks to gives effect to the evolving capacities model of children's rights. It does this by stipulating that young children lack the capacity to consent to the processing of personal data and that the supervision of children's access to SNSs is a natural duty of modern-day parents, whilst also recognising that older children, who have the capacity to make decisions regarding the privacy implications of the disclosure of their personal data, need both privacy from their parents and assistance from SNSs to comprehend privacy notices and unambiguously consent to the processing of their personal data.

However, there are some problematic aspects to the GDPR. First, allowing member states to fix the threshold age between 13–16 years is conceptually incoherent. A regulation that seeks to give effect to children's evolving capacities for decision-making should be guided by expert advice on children's capacities, rather than set ages according to Member States' preferences. Thus, a key recommendation of this chapter is that the European Commission and/or Member States' supervisory authorities sponsor research into children's interaction with SNS's privacy notices and their capacity to understand privacy notices, information regarding profiling, advertising and advergames—and then use the findings to fix a minimum threshold age of capacity to consent to the processing of personal data in member states.

Fixing a uniform threshold age of consent in all Member States would have the additional benefit of reducing the compliance burden for SNSs operating on a transnational basis that would otherwise be obliged to alter their terms and conditions and age verification mechanisms in different Member States. It would also minimise the attendant supervisory problems for national supervisory authorities.

The GDPR requires Member States, SNS data controllers and parents to take practical steps to give effect to the provisions regarding verified consent. Success will depend on the development of a low-cost age-verification process capable of being integrated into SNSs that operate on a transnational basis. This is where other unresolved challenges lie: How to

improve the digital literacy of parents and how to enforce verifiable age and consent provisions. The current practice of children (and children assisted by parents) providing false age details to SNSs will not end unless the digital literacy of parents and children increases. Likewise, parents will only be in a position to give consent to the processing of their children's data if they are digitally literate and possess the requisite knowledge to understand terms of service and privacy notices. Overcoming these challenges will require close cooperation and dialogue between national data protection regulator, SNS owners and related industry representatives, and child protection experts. Until then, the GDPR should be viewed as a welcome but only partially successful legal measure.

[1] Emilee Rader, "Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google" (2014). Paper published in *Proceedings of the Tenth Symposium on Usable Privacy and Security*. Available online at <https://www.usenix.org/system/files/conference/soups2014/soups14-paper-rader.pdf>, accessed 9 November 2016.

[2] 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 L281/31.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[4] Verdoodt and others considered the compatibility of a draft text of the GDPR with the UN Convention on the Rights of the Child and the EU Charter of Fundamental Rights when the ability to consent in certain situations was restricted to those over the age of 13, below which parental consent would be required was proposed: Valerie 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.

[5] Danah Boyd & Nicole Ellison, "Social Network Sites: Definition, History, and Scholarship" (2007) 13 (1) Journal of Computer-Mediated Communication 210, 211.

[6] Kit Smith, "Marketing: 96 Amazing Social Media Statistics and Facts for 2016" (*Brandwatch*, 7 March 2016) <https://www.brandwatch.com/2016/03/96-amazing-social-media-statistics-and-facts-for-2016/>, accessed 9 November 2016.

[7] "That Facebook friend might be 10 years old, and other troubling news" (*Consumer reports magazine*, June 2011) <http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/facebook-concerns/index.htm>, accessed 9 November 2016.

[8] In this survey, a random stratified sample of 25,142 children aged 9–16 who use the internet, plus one of their parents, was interviewed during Spring/Summer 2010 in 25 European countries: Sonia Livingstone, Leslie Haddon, Anke Görzig and Kjartan Ólafsson, "Risks and safety on the internet: The perspective of European children: Full findings and policy implications from the *EU Kids Online* survey of 9–16 year olds and their parents in 25 countries" (EU Kids Online, LSE 2011). Available online at <http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf>, accessed 9 November 2016.

[9] *ibid*. 5.

[10] Ito Mizuko & others, "Living and Learning with New Media: Summary of Findings from the Digital Youth Project" (The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning, November 2008). Available online at <http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf>, accessed 9 November 2011; Malene Larsen, "Understanding Social Networking: On Young People's Construction and Co-construction of Identity Online" in K. Sageetha (ed), *Online Networking – Connecting People* (Icfai University Press 2008); Amanda Lenhart & Mary Madden, "Teens, Privacy and Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace" (*PEW/Internet*, 18 April 2007) <http://www.pewtrusts.org/~/media/legacy/uploadedfiles/wwwpewtrustsorg/reports/society_and_the_internet/pipteensprivacysnsreportfinalpdf.pdf>, accessed 9 November 2016; Kelly Mendoza, "'WATZ UR NAM?': Adolescent Girls, Chat Rooms, and Interpersonal Authenticity" (2007) Media Education Lab Working Paper Series 403. Available online at <http://www.mediaeducationlab.com/sites/mediaeducationlab.com/files/403_WorkingPapers_Mendoza.pdf>, accessed 9 November 2016; Danah Boyd, "Why Youth [Love] Social Network Sites: The Role of Networked Publics In Teenage Social Life" in David Buckingham (ed), *Youth, Identity, and Digital Media* (The John D. and Catherine T. MacArthur Foundation Series on

Digital Media and Learning, The MIT Press 2008); Danah Boyd, *It's Complicated: The Social Lives of Networked Teens* (Yale University Press 2014).

11 Livingstone, Haddon, Görzig, & Ólafsson (n 8) 5.

12 *ibid*. See also Ofcom, "Children and Parents: Media Use and Attitudes Report" (November 2015) <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/children-parents-nov-15/childrens_parents_nov2015.pdf> 80, accessed 9 November 2016. This survey of U.K. children in 2014–15 reported similar findings: 1% of 3–4 year olds, 2% of 5–7 year olds, 21% of 8–11 year olds and 74% of 12–15 year olds had an SNS profile.

13 Lauren Spies Shapiro & Gayla Margolin, "Growing Up Wired: Social Networking Sites and Adolescent Psychosocial Development" (2014) 17 (1) Clin. Child Fam. Psychol. Review 1.

14 Children's Online Privacy Protection Act 1998, 15 U.S.C. ch. 91 ("COPPA").

15 Laurence Eastham, "Age and Online Access" (*Society of Computers & Law: Editor's Blog*, 3 August 2015) <http://www.scl.org/site.aspx?i=bp43363>, accessed 9 November 2016. See also, Danah Boyd & Alice Marwick, "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies" (Oxford Internet Institute's A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society conference, 22 September 2011) 8. Available online at <http://www.ssrn.com/abstract=1925128>, 9 November 2016.

16 Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4 (5) Harvard Law Review 193.

17 Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Reissue edn, Vintage Books 1983), 10–11.

18 Richard Posner, *The Economics of Justice* (Harvard University Press 1893), 271.

19 Jeffery Reiman, "Privacy, Intimacy, and Personhood" (1976) 6 (1) Philosophy & Public Affairs 26.

20 James Rachels, "Why Privacy is Important" (1975) 4 (4) Philosophy & Public Affairs 323.

21 The concept of "informational self-determination" was first espoused in BVerfGE 65, 1 vom 15.12.1983 (Volszählungsurteil). An English language translation is available in Eibe Riedel, "New Bearings in German Data Protection. Judgment of the Federal Constitutional Court, Karlsruhe, of 15 December 1983" (1984) 5 Human Rights Law Journal 37 and 94. Although this case pre-dates SNSs, the concept of "informational self-determination" remains relevant and appropriate in the Web 2.0 era.

22 Alan Westin, *Privacy and Freedom* (Atheneum 1967) 7. See also: Arthur Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (Ann Arbor: University of Michigan Press 1971) 25; Lee Bygrave, "The Place of Privacy in Data Protection Law" (2001) 24 (1) University of New South Wales Law Journal 277. Available online at <http://www.unswlawjournal.unsw.edu.au/sites/default/files/6_bygrave.pdf>, accessed 9 November 2016.

23 European Convention on Human Rights and Fundamental Freedoms (1950) ("the ECHR"), art. 10; the EU Charter, art. 11.

24 The EHCR, art. 8; the EU Charter, art. 7.

25 Statement of Rights and Responsibilities (*Facebook*, 30 January 2015) <https://www.facebook.com/legal/terms>, accessed 9 November 2016.

26 Sara Grimes, "Persistent and Emerging Questions About the Use of End-User Licence Agreements in Children's Online Games and Virtual Worlds' (2013) 46 (3) UBC Law Review 681, 690. See also Sarah Grimes "Digital play structures: Examining the terms of use (and play) found in children's commercial virtual worlds" in Anne Burke & Jackie Marsh (eds) *Children's Virtual Play Worlds: Culture, Learning and Participation* (Peter Lang 2013).

[27] Joseph Bonneau & Sören Preibusch, "The Privacy Jungle: On the Market for Data Protection in Social Networks" (The Eighth Workshop on the Economics of Information Security, London, 24 June 2009) 1. Available online at <http://www.jbonneau.com/doc/BP09-WEIS-privacy_jungle.pdf>, accessed 9 November 2016.

[28] *ibid*.

[29] European Commission, "Special Eurobarometer 447: Online platforms" (June 2016) <http://ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf> 65, accessed 9 November 2016.

[30] Grimes (n 26). Grimes observed that children have a more limited capacity to understand the nature and implications of contractual agreements and commercial processes.

[31] Lina Jasmontaite & 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" (2015) 5 (1) International Data Privacy Law 2, 22.

[32] Kingdom of Spain, Royal Decree 1720/2007 of 21 December approving the Regulations implementing Law 15/1999 on the Protection of Personal Data, §13.1: "En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores."

[33] "Joint Select Committee on Cyber-Safety Inquiry: Cybersafety issues affecting children and young people" Statements of Mozelle Thompson (Australian House of Representatives, Parliament of Australia, 21 March 2011) <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Fcommjnt%2F13702%2F0001%22>, accessed 16 November 2016.

[34] *ibid*.

[35] Livingstone, Haddon, Görzig, & Ólafsson (n 8).

[36] ComRes, "BBC – Safer Internet Day survey" (2016) <http://www.comres.co.uk/wp-content/uploads/2016/02/BBC_Safer-Internet-Survey_Data-tables_Revised-28-Jan.pdf>, accessed 9 November 2016.

[37] Jose van Dijck & Thomas Poell, "Understanding Social Media Logic" (2013) 1(1) Media and Communication, 9.

[38] Kathryn Montgomery, "Youth and surveillance in the Facebook era: Policy interventions and social implications" (2015) 39 (9) Telecommunications Policy 771.

[39] Jennifer Golbeck, "The curly fry conundrum: Why social media "likes" say more than you might think" TED Talk (*TED*, October 2013) <https://www.ted.com/talks/jennifer_golbeck_the_curly_fry_conundrum_why_social_media_likes_say_more_than_you_might_think?language=en>, accessed 9 November 2016.

[40] Michal Kosinski, David Stillwell & Thore Graepel, "Private traits and attributes are predictable from digital records of human behaviour" (2013) 110 (15) Proceedings Nat'l Academy Sci Early Ed 5802. Available online at <http://www.pnas.org/content/110/15/5802.full.pdf?sid=ea5d4ee9-8f6e-4554-a013-dc5272b7e2e5>, accessed 9 November 2016. In 2013, these researchers developed a model that accurately predicts the sexual orientation of Facebook users in 88% of cases and can differentiate between caucasians and blacks 95% of the time using only a user's Facebook "Likes," which are used to express a "positive association" with a particular brand, artist, public figure, or social issue.

[41] Advertising Standards Agency, "Children and advertising on social media websites: ASA compliance survey" (July 2013) 5. Available online at <https://www.asa.org.uk/News-resources/Media-Centre/2013/~/media/Files/ASA/Reports/ASA%20Compliance%20Survey_Children%20and%20advertising%20on%20social%20media%20websites.ashx>, accessed 9 November 2016.

[42] Advertising Standards Agency, "ASA Ruling on Kellogg Marketing and Sales Company (UK) Ltd" (15 February 2012) <https://www.asa.org.uk/Rulings/Adjudications/2012/2/Kellogg-Marketing-and-Sales-Company-(UK)-Ltd/SHP_ADJ_176601.aspx#.V9Zm7Tu9iFJ>, accessed 9 November 2016. Facebook members were required to log

in to their Facebook profile to play the game and Facebook checked a member's date of birth in their profile information before allowing them to play. As Kellogg had taken steps to ensure that people under 17 could not access the game, it did not breach U.K. advertising rules.

43 University of Bath Institute for Policy Research, "Advergames: It's not child's play" (May 2014). Available online at <http://www.bath.ac.uk/ipr/pdf/policy-briefs/advergames.pdf>, accessed 9 November 2016.

44 Advertising Standards Agency, "Children and advertising on social media websites: ASA compliance survey" (n 40) 9–10.

45 European Commission, "Study on the impact of marketing through social media, online games and mobile applications on children's behaviour: Executive Summary" (March 2016) <http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/executive_summary_impact_marketing_children_final_version_approved_en.pdf>, accessed 9 November 2016.

46 Frances Leslie, Linda Levine, Sandra Loughlin & Cornelia Pechmann, "Adolescents: Adolescents' Psychological & Neurobiological Development: Implications for Digital Marketing" (Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children, Berkeley 29–30 June 2009) 6. Available online at <http://digitalads.org/documents/Leslie_et_al_NPLAN_BMSG_memo.pdf>, accessed 9 November 2016.

47 *ibid*.

48 European Commission, "Joint Statement on the final adoption of the new EU rules for personal data protection" (Brussels, 14 April 2016) <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm>, accessed 9 November 2016. See also European Commission, "Priority: Digital Single Market: Bringing down barriers to unlock online opportunities" <http://ec.europa.eu/priorities/digital-single-market/>, accessed 9 November 2016.

49 Meglena Kuneva, "European Consumer Commissioner Keynote Speech" (Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009) <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>, accessed 9 November 2016.

50 European Commission, "The EU Data Protection Reform and Big Data: Factsheet" (March 2016) <http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf> 1, accessed 9 November 2016.

51 Kit Smith, "Marketing: 47 Facebook Statistics for 2016" (*Brandwatch*, 12 May 2016) <https://www.brandwatch.com/2016/05/47-facebook-statistics-2016/>, accessed 9 November 2016.

52 "Social Network Ad Spending to Hit $23.68 Billion Worldwide in 2015: Advertisers in North America spend the most to be social" (*eMarketer*, 15 April 2015) <http://www.emarketer.com/Article/Social-Network-Ad-Spending-Hit-2368-Billion-Worldwide-2015/1012357#sthash.rWnSDQxY.dpuf>, accessed 9 November 2016.

53 Viviane Reding, "EU data protection reform and social media: Encouraging citizens' trust and creating new opportunities" (Economist conference "New frontiers for Social Media Marketing", Paris, 29 November 2011) <http://europa.eu/rapid/press-release_SPEECH-11-827_en.htm?locale=en>, accessed 9 November 2016.

54 See the GDPR, recital 18 and art. 2(2)(c).

55 European Commission, "Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union" (June 2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> 196 and 203, accessed 9 November 2016.

56 European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union" COM (2010) 609 (Brussels, 4 November 2010) 6. See also European Commission, "Eurobarometer: Safer Internet for Children: Qualitative Study in 29 European

Countries: Summary Report" (May 2007) <http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf>, accessed 9 November 2016.

57 Jos de Haan, Simone van der Hof, Wim Bekkers & Remco Pijpers, "Self-regulating online child safety in Europe" in Brian O'Neil, Elisabeth Staksrud & Sharon McLaughlin (eds), *Towards a better internet for children—policy pillars, players and paradoxes,* (Nordicom 2013); Milda Macenaite, "Protecting children's privacy online: a critical look to four European self-regulatory initiatives" (2016) 7 (2) European Journal of Law and Technology. Available online at <http://ejlt.org/article/view/473/661>, accessed 9 November 2016.

58 European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Strategy for a Better Internet for Children" COM (2012) 196 final (Brussels, 2 May 2012).

59 The UNCRC, art. 1.

60 Michael Freeman, *Article 3: The Best Interests of the Child* (Leiden 2007); Michael Freeman, "The Human Rights of Children" (2010) 63 (1) Current Legal Problems 1.

61 *In re S (A Minor) (Independent Representation)* [1993] Fam. 263.

62 *ibid.* 279–280.

63 For example, Case C-540/03, *European Parliament v Council of the European Union* [2006] ECR I-5769, para. 37; Case C-244/06 *Dynamic Medien Vertriebs GmbH v Avides Media AG* [2008] ECR I-00505, para. 39.

64 European Commission, "Communication from the Commission Towards an EU Strategy on the Rights of the Child" COM (2006) 367 final (Brussels, 4 July 2016); Decision No. 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies [2008] OJ L348/118; European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union" COM (2010) 609 final (Brussels, 4 November 2010); "An EU agenda for the rights of the child" <http://ec.europa.eu/justice/fundamental-rights/rights-child/eu-agenda/index_en.htm>, accessed 10 November 2016.

65 The Treaty on the European Union, art. 3.

66 See, for example, Joseph Savirimuthu, "Networked Children, Commercial Profiling and The EU Data Protection Reform Agenda: In the Child's Best Interests?" in Igni Iusmen & Helen Stalford (eds), *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions* (Barbara Budrich 2016).

67 UN Committee on the Rights of the Child, "General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights" CRC/C/GC/16 (17 April 2013) 3.

68 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" COM (2012) 11 final (Brussels, 25 January 2012).

69 American Chamber of E-Commerce to the European Union, "AmCham EU Proposed Amendments on the General Data Protection Regulation" 85. Available online at <https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/AmCham_EU_Proposed_Amendments_on_Data_Protection.pdf>, accessed 10 November 2016.

70 Facebook, "Comments from Facebook on the European Commission's proposal for a Regulation 'On the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'"

(25 April 2010) 10. Available online at <https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Facebook.pdf>, accessed 10 November 2016.

71 American Chamber of E-Commerce to the European Union (n 68), 85.

72 European Council, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] – Preparation for trilogue" leaked draft (*Statewatch*, 2015) <http://statewatch.org/news/2015/dec/eu-council-dp-reg-prep-trilogue-14902-15.pdf>, accessed 10 November 2016.

73 European Commission, "Commission Staff Working Paper: Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data" SEC (2012) 72 final (Brussels, 25 January 2012) 68.

74 Advertising Education Forum, "Children's data protection and parental consent: A best practice analysis to inform the EU data protection reform" (October 2013). Available online at <http://www.aeforum.org/gallery/5248813.pdf>, accessed 10 November 2016.

75 Nic Murfett, "Europe's data protection laws are changing, are you prepared?" (*GamesIndustry.biz*, 22 January 2015) <http://www.gamesindustry.biz/articles/2015-01-22-europes-data-protection-laws-are-changing-are-you-prepared>, accessed 10 November 2016.

76 For a history of COPPA's passage, see Kathryn Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (The MIT Press 2007) 67–106. See also Deborah John, "Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research" (1999) 26 (3) Journal of Consumer Research 183.

77 Janice Richardson, "European General Data Protection Regulation draft: the debate" (*Medium*, 10 December 2015) <https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.ncphvtori>, accessed 10 November 2016.

78 Larry Magid, "Europe Could Kick Majority of Teens Off Social Media, and That Would Be Tragic" (*The Huffington Post*, 10 December 2016) <http://www.huffingtonpost.com/larry-magid/europe-could-kick-majorit_b_8774742.html> accessed 10 November 2016.

79 Regulation (EU) No XXX/2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), consolidated text. Available online at <http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884>, accessed 10 November 2016.

80 John Carr, "Poor process, bad outcomes" (*Desiderata*, 29 March 2016) <https://johnc1912.wordpress.com/2016/03/29/poor-process-bad-outcomes/>, accessed 10 November 2016.

81 University of Bath Institute for Policy Research (n 42).

82 See Jasmontaite & De Hert (n 31); Savirimuthu (n 65).

83 eNACSO, "When Free Isn't: Business, Children and the Internet" (April 2016) <http://www.enacso.eu/wp-content/uploads/2015/12/free-isnt.pdf> 45, accessed 10 November 2016.

84 eNACSO, "Is the UNCRC fit to purpose in the Digital Era?" (November 2012) <http://www.enacso.eu/wp-content/uploads/2015/11/eNACSO_Report_UNCR_IGF_2012.pdf> 11, accessed 10 November 2016.

85 UNCRC, art. 3(1) and the EU Charter, art. 24.

86 UNCRC, art. 5.

87 Danah Boyd, "What If Social Media Becomes 16-Plus? New battles concerning age of consent emerge in Europe" (*Bright*, 18 December 2015) <https://medium.com/bright/what-if-social-media-becomes-16-plus-866557878f7#.6rmppea9s>, accessed 10 November 2016.

88 Ofcom (n 12) 134.

89 Anja Bechmann, "Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook" (2014) 11 (1) Journal of Media Business Studies 21; Lorrie Cranor & Aleecia McDonald, "The Cost of Reading Privacy Policies" (2008) 4 (3) I/S: A Journal Of Law And Policy For The Information Society 543.

90 For further discussion of "sharenting" see Stacey Steinberg, "Sharenting: Children's Privacy in the Age of Social Media" University of Florida Levin College of Law Legal Studies Research Paper Series Paper No 16-41. Available online at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711442>, accessed 10 November 2016.

91 "Woman sues parents for sharing embarrassing childhood photos" (*The Local*, 14 September 2016) <http://www.thelocal.at/20160914/woman-sues-parents-for-sharing-embarrassing-childhood-photos-on-facebook>, accessed 10 November 2016.

92 UN Committee on the Rights of the Child (n 66) 4.

93 For an overview of age verification mechanisms that seek to exclude under 18s (but do not seek to distinguish between different age groups of children), see Victoria Nash, Rachel O'Connell, Bendert Zevenbergen & Allison Mishkin, "Effective age verification techniques: Lessons to be learnt from the online gambling industry" (December 2013). Available online at <https://www.oii.ox.ac.uk/archive/downloads/publications/Effective-Age-Verification-Techniques.pdf>, accessed 10 November 2016.

94 The GDPR, recital 65 and art. 17.

95 *ibid.* recital 65.

96 Article 29 Working Party, "Opinion 2/2010 on online behavioural advertising" (2010).