2013

Who Cares?:Practical Ethics and the Problem of Underage Users on Social Networking Sites

Brian O'Neill
Technological University Dublin, brian.oneill@tudublin.ie

Recommended Citation

O'Neill, B. (2013). Who cares? Practical ethics and the problem of underage users on social networking sites. *Ethics and Information Technology*, vol. 15, no. 4, 253–262. doi:10.1007/s10676-013-9331-4

Who cares? Practical ethics and the problem of underage users on social networking sites

Abstract

Internet companies place a high priority on the safety of their services and on their corporate responsibility towards protection of all users, especially younger ones. However, such efforts are undermined by the large numbers of children who circumvent age restrictions and lie about their age to gain access to such platforms. This paper deals with the ethical issues that arise in this not-so-hypothetical situation. Who, for instance, bears responsibility for children's welfare in this context? Are parents/carers ethically culpable in failing to be sufficiently vigilant or even facilitating their children's social media use? Do industry providers do enough to enforce their own regulations and remove those users they know to be underage? How far does a duty of care extend? Regulation of age restrictions has, it is argued, created unintended consequences that heighten online dangers for young people. While children are inevitably drawn to new online spaces for entertainment and fun, should their rights to participate in the social world around them be curtailed to ensure their best interests and those of the wider community? Such questions now pose significant practical and ethical dilemmas for policy makers and other stakeholders involved in internet governance. It especially highlights the question of responsibility for protection of minors online and calls into question whether the current model of shared responsibility is working.

Keywords: social networking, internet safety, protection of minors, children and privacy, self-regulation

Introduction

Social networking is now one of the most popular applications on the internet, providing a virtual platform for millions of people across the globe to effortlessly share information and communicate with friends and family, irrespective of time or location. The phenomenal rise of services such as Facebook has been a crucial driver of growth in the internet industry, bringing new populations who may previously have been excluded into the online world. Online social interaction is ideally suited to many populations with special needs, enabling them to participate more fully in a virtual environment than they might in the offline world (Dobransky and Hargittai 2006). Older internet users, for instance, constitute one of the fastest growing demographics on social networking platforms, counteracting the impression that they are somehow less technologically adept (Eugène Loos et al. 2012; Buse 2009). This article is concerned with the other end of the age spectrum and deals with the youngest users of social networking sites, specifically those who are underage, as determined by the age restriction of 13 years placed on most social networking sites (SNS).[1]

Child online safety and the protection of minors in the digital environment has been an important area of policy concern since the development of the world wide web. Wide-ranging international protocols are in place to counteract the most egregious of online abuses affecting children (UNICEF 2011; ITU 2009). Extensive efforts are also made by internet companies, by legislators and by civil society to

[1] The age restriction of 13 years stems from data protection legislation in the United States, the Children's Online Privacy Protection Act of 1998 (COPPA), whereby websites that collect information from users under the age of 13 must obtain verifiable parental consent. As such, many internet services set 13 as the age bar above which parental consent is no longer required. See Montgomery, K. C. (2007). *Generation digital: politics, commerce, and childhood in the age of the internet*. Cambridge, Mass. ; London: MIT.

ensure high standards in online child safety policy. There are many services specifically dedicated to the needs of children, providing a protected, 'walled garden' in which the youngest children can explore and learn safely within an online environment (Reese et al. 2010). Technology solutions have also been developed to enable parents and carers to play an active role in monitoring or filtering younger children's internet access (FOSI 2011; Kirwil 2009). Yet, inevitably children's innate curiosity, combined with peer pressure and the appeal of exciting content on major SNS platforms has meant that large numbers of young people lie about their age to register on services that were not designed for them. How concerned we should be about this is a matter of debate. The purpose of this article is to examine some of the ethical issues that arise, including perspectives from industry, parents and from children themselves. While social networking services are largely international in nature, the scope of the current discussion is confined primarily to the European Union where the topic has received particular attention, as well as the United States where legal provisions for children's online privacy protection provides an important determining framework. The problem of 'underage' children using social media applications in contravention of the terms of service challenges the model of shared responsibility for protecting children's welfare online. Resolving the many anomalies that this creates remains a thorny problem for policy makers but the debate is one that has significant implications for wider issues of internet governance, ethics and the social uses of technology.

Defining the problem

Many social networking companies set the age of 13 as the minimum age for registering on their service. This particular age restriction derives from the Children's

Online Privacy Protection Act (COPPA) enacted in the United States in 1998 and effective since 2000. Under COPPA, commercial websites must acquire verifiable parental consent in order to collect and use information from children under the age of 13. For users under this age, companies must put in place a series of mechanisms and protections to comply with COPPA regulations. As a result, many internet companies operating in the United States have chosen to avoid such obligations altogether by restricting access via their terms of service to those over the age of 13. Not all services are age-restricted and most companies also provide additional privacy protection for users over 13 and under the age of 18. Those services that do restrict access to over-13s require users to enter a date of birth on registration but typically do not employ any other means of age verification. Therefore, simply entering a false age will enable anyone to register on the platform in question.

Research shows that such age restrictions on social networking sites have largely proved ineffective or are widely ignored. In the United States, for instance, where the most popular services are based (Facebook, Google+, MySpace etc.), more than half of teenagers aged 12 to 13 use online social networks, rising rapidly to over 80% of older teenagers (Lenhart et al. 2010). In Europe, social networking is similarly amongst the most popular of online activities for children aged between 9 and 16 years. According to EU Kids Online, three quarters of all young internet users in Europe between the ages of 13 and 16 and one third of 9-12 year olds has a profile on a social networking service (Sonia Livingstone et al. 2011).[2] Taking Facebook as an example – given its position as the most popular social networking service in Europe – one in 5 of all 9-12 year olds in Europe who use the internet have circumvented the

[2] EU Kids Online is a thematic network supported under the European Commission Safer Internet Programme and is aimed at enhancing knowledge of children's and parent's experiences and practices regarding risky and safer use of the internet and online technologies. In 2010, it conducted a face-to-face, in-home survey of 25,000 9-16 year old internet users and their parents in 25 countries using a stratified random sample and self-completion methods for sensitive questions.

age restriction to register a profile on the service. This rises to 34% of 9-12 year olds in the United Kingdom and Finland, 42% in Denmark, 46% in the Czech Republic and 48% in Slovenia. Ireland and the UK, as examples, are fairly typical of the European profile with about 1 in 5 or 20% of 9 year olds using SNS. However, this rises sharply after the age of 10 so that by the age of 12, approximately 60% of children have registered a Facebook account, using an incorrect date of birth (O'Neill and Dinh 2012).

There is evidence to suggest that many parents or carers are complicit in allowing underage children to gain access to social networking sites. Over three quarters of parents surveyed in the United States believed it was acceptable to allow their child to create an account on a social networking service in violation of the minimum age requirement (boyd et al. 2011). Most also believed that it is parents who should have the final say as to whether their child could access social networking services. In Europe, EU Kids Online found that half of all parents do not restrict their child's use of SNS. Among children whose parents impose no restrictions, most have an SNS profile, including three quarters of the youngest ages (Sonia Livingstone et al. 2011). Interestingly, among those whose parents restrict their SNS use, younger children appear to respect parental regulation and for the most part do not have a profile at all.

The risks that arise for underage SNS users stem from the fact that given they have entered an indeterminate age (and possibly name), they violate the 'real identity' policy of most social networking providers and will not be able to avail of the protections and default settings in place for their general age group.[3] Thus, EU Kids

[3] According to the Safer Social Networking Principles of the EU, service providers endeavor to make their platforms age appropriate for minors (typically between the ages of 13 and 18) by restricting the visibility of profiles, maintaining privacy by default, providing easy to use tools, terms of service and help resources as well as response mechanisms. See European Commission (2009)

Online found that over a quarter of 9-12 year olds had a profile set to public so that anyone could see their information (Livingstone et al. 2012). By contrast, a correctly entered age for an account under the age of 18 would typically have a default private setting and would not be visible in a public web search. EU Kids Online also found that of those with a public profile, a third of 11-12 year olds admitted they did not know how to change privacy settings. Moreover, children were more likely to post personal information such as identifying information including their address and phone number when their address was set to public rather than private or partially private (Sonia Livingstone et al. 2011).

Young people report that despite the many benefits, their online experiences are not trouble free. Over half of all children say that there are things online that bother children their age (S. Livingstone et al. 2011) and cite examples of unwanted contacts by strangers, scary things online and cyberbullying as among the persistent problems they encounter (Görzig 2011; Livingstone et al. 2013). Therefore, while understandably drawn to participate on platforms that have proved enormously popular among young people, children under the age of 13 – with or without their parents' knowledge – run significant risks of encountering potentially harmful content or contact online (Elisabeth Staksrud et al. 2012). The ethical implications for the various stakeholders involved are considered in the remainder of this paper.

Industry perspectives

The presence of substantial numbers of 'underage' children on websites and services designed for older audiences provides something of a dilemma and an embarrassment for many internet companies. Companies such as Facebook do not readily admit to the issue but reportedly delete approximately 20,000 children a day

for lying about their age.[4] Officially, where a web service becomes aware of an underage account in contravention of their terms of service, they take steps to have that account deleted.[5] In setting an age restriction at 13 and including this in their terms of service, such companies explicitly make a statement that they neither cater for or allow young children access their sites. Facebook's CEO, Mark Zuckerberg, famously remarked that kids under 13 should be allowed on the service, vowing to challenge the age restrictions on privacy rules imposed under COPPA (Lev–Ram 2011). Yet, despite suggestions in the *Wall Street Journal* in the run up to its public listing in 2012 that Facebook was preparing to launch an under 13s service, at the time of writing this had not materialized.[6] While it would be perfectly possible to adapt such a service or make provision for younger children, in order to be COPPA-compliant companies would have to abide by stricter privacy regulations and to tailor their safety information to a much younger audience, involving greater effort and expense, suggesting that most companies intend to maintain the status quo (E. Staksrud and Livingstone 2011).

The argument that companies need to do more in recognition of the large numbers of younger subscribers stems from the notion that they have a duty of care to all those who use their online services whether they are legitimately registered or not. Duty of care may be defined as a legal obligation on individuals or entities to ensure that they adhere to a standard of reasonable care while performing any acts that could foreseeably harm others (Henderson and Yarbrough 2002). The duty of care rule is well-established in many areas of law though its application to cyberspace is not

[4] This was divulged in the testimony of one Facebook's privacy advisors before an Australian parliamentary cyber-safety committee. See: http://www.dailytelegraph.com.au/news/banning-baby-faces-from-social-site-facebook/story-e6freuy9-1226025663992

[5] Facebook provides a form to report underage users: https://www.facebook.com/help/contact/?id=210036389087590

[6] http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html

always clear (Henderson and Yarbrough 2002). For a variety of reasons, internet service providers or ISPs enjoy as internet intermediaries an immunity from obligations arising from duty of care regarding content carried on their networks. Such immunity exists on the basis that ISPs act as a mere conduit and do not in theory have specific knowledge of any potentially harmful material carried on their networks. Such exemptions have been approved, for instance under the European E-Commerce Directive, on the basis that where harmful content is identified, providers undertake to comply with 'so-called notice and take down' court orders to remove offending content, (Schellekens 2011; Verbiest and Spindler 2007). When it comes to data protection, the European Union's Data Protection Directive applies strict rules that require companies to take all appropriate measures to protect data and information they possess against accidental or unlawful destruction or loss (Tikk 2011). Thus internet companies place a high priority in ensuring the security of their systems and are subject to audit by public regulatory authorities in how they store and protect data (Office of the Data Protection Commissioner 2011).[7]

Liability for other aspects of services offered by social networking companies and responsibility towards users of the platform are set out in the Terms of Service provided by companies. From a legal standpoint, service providers must clearly specify the limitations on their responsibility by outlining the terms and conditions governing access to their services. Thus, in the case of Facebook's Statement of Rights and Responsibilities, users are required to provide their real name and information (section 4), including age, and confirm that they are over the age of 13 (section 4.5).[8] Furthermore, the terms notify that while Facebook attempts to keep the

[7] See for instance the report of the Irish Data Protection Commissioner in its audit of Facebook Ireland Ltd. (Office of the Data Protection Commissioner 2011)
[8] See: http://www.facebook.com/legal/terms

platform safe, it cannot guarantee it (section 3), and that it is provided as a service for people to use as is and at their own risk (section 16.3).

If there is no strict legal obligation on companies such as Facebook to assume responsibility for underage users, there is surely an ethical obligation stemming at the very least from the requirement in common law to exercise a due standard of care in ensuring the safety of the service given the likelihood that it will be accessed by many kinds of users with varying levels of skill or ability (Vedder 2001).

A framework for the safety provisions provided in social networking environments is contained in the Safer Social Networking Principles, a code of practice developed jointly by the European Commission and 21 of the most prominent social networking companies (European Commission 2009). Under these principles, companies undertake to make their services age-appropriate and safe for the intended audience. Thus, according to the principles, acceptable use policies should be made available to all users in a clear, easily understood manner; easy to use mechanisms and tools to report harmful or abusive content should be in place; and companies should enable and encourage users to employ a safe approach to personal information and privacy. In the case of Facebook, the company cites special precautions to ensure that users between the ages of 13 and 17 have more restrictive privacy settings (Donoso 2011). For instance, accounts of minors are never listed in public searches, sharing of information for under-18s is limited to friends and networks, and where geo-location services are used, a minor's account can only disclose their location to confirmed friends.[9] Such privacy-enhancing provisions are part of wider efforts to ensure better safety and control of social networking services for under-18s. Crucially however, if an under 13s user enters an incorrect age, i.e. over the age of 18, they are

[9] See Facebook Self-Declaration for EU Safer Social Networking Principles, http://ec.europa.eu/information_society/activities/social_networking/docs/new_self_decl_2010/facebook.pdf

likely to be exposed to far greater risk (and have adult settings applied) than if the age entered is under 18.

An effective system of age verification would, of course, be a solution to the problem of registrations based on a false age. Currently, social networking sites may be said to operate a system of self-certification whereby the only verification provided is the word of the individual user. An age verification solution is one that requires additional, verifiable confirmation of the identity and the age of the individual attempting to register or access the proposed (age-restricted) service. Age verification is required by law in some countries, for instance in the United Kingdom, for access to certain services such as online gambling (limited to over 18s), or to e-commerce services selling alcohol, cigarettes and medication (France). In Germany, a more elaborate system of verifying identity and age is in place to control access to all online adult services. A report prepared by the European Commission for the Safer Internet Forum in 2008 concluded that while a variety of systems have been deployed for specific services, including electronic identity cards, use of credit/debit cards, and semantic analysis technologies, there was no existing approach that was fully effective or was capable of being applied on a pan-European basis (European Commission 2008). Each has limitations or can be easily circumvented. Age verification techniques that seek to draw on social security numbers for instance may also be subject to legal restrictions. Additionally, using technical means of age verification may create additional risks or have unintended consequences through 'the illusion of a safe zone which is not actually safe from determined and highly motivated predators' (European Commission 2008). For all of these reasons, safety advocates have tended to argue that technical methods of verification on their own are

never enough. Parental responsibility and education for user responsibility must, it is argued, be the primary focus of awareness raising efforts.

Parental responsibility

Parents have long been deemed the most important guardians of children's welfare online (Kaiser Foundation 2004; Livingstone and Bober 2006). Since its inception, the European Union's Safer Internet Programme has focused efforts on encouraging the development of classification systems equivalent to those that operate in the traditional media world as guidance for parents and carers in supervising their children's online use (Keller and Verhulst 2000). In addition, extensive awareness-raising efforts have been developed to educate parents, teachers and other adults with responsibility for youth about online risks through the provision of safety tips and advice about how to best monitor young people's use of internet technologies. Parental controls or filtering technologies that allow parents and guardians to monitor what young people do online and to restrict access to unapproved sites have been a central part of this policy (FOSI 2011). Such tools are designed to empower parents to set limits on the amount of time that children spend online, decide on which content or which services are appropriate for children and to facilitate a dialogue between parents and children about online use.

More widely, a marked shift has taken place in policies protecting young people in the audiovisual arena whereby the kind of close regulation of content found on media systems such as broadcasting and theatrical cinema distribution applies in a much weaker form in the online environment. Thus, while the European Union's Audiovisual Media Services Directive (European Commission 2007), Europe's pre-eminent media policy instrument for the audiovisual sector, recognizes that online,

on-demand services greatly increase choices to the consumer, it warns that consumers must also ultimately take responsibility for the content they access (Helberger 2008). Measures to protect against children's access to the most harmful content are mandated through the use of access codes and other means. However, content that on traditional television could be defined as simply 'harmful' and would normally be scheduled after the 'watershed', has no restriction in an online or on-demand environment. It is in this context, that emphasis is placed on parents assuming responsibility and being vigilant in supervising young people's media consumption and communication habits (Helberger 2007; McGonagle 2003).

It may well be the case that when it comes to social media, many parents in fact decide to allow their children to access social networking services. Parents may feel, for example, that while their children are underage, they are confident they are able to manage the risks. This is the case established by boyd et al's research (2011) in the United States where one fifth of parents of 10 year olds, a third of parents of 11 year olds and over half (55 per cent) of parents of 12 year olds acknowledged that their children had Facebook accounts. Many parents also admitted that they helped their children set up the account. Among those who knew that their child was below the age of 13 when they joined, over two thirds reported that they had assisted in creating the account. Moreover, most (90 per cent) were aware of the age restrictions, though a third believed this was a recommendation rather than a requirement. Among reasons given as to why they would allow their child use a platform in violation of the terms of service, most parents cited educational and school-related purposes, and to communicate with family and friends. Half also said they would allow use of the service only under supervision.

Research from EU Kids Online shows that there are considerable cultural variations in parental attitudes to children's social networking use (Lobe 2011; Sonia Livingstone et al. 2011). Across Europe, one third of parents do not allow their child to have an SNS profile. A fifth say their child can only use SNS with supervision and half say they do not restrict their child's use of SNS. This varies considerably from country to country, however. In France, nearly half of all children (45%) are not allowed to use SNS (and accordingly, there are relatively few underage children on social networking platforms). Similar numbers of parents place restrictions on younger children's internet use in countries such as Greece, Italy and Spain while children in Northern European countries such as Lithuania, Estonia, the Netherlands and Denmark experience the fewest restrictions (and higher numbers of underage users).

From a practical standpoint, two interpretations of findings such as these are possible. On the one hand, it might be argued that whether through pressure from younger children or by deciding that regulations imposed by social networking providers are inadequate, many parents take the decision to allow younger children to use services designed for over 13s. Internet safety policy advice has long promoted the importance of active dialogue between parents and children about their internet use and one might therefore view such practice as a positive example of parents and children successfully negotiating the nature and limits of their online activity (Tufte and Tufte 1999; Livingstone and Helsper 2008). On the other hand, an alternative interpretation of parents' actions in this area might suggest that the burden of responsibility that falls on them is too great. Many parents may feel so overwhelmed, possibly through their own lack of digital skills, that they fail to take adequate control of their children's digital lives. Whether the former approach constitutes responsible

parenting, given the nature of the risks involved, is another matter. The latter interpretation raises issues about the unfair burden of responsibility, particularly in light of the lack of support that many parents feel in the digital arena and similarly highlights a debate about the shared nature of responsibility in children's online safety. Yet children also are actors in this and must assume some element of responsibility for their actions in the digital space.

Role of young people

As the direct users of social networking services, young people by accessing and using social networking services take responsibility for their actions and behaviour in the online world and for their personal safety. Among the many risks that young people face online indeed are those created by young people themselves, whether in the form of cyberbullying between peers, misuse of personal data or hacking into friends' accounts, or harmful or offensive content created by other users (S. Livingstone et al. 2011; Elisabeth Staksrud et al. 2012). While policy makers understandably continue to emphasise the importance of empowering young people to take responsibility for their own actions, to develop better and safer practices and models of digital citizenship, the reality is that in many cases, young people lack the basic skills and only become aware of safety issues when something goes wrong. In the EU Kids Online survey, 45% of younger Facebook users, aged 11 to 12, said they did not know how to manage their privacy settings. A further 39% said they did not know how to block another user. Skills do increase with age and by the age of 15 or 16, the vast majority of young people have mastered the privacy and safety mechanisms associated with social networking sites (Sonia Livingstone et al. 2011). Age, in this sense, is used as a proxy for intellectual and emotional maturity though a

difficulty in determining an appropriate age for the necessary cognitive and practical skills required to manage one's own safety is that children vary in their pace of development (Berger 2012). Hence, setting age 12 or 13 as a cut-off above which young people are assumed to be capable of managing their own safety ignores the fact that some will be sufficiently mature at an earlier age, yet others will still lack sufficient maturity until a later age.

Notwithstanding the complex issues of child and adolescent development, all minors under the age of 18 are entitled to protection of their personal safety and of their data, a fact recognised by internet companies in setting certain default measures such as restricting access to personal profiles or preventing visibility of personal data beyond approved contacts (European Commission 2009). The question arises, therefore, whether such rights are forfeited once children find and exploit breaches in the measures taken by companies to restrict access to their services. If due care and diligence has been exercised by the owner, surely users avail of services, particularly in unauthorised forms, at their own risk? The counter argument from a child protection standpoint is that where the protective measures designed to restrict access are so weak as to allow easy access to anyone, arguably it is the owner rather than the user who has failed in their responsibility.

The practical ethics of social networking

The sharing of responsibility for protecting young people online is a necessary response to the effective management of risks in the virtual environment and the related, complex issues that arise in internet governance and regulation. However, in the case of underage users of social networking services, it leads to a highly contested area that renders online safety less effective and creates new, unintended and

potentially more dangerous risks for children who breach safety regulations. Considering the practical ethics of the conflicts that arise in this context is likely to prove more effective than merely focusing on the legal aspects of negligence involved. Social networking is very much a 'social technology' (Nelson and Nelson 2002), combining both technical innovations as well as widely diverse communicative and behavioural dimensions on the part of social actors. Following Thomson (2007), a debate on the practical ethics involved – as opposed to contesting companies' legal responsibilities – has three broad advantages. Firstly, it provides a bridge between theory and practice, enabling a principled approach to be taken in an area not well catered for in existing policy or regulatory practice. Secondly, it is particularly helpful in assessing the institutional context in which social networking interactions are located. Where ethics in the main has been concerned with either individual or societal levels of behaviour, the institutional middle ground has received less attention and a practical ethics is better suited to framing the issues and potential conflicts at this middle range level. Thirdly, practical ethics is also helpful in highlighting the political nature of decision making involved, focusing attention on authority and the deliberative process by which decisions are made, particularly in the context of professional practices that are self-regulated, as is the case in most instance of internet governance.

With this in mind, how does one assess the practical ethical issues contained in the contested topic of underage use of social networking services? Following the logic of shared responsibility for child safety online which includes all relevant stakeholders, it might on the face of it be argued that industry, parents, educators and children themselves all share some element of responsibility for such anomalous and risky online practices. Equally, responsibility for resolving the problems can be seen

as shared by all. Such an approach is plausible and in keeping with the efforts of educators and internet safety experts who seek to instil in young people the skills and awareness of their own abilities in protecting themselves.

However, to grant all stakeholders equal status is surely unreasonable when it is clear, particularly in the case of the youngest users, there are gross disparities in power and capability when it comes to making effective choices in safety. As 'special needs' users, children under the age of 13 in general lack the maturity (as recognised in privacy legislation) and the ability to grant consent for their data to be used and therefore cannot be held to the same level of accountability as those in positions of authority whether they be parents, guardians or providers of internet services.

Considering, therefore, the differing levels of power wielded by the various stakeholders concerned, the oft-repeated analogy between online safety and safety in the built environment may be of some assistance. In this way, online safety is often compared to the need for safety on roads, particularly in areas where children are playing; similarly, children's play spaces be they physical or virtual, in playgrounds or in online environments, require similar considerations for safe practices as well as good design. Parental responsibility is necessarily all the greater in accordance with the children's age and level of development. Thus, just as parents ensure that children don't cycle on the open road before they are ready, or without wearing a bicycle helmet, or don't cross roads where it is unsafe to do so, similarly they are advised to take equivalent precautions regarding their children's activities in the online space.[10] Parents, therefore, in the circumstances considered here assume a greater share of responsibility than their children in facilitating social network access, or by failing to take account of dangers their children may encounter.

[10] Or for example, the analogy drawn in the Byron report, commissioned by the UK Prime Minister Gordon Browne into provision for online safety, where pointedly it was argued we do not let children dive into a swimming pool before learning how to swim. See: (Byron 2008)

However, the analogy is not just focused on end users – parents or children – it also applies to the engineers, providers and other agencies responsible for creating and servicing the built environment. Where evident deficiencies exist in the design, safety features, or measures designed to restrict access to an area deemed unsuitable for certain age groups, it is to the designers we should look to examine more closely how seriously they have taken their commitment to enforce their own regulations. As we have seen, social networking companies who apply age restrictions declare openly that they neither allow nor cater for underage users. Moreover, many declare that they take further measures to identify and delete underage users from their services and prevent them from attempting to re-register, by employing cookies for example. Yet, despite substantial evidence revealing that such efforts are ineffective or easily flouted, many of the major companies involved have resisted adopting any further measures to verify younger users' age or identity, casting doubt over the priority they accord to the issue of underage use.

Applying an ethics of 'safety by design' would yield a different result. Were companies to adopt the principle that its services would, from the outset, be designed around fitness for purpose for the intended age group, measures to confirm users' credentials would be a primary requirement. Similarly, default settings to ensure maximum levels of safety, security and privacy would be enforced, including graduated measures tailored to the ages (and needs) of different categories of audiences.

Policy responses

A consideration of the practical ethics of underage user on social networking services as discussed above points inevitably to the political process in which policy is shaped, in which deficiencies in current arrangements are addressed and prospects for future, better provision is debated. It is in this context that the European Union's Vice President for the Digital Agenda, Neelie Kroes, convened a coalition of the CEOs of leading internet companies operating in Europe to take action on specific measures designed to enhance online child safety and to agree industry-wide measures to tackle a range of persistent problems that had the effect of undermining public confidence.[11] The CEO Coalition identified five central issues with which it would engage to proffer new solutions in support of better safety for children. Age verification, or mechanisms to manage underage use, was not one of these.[12] Instead, a consideration of age featured in its work through a commitment to provide better classification and labelling of age-appropriate content and through a commitment to make privacy settings as safe as possible for the ages concerned. While sometimes short on specifics, the implication of such commitments is that better controls could be developed and implemented and that this is something that industry alone can provide.

One of the reasons presumably that age restrictions on access to services was not specifically dealt with is that it places an expensive burden on industry to introduce access controls in conflict with their open access business model. Unlike the case of online gambling, for instance, where specific legal restrictions apply, the

[11] The CEO Coalition to make the internet a better place for kids was convened in December 2011 and committed over the course of one year to take positive action to ensure internet experience was beneficial for children. See:
http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm

[12] The five areas were: i) Simple and robust reporting tools for users; ii) Age-appropriate privacy settings; iii) Wider use of content classification; iv) Wider availability and use of parental control; and v) Effective takedown of child abuse material.

question of underage SNS access is one of policy, not law. There may be broad consensus between companies and stakeholders of the desirability of better age verification mechanisms though its priority lies below that of other online child protection measures. As an alternative, policy makers and industry have preferred to focus on improving the effectiveness and the take of parental control technologies. Parental control tools allow parents and guardians to set restrictions at the point of access whether on the device itself (e.g. smartphone, laptop, personal computer) or at the service level (for instance, on a network router controlling access to defined web sites or services, or on browser software). Thus parents are enjoined through better recognition of the age-appropriateness of online content and services to apply the necessary technical solutions to implement age controls. The application of parental control tools goes beyond the use of social media and their use remains sometimes controversial (O'Neill et al. 2013), yet parents have never had such an array of technology available to them to monitor and shape their children's media and internet exposure (Thierer 2009).

What policy makers have sought to do, however, is confirm the underlying age limits for consent to participate in online social media services. The most recent revision of children's online privacy protection legislation in the United States (COPPA) confirms the applicability of verifiable parental consent for children under 13 for all commercial websites, online services, mobile apps and plug-ins. New means of supplying parental consent include electronic scans, parental payment systems, video or phone conference, or through the use of government-issued IDs. A similar recognition of 13 as the age below which parental consent is required to collect data from children is included in European proposals for a revised privacy regulation, thus bringing these regimes formally into line (European Commission

2012). However, service providers are not obliged to obtain any additional verification of age once users register, truthfully or otherwise, to access their service. COPPA's primary objective is to place parents in control of information collected for commercial purposes under the age of 13. It is not specifically about safety, nor does a COPPA-compliant website represent an endorsement of its suitability for children. Similarly, where parents choose to support underage children accessing over-13 sites, it is not inherently dangerous but does violate the original objective of COPPA (Magid 2013).

It would appear, therefore, that promotion of parental control tools by initiatives such as the CEO Coalition with the wider legislative recognition of protecting younger children (under 13) in the online world underlines further the role of the parent rather than the industry in online safety. This perpetuates an individualist emphasis in devolving responsibility to parents and children alike for a wide range of decisions about media access (O'Neill 2010). Despite the greater collective emphases exhibited in pan-industry cooperation in improving safety provisions, the balance of responsibility for younger children's safety and security has not substantially altered. This despite the fact that protection of minors in the online world has been recognised as one of the core values of the European audiovisual system to which policy makers, governments and industry alike have been asked to devote increased attention (European Commission 2013). It would appear that industry efforts to make internet services safer for children include development of more effective control mechanisms but under the broad heading of user empowerment, their implementation is fundamentally one which is left to young people and their parents for final arbitration.

Conclusion

The phenomenon of young people's use of social networking services is one that has arisen in relatively recent times and has brought to the fore many issues regarding responsibility for online safety especially when access to such services is unauthorised. This article has considered the particular case of underage use of social media services in cases where providers have chosen to ban access to those under the age of 13 rather than adopt the legislative requirement for verifiable parental consent for younger children. The questions that arise in this context concern who bears responsibility for children's safety and welfare. Industry declares in such circumstances that it neither supports younger users nor has knowledge of underage use of such services. Where it does detect unauthorised access, it moves swiftly to remove the users concerned. However, research shows that the intrinsic appeal of social media services proves irresistible to many young people and that as many as 60% of 11 and 12 year olds in some countries routinely use services intended for an older audience. The harm that may arise from such use is a matter for further research but the issue remains that such users contravene terms of service for the sites involved and fail to gain the protection afforded to legitimate users. In many instances, parents have been shown to be complicit in allowing such a scenario to develop either through concern that their children are not left out of digital opportunities or through a lack of awareness of the risks involved. Young people themselves also bear responsibility for their own actions in seeking to gain access in the first place through supplying false information on first registration.

The main consideration in this article has been on the practical ethics, or decision-making relating to appropriate conduct, in a situation where online safety and welfare of children has long been recognised as a shared responsibility. The respective roles of industry, of parents and of young people themselves were assessed

in turn and to whom obligations in each case are seen to apply. In the practical realm of implementation of policies designed to enhance online young people's safety, industry efforts to develop new initiatives to promote safer use were identified. In this context, industry leadership arises as a result of its role as originator of services for whom a duty of care applies. However, it is to parents and caregivers more often than not that decision making and implementation of policies falls. Wide legal protections are afforded to younger children against commercial data collection methods, yet enforcement is noticeably weak and prompts, as the title of this paper provocatively suggests, a question as to whether this is a topic to be taken seriously. The continuing policy priority accorded to protection of minors in the audiovisual world would imply that it is, however undermined by the anomalies of youthful participation in social media. Arguably, more sustained attention to the public policy dimensions of this debate would imply greater attention to the infrastructural and design aspects of internet service provision just as they do in all aspects of the built environment. Such an emphasis would necessarily require greater clarity about safety standards, underpinned by an ethics of public space, and reduce the opportunity or need for enforced risk-taking by younger children.

References

Berger, M. (2012). A safe place to surf. *Science*,

boyd, d., Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act. *First Monday, 16*(11),

Buse, C. E. (2009). When you retire, does everything become leisure? Information and communication technology use and the work/leisure boundary in retirement. *New Media & Society, 11*(7), 1143-1161, doi:10.1177/1461444809342052.

Byron, T. (2008). Safer Children in a Digital World: The report of the Byron Review. London: DCSF.

Dobransky, K., & Hargittai, E. (2006). The disability divide in internet access and use. *Information, Communication & Society, 9*(3), 313-334, doi:10.1080/13691180600751298.

Donoso, V. (2011). Assessment of the Implementation of the Safer Social Networking Principles for the EU on 14 Websites: Summary Report. Luxembourg: European Commission, Safer Internet Programme.

Eugène Loos, Haddon, L., & Mante-Meijer, E. (Eds.). (2012). *Generational Use of New Media*. London: Ashgate.

European Commission (2007). Audiovisual Media Services Directive (AVMS) Directive 2007/65/EC. Brussels: European Commission

European Commission (2008). Background Report On Cross Media Rating And Classification, And Age Verification Solutions. Luxembourg: European Commission Safer Internet Programme.

European Commission (2009). Safer Social Networking Principles for the EU. Luxembourg: European Commission Safer Internet Programme.

European Commission (2012). Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century.

European Commission (2013). Green Paper COM(2013) 231 final. Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values. Brussels: European Commission.

FOSI (2011). Who Needs Parental Controls? A Survey Of Awareness, Attitudes, And Use Of Online Parental Controls. Washington, DC: Family Online Safety Institute.

Görzig, A. (2011). Who bullies and who is bullied online? LSE, London: EU Kids Online.

Helberger, N. (2007). The Changing Role of the User in the "Television Without Frontiers Directive", IRIS Special In *Legal Aspects of Video on Demand*. Strasbourg: European Audiovisual Observatory.

Helberger, N. (2008). The Media-Literate Viewer. In N. v. Eijk, & P. B. Hugenholtz (Eds.), *Dommering-bundel: Opstellen over informatierecht aangeboden aan prof. mr. E.J. Dommering* (pp. 135-148). Amsterdam: Otto Cramwinckel Uitgever.

Henderson, S. E., & Yarbrough, M. E. (2002). Suing the Insecure?: A Duty of Care in Cyberspace. *New Mexico Law Review, 31*, 11-25.

ITU (2009). Child Online Protection. Geneva: International Telecommunication Union.

Kaiser Foundation (2004). Parents, Media and Public Policy. Washington, DC: Kaiser Family Foundation.

Keller, D., & Verhulst, S. G. (2000). Parental Control in a Converged Communications Environment Self-Regulation, Technical Devices and Meta-Information.

Kirwil, L. (2009). Parental mediation of children's internet use in different European countries. *Journal of Children and Media, 3*(4), 394-409.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social media and mobile internet use among teens and young adults. Boston, MA: Pew Internet and American Life Project.

Lev–Ram, M. (2011). Zuckerberg: Kids under 13 should be allowed on Facebook. *Fortune,* (May 20),

Livingstone, S., & Bober, M. (2006). Regulating the internet at home: contrasting the perspectives of children and parents. In David Buckingham, & R. Willett (Eds.), *Digital generations: children, young people, and new media* (pp. 93-114). London: Routledge.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.

Livingstone, S., & Helsper, E. J. (2008). Parental Mediation of Children's Internet Use. [Article]. *Journal of Broadcasting & Electronic Media, 52*(4), 581-599, doi:10.1080/08838150802437396.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2013). In their own words: What bothers children online? : LSE, London: EU Kids Online.

Livingstone, S., Ólafsson, K., O'Neill, B., & Donoso, V. (2012). Towards a better internet for children. London, LSE: EU Kids Online.

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). Social Networking, Age and Privacy. London, LSE: EU Kids Online.

Lobe, B., Livingstone, S., Ólafsson, K. and Vodeb, H. (2011). Cross-national comparison of risks and safety on the internet: Initial analysis from the EU Kids Online survey of European children. London: EU Kids Online, LSE.

Magid, L. (2013). FTC Clarifies Children's Online Privacy Law (COPPA). http://www.forbes.com/sites/larrymagid/2013/04/25/ftc-clarifies-childrens-online-privacy-law-coppa/.

McGonagle, T. (2003). Practical and Regulatory Issues Facing the Media Online. In C. Hardy, & C. Möller (Eds.), *Spreading the Word on the Internet: 16 Answers to 4 Questions* (pp. 81-94). Vienna: OSCE.

Nelson, R. R., & Nelson, K. (2002). Technology, institutions, and innovation systems. *Research Policy, 31*(2), 265-272.

O'Neill, B. (2010). Media Literacy and Communication Rights Ethical Individualism in the New Media Environment. *International Communication Gazette, 72*(4-5), 323-338.

O'Neill, B., & Dinh, T. (2012). Social Networking Among Irish 9-16 year olds. *Digital Childhoods Working Paper No. 3*. Dublin: Dublin Institute of Technology

O'Neill, B., Staksrud, E., & McLaughlin, S. (Eds.). (2013). *Towards a better internet for children? Policy Pillars, Players and Paradoxes*. Goteborg: Nordicom/UNESCO Clearinghouse for Children and Media.

Office of the Data Protection Commissioner (2011). Facebook Ireland Ltd Report of Audit.

Reese, L. d., Petito, L., & Pijpers, R. (2010). Producing and providing online content for children and young people: An inventory. Luxembourg: European Commission, Safer Internet Programme.

Schellekens, M. (2011). Liability Of Internet Intermediaries: A Slippery Slope? *SCRIPTed, 8*(2), 154-174.

Staksrud, E., & Livingstone, S. (2011). A-B-Cyberspace. Can children ever be safe on social networking sites?'. *Public Service Review, European Union, 22*,

Staksrud, E., Ólafsson, K., & Livingstone, S. (2012). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior*(0), doi:10.1016/j.chb.2012.05.026.

Thierer, A. (2009). *Parental controls & online child protection: A survey of tools and methods*. Washington, DC: The Progress & Freedom Foundation.

Thompson, D. F. (2007). What is practical ethics? *Ethics at Harvard, 1987-2007*,

Tikk, E. (2011). Ten Rules for Cyber Security. *Survival, 53*(3), 119-132, doi:10.1080/00396338.2011.571016.

Tufte, B., & Tufte, T. (1999). Parental Control of Broadcasting, Film, Audiovisual and On-line Services in Denmark. *NORDICOM Review, 1*.

UNICEF (2011). Child Safety Online - Global challenges and strategies. Florence: UNICEF Innocenti Research Centre.

Vedder, A. (2001). Accountability of Internet access and service providers ‚Äì strict liability entering ethics? *Ethics and Information Technology, 3*(1), 67-74, doi:10.1023/a:1011492109277.

Verbiest, T., & Spindler, G. (2007). Study on the Liability of Internet Intermediaries. Brussels: European Commission.