PHRG
PEACE HUMAN
RIGHTS GOVERNANCE

Volume 4, Issue 1, March 2020

'Sharenting': The Forgotten Children of the GDPR

Sheila Donovan

Research Articles*

DOI:

10.14658/pupj-phrg-2020-1-2

How to cite:

Donovan, S. (2020) '"Sharenting": The Forgotten Children of the GDPR', *Peace Human Rights Governance*, 4(1), 35-59.

Article first published online

March 2020

*All research articles published in PHRG undergo a rigorous double-blind review process by at least two independent, anonymous expert reviewers

PADOVA UP

PHRG 4(1), March 2020

‘Sharenting’: The Forgotten Children of the GDPR

Sheila Donovan *

Abstract
The exponential growth of the internet and social media use in the recent past followed by a widespread increase of the scale, scope and sharing of information has impacted greatly on the concept of privacy. This growth has been accompanied by innumerable duplication and storage in perpetuity of personal data. While debates surrounding the protection and safety of social network users, in particular minor users have emerged as a matter of concern, there has been minimal focus on the privacy of minors, in particular, those minors who are the subject of ‘sharenting’ which is defined as ‘the online posting of images and data of children’. The introduction of the General Data Protection Regulation 2016 was designed to give more robust protection and rights to all individuals, in particular children, who were recognised as being particularly vulnerable. The GDPR, however, in seeking to address the security and safety of the private identity of minors who engage in social networking, places the oversight of minors’ digital privacy into parental hands, regardless of their digital competency. This hastened attempt to guarantee minors’ online safety failed to address the privacy of all minors, in particular those minors who are the most vulnerable members of our society and who have an increased online presence and exposure to danger as a result of their parents’ online networking.

Keywords: *Autonomy, Digital Privacy, Parental Control, Self-determination*

* School of Law, College of Business, Public Policy & Law at the National University of Ireland, Galway; e-mail: S.Donovan7@nuigalway.ie

Introduction

In 2015, the European Parliament, the Council and the Commission agreed on a harmonised data protection regulation with the general expectation that it was going to benefit all citizens. The General Data Protection Regulation (GDPR) which came into effect on the 25th May 2018 harmonises European privacy measures with the imposition of monetary sanctions for infringements (Article 83 GDPR). Its advent was welcomed as a 'holistic effort to regulate data, which, in consideration of its value, is regarded as the "new oil" of this era' (Livingstone 2018, 18). Data portability, privacy icons and data protection by 'design and default' were among the measures introduced to engender opportunities of innovation and competition in data protection and consumer friendly products and services (Albrecht 2016, 288).

The GDPR was heralded to be paving the way for universal data privacy. It aimed to 'entrench privacy with trust as its cornerstone' (Buttarelli 2016, 77). With its introduction, the emphasis, from the perspective of minors has focused solely on the oversight and safeguarding of teenagers' online activity, with little attention being paid to the privacy and identity safety of young children whose private identity is being openly eroded by parental online postings. This issue is further complicated by Recital 18 of the GDPR which exempts household and personal online activities from the constraints and protections imposed by the GDPR.

Chief among those personal online activities escaping the GDPR constraints is that of 'sharenting' which is widespread and growing. The explosion of the 'social networking tsunami' has magnified the exposure of private life over a relatively short interval (Kuczeraway and Coudert 2010, 232). Research indicates that 'sharenting' benefits parents at an immense cost to the privacy and private identity of the child. A significant lacuna in the Regulation is the lack of protection for the private identity of the child whose images are shared on social networks sites.

This paper addresses this previously unaddressed and ignored issue and represents one element of a wider research project which is currently being undertaken by the author: an analysis into the extent to which parental freedom of expression impinges on the child's right to autonomy and a private identity. This project is based on doctrinal research and an examination of the legislative framework in support of the child's right to a private identity and includes an empirical research into the level of parental awareness as to the right of the child to privacy and the ramifications of 'sharenting' for the child's private identity. It is envisaged that this research, once completed, will broaden the discussion on child online safety and privacy.

Much of the discussion on this topic has up to now centred solely around the online dangers posed to teenage social media users. Little if any recognition, however, was given to the threats posed to younger children by the online sharing practices of their parents. It is anticipated that the establishment of evidence highlighting the potential threats to minors' identity and privacy will pave the way for the introduction of regulatory/legislative framework protection designed to encourage parents to engage in responsible and safe online posting of data related to their minor children. While parents may recognise the dangers associated with 'sharenting', the computer creates a 'false sense of intimacy' (Kuczeraway and Coudert 2010, 232). There is, therefore, a need to create a safe haven for children who are the subjects of 'sharenting'.

This paper, examining the rationale underlying the introduction of the GDPR, considers in particular Recital 18 of the GDPR and its potential impact for the privacy and protection of young children who are the subjects of 'sharenting'. In recognition of the broad remit of Recital 18, the prevalence, reasons and potential ramifications of 'sharenting' are all examined. This examination will focus on the effect of 'sharenting' on children's rights to a private identity, freedom of expression and protection, rights which are upheld by the UNCRC and which may be compromised as a result of 'sharenting'. The contention that 'sharenting' poses a particular danger may be substantiated by an evaluation of the manner in which social media providers disregard the GDPR's measures for safety and privacy in the online arena. The conclusion will pinpoint a way forward which will best embrace the protection of minors' privacy and which will be in full compliance with international best practice.

1. Rationale of the GDPR

The main purpose of the GDPR 2016 was to introduce long-overdue privacy and data security standards, upon which consumers, including all children, could rely. Given that social networking and other online companies which collect large amounts of personal data now have to appoint a data protection officer (Article 37(1)), the freedom to transfer personal data to third parties for other purposes without the user's consent is curtailed and is subject to particular restrictions (Art.8(1)).

Up to now, the data practices which targeted children were the same as the ones used for adults and were inappropriate in that they did not respect teenagers' digital literacy. While teenagers may deserve greater opt-in, transparency and individual control, are special provisions for children

warranted? Some like Sorensen argue yes (Sorensen, 2016), whereas others like Livingstone contend that we all require protection and can be vulnerable given the situation (Livingstone, 2018). This raises questions as to whether the GDPR's reliance on responsible parents is counterproductive and whether or not the GDPR has, in fact, contributed to the vulnerabilities of minors.

Does the parental role of 'gatekeeper' impact on the child's right to autonomy, privacy and self-digitalisation? Where does 'sharenting' fit within this and how ought it be addressed if the digital privacy of all minors is to be safeguarded?

The GDPR's reliance on responsible parents may be counterproductive as it may result in children lying about their age, not requesting parental permission and pushing their online use further under the parental radar, thereby making it difficult for well-meaning parents to guide them. Furthermore, the reliance on parents as 'gatekeepers' of their children's digital safety and privacy neglects to acknowledge that not all parents may be computer literate and technologically aware. It relies on the presumption that all parents act in their child's best interests. More significantly, the GDPR fails to consider the safety and digital privacy of children whose images are shared online by their parents. The GDPR under Recital 18 exempts household and personal online activities from the constraints of the GDPR. This coupled with a failure to define and consider the actual size and scope of personal activities creates doubt as to the privacy and safety of those who are the subjects of 'sharenting'.

1.1 Recital 18 of the GDPR

The General Data Protection Regulation 2016, in recognition of the perceived vulnerabilities of children offers increased data protection to the child. Recital 38 of the GDPR stipulates that:

> 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'.

Such specific protection applies 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. This provision is novel as it openly acknowledges the vulnerabilities of children and their corresponding need for additional protection. While there may be a danger that vulnerabilities referred to under recital 38 may mask children's ability, there is also a belief that it is a

'dynamic phenomenon' with great potential for children's rights (Kisunaite 2019, 175).

Conversely, Recital 18 of the GDPR states that the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. In other words, it does not apply to activities that are unconnected to professional and commercial activities. This represents a very broad-based measure that allows for the processing of personal/household data and images with no provisions for any particular degree of oversight.

Recital 18 seems to be at odds with the protection offered by Recital 38 and appears to be embracing and deferential to the familial dynamic. In the digital arena, images are more visible, shareable and durable to known and unknown audiences, the question that should dominate is 'where does the parental self-end and the child self-begin?' (Blum-Ross and Livingstone 2017, 111). As far as adult internet users are concerned, recital 18 is mostly empowering and whether intentional or not, this measure could wind up disempowering and disenfranchising millions of future young internet users.

This measure is at odds with the Irish Constitutional amendment of 2012 which acknowledges under article 42A 'standalone' rights for all children'. There is no recognition given under Recital 18 to the possibility of imbalance within households and the tendency of parents to overwrite the privacy and freedom of expression of their children. It fails to recognise the complicated world of family life and households. Recital 18 offers households considerable latitude to post private and personal data on social media. There is no recognition given to the rights of individual members within the family/household and their individual desires and wishes. There is no acknowledgment that this broad-based measure may deprive children of their private identity and may increase their vulnerability. There is no recognition given to the fact that recital 18 may be compromising the human rights of our children who are the subjects of 'sharenting'.

Cognisant of the broad application of the GDPR with regard to the freedom of the parental right to the online sharing of personal and household activities, there is an issue with online data protection. The GDRP is a hastened attempt to address data protection. It views children as vulnerable parties and places their online protection in the hands of their parents.

This does not take account of issues such as parents' lack of competence in the digital arena, their corresponding lack of awareness of the digital footprint and the resulting abuse and misuse of abuse and misuse of data

posted online. With regard to 'sharenting', parents may use their children's images to portray themselves and their happy lives. This has the potential to create serious issues regarding the privacy and identity of children. These issues are compounded by the exemption of 'household and online personal activities' under Recital 18 of the GDPR. Recital 18 fails to define precisely what this exemption involves and in the light of the paternalistic attitude that parents always know best, this raises serious concern for the protection of the child who is the subject of 'sharenting'. This article focuses solely on the issue of 'sharenting' and the accompanying implications and dangers that it poses for the rights of children who are the subjects of 'sharenting'.

2. The Prevalence and Reasons for 'Sharenting'

Childhood and family life are undergoing increasing mediatisation (Krotz and Hepp 2013), which is resulting in a growing online visualization following a huge increase in online photograph sharing, designed to create 'online biographies' (Autenrieth 2018, 220).

It is argued that the contemporary child is conceived and raised in a world that is 'increasingly monitored, analysed and manipulated through technological processes' (Wilson 2019, 1).

Previously, much of the participation on social media was done by children when they reached a certain age (much younger than the current age of 16), however, many minors nowadays are on social media as a result of their parents' social networking. 'Sharenting' is growing and expanding at an alarming rate in most jurisdictions. Children's images are posted before birth in the form of prenatal scans and at birth. In the US, more than 90% of children under the age of 2 years have an online presence (Steinberg 2017, 849).

The Central Statistics Office (CSO, 2017) reported that 89% of Irish households in 2017 had home internet access. Smartphones were used by 87% of respondents to access the internet and social media activity was depicted as the third most popular online activity, the most popular being Facebook which, in March 2018, claimed 2.2 billion monthly active users (Facebook 2018). This online activity included networking and uploading of photographs. In 2015, Facebook, is said to have hosted over 250 billion photographs, with a daily upload rate of 350 million (Malik et al. 2016, 365). It is clear that Ireland like many other jurisdictions is engaging in the digital world, where connectivity is king. 'Sharenting' is widespread, children according to Kidron have become the 'click bait' of this decade (Kidron 2018).

Parents regard social media and 'sharenting' as having a central role in their parenting experience (Archer and Tao 2018, 134). Facebook facilitates a new wave of social interaction and allows for the sharing of content with friends and family. However, there is a tendency to forget that the Facebook environment is not the same as friendship in the off-line world (Kuczeraway and Coudert 2010, 232). Photographs are considered to be worth a thousand words and by posting them online, parents can indirectly communicate with a wide audience. This enables other users to remain informed about a person's life without the need to engage in direct conversation (Eftekar et al. 2016, 164).

Consequently, social media is a valuable vehicle for the building and maintaining of relationships. It also provides a means through which the user can convey and boost their individualism and personality.

Parents can display their artistic ability in photography. Similarly, photographs of children can acquire a social boost for the parent if they receive a lot of 'likes' or if other users leave comments on posts.

Positive attention paid to a child reflects favourably on the parent's reputation. Goffman's self-presentation theory maintains that social situations consist of persons displaying desired impressions of themselves to others (Goffman 1959). This typically means accentuating characteristics that the individual wants to highlight. People may present a preferred version of themselves, this impression being more perfect than the real version of themselves. Posting photographs on social media enables the user to engage in what Goffman described as 'impression management' and convey the desired image that they wish to present to the public (Goffman 1959). Photographs of children convey an image about the parent's ability as a loving parent and in turn depict a more positive profile as images of their laughing child signify their success as a parent and a happy home creator.

Irrespective of the reasons as to why parents share their children's images online, which are broad and are to the parents' benefit, the effects of 'sharenting' on children can be vast, wide reaching and persistent.

Discrimination against children is prevalent in the digital arena where the 'global digital divide and algorithms affect civil, social and economic rights' (Skelton and Mezmur 2019, 296).

2.1 The Effects of 'Sharenting'

'Sharenting' engenders a surveillance culture, which in turn transforms children into 'calculable persons', calculated by the parental practice of 'sharenting' and the child's own engagement with the internet of toys (Mascheroni 2018, 519). The Internet of Toys refers to the connection of

digital and physical entities to gain access to new applications and services. Toys such as 'Hello Barbie' and 'Smart Toy Bear' using voice and/or image recognition connect to the cloud which allows children›s conversations and images to be analysed and processed (Donovan RTÉ Brainstorm, 2019).

Today's child is born into and raised in a digital world that is monitored, analysed and manipulated through technological processes which has led to the 'childhood becoming a site of datafication and dataveillance' (Mascheroni 2018, 517). Visualisation is embedded deep into 'sharenting' (Autenrieth 2018, 228).

Parents post images of their children online with little comprehension or regard for the fact that they are crafting their children's online footprint and compromising their private identity along with interfering with the child's right to digital self-actualisation. Arguably, parents are sacrificing their children's privacy in return for their own positive online connectivity. Today's children are the first to grow up in this digital arena and their online presence can often begin with the uploading of their prenatal scan. Given the evolving nature of technology, it is difficult to ascertain the effects of 'sharenting'.

While the digital environment can potentially realize many rights for children, it can equally expose minors to substantial dangers and threats (Skelton and Mezmur 2019, 277). The ramifications of 'sharenting' are far reaching and long lived. Minors may regard the effects as 'interpersonal, however the monetising and misuse of personal data' have the potential to disempower and disenfranchise minors. Many parents are ill-informed as to the potential dangers of 'sharenting'. Children, whose images are posted are exposed to identity theft or misuse and may be the target of other online crime not to mention the erosion of their autonomy and self-determination (Steinberg 2017, 854).

There is also the additional threat of commercial exploitation of images (Steinberg 2017 49). While the Internet may have been hailed as the 'great equalizer', it can equally be classified as the 'great unequalizer' (Skelton and Mezmur 2019, 284). It is currently a real threat as technology is becoming increasingly advanced in its capacity to analyse photographs. Google acknowledges that the integration of artificial intelligence into its photo service facilitates the classification of photographs based on their contents. By viewing an image of a child's birthday cake, Google software can, not only, recognise the cake, but also extract other pertinent facts regarding the subjects in the photograph (Lee 2017). This shows the potential of data mining, one such potential being targeted advertising. New technologies are said to 'be capable of triggering intrusive mechanisms in human rights' with mixed results (Cocolli 2017, 225).

Sharing and curating moments of great joy in an online platform initiates a child's social media footprint and 'normalises a culture of surveillance' (Leaver and Highfield 2018, 44). This personal information facilitates specific marketing. In identifying a person's personality and interests, it can ascertain which products or services that they would be likely to buy (Corrigan et al. 2014, 161).

Facebook's primary revenue comes from not only selling advertising space, but also from the sharing of information with third parties who may in turn target the subject elsewhere. Livingstone refers to the inability of parents to recognise persuasive advertising and its potential effects for the individual child (Livingstone 2009). Livingstone contends that parents have a limited understanding and awareness of online advertising. Technology enables companies to 'track and trace' people as they visit different websites (Acquisti et al. 2016, 463). Furthermore, information collected today has the potential to manipulate the subject's privacy for years and it may result in persistent targeted advertising in later life. The evolution of data mining techniques increases the amount of sensitive information that can be garnered from collected data (Acquisti et al. 2016, 481).

The full extent and long-term effect of the practice of 'sharenting' on a child's lifetime is unquantifiable as technology is transient. This is complicated by the fact that the effect of 'sharenting' may not be immediate. Rather, it involves the amassing of a wealth of information which can be exploited in the future, making the quantification of the consequences of 'sharenting' difficult to ascertain. This underlines the need to shield children against the publication of their image on social media and it illustrates the depth of potential repercussions.

It is not the mere display of photographs on social media that alone can cause harm, but rather the commercial advantages that may be extracted from these images now and in the future.

Those young people who have been born into and are growing up with technology and social media are known as generation z and although they are particularly 'adept in the use of technology, their awareness of the impact of social media on their privacy is limited' (Oswald et al. 2016, 199). There is a strong presumption that the family always acts in the child's best interests. Research indicates that while some parents may consider consulting their minor children prior to uploading photographs, the majority rarely considered the child's opinion justifying their position by claiming that parents have a right to 'decide and to control the information shared' (Siibak and Traks 2019, 118). Society needs to move away from the belief that the family is above scrutiny. The 2012 Irish Constitutional Amendment acknowledging

the child's stand-alone rights serves no purpose if one continues to regard children's rights as being aligned exclusively with those of the parent.

The implications of 'sharenting' are real for minors and have the potential to have long lasting effects on minors' lives. However, the wider implications of 'sharenting' pose a more serious threat to minors' wellbeing. The manner in which 'sharenting' impinges on the child's right to a private identity, freedom of expression and protection is all too substantial to be disregarded. In addition, information shared can be de-contextualised, which could have significant ramifications for the digital privacy of the minor in question. Privacy settings could prove a valuable tool in preventing the compromise of private data. However, the ambiguity of privacy settings along with consumers' lack of awareness with the complexity of the tool and a lack of transparency all contribute to the challenge associated with the preservation of privacy (Kuczeraway and Coudert 2010, 238). Arguably 'sharenting' is undertaken with little regard for the child's rights although it represents a serious incursion into children's rights to privacy, autonomy and protection. The ephemeral benefits of 'sharenting' derived by parents can have longstanding effects on the child's privacy and private identity which can continue far into the adult life of the child. Forgetting personal information can be difficult and costly, whereas, remembering proves inexpensive and relatively easy to store.

Despite the introduction of the GDPR in an effort to comply with article 8 of the UNCRC which preserves the child's identity, it has resulted in the compromise of the child's right to privacy under article 16, right to freedom of expression under article 13 and the right to protection under article 19 of the UNCRC.

3. The Right of the Child to Privacy and a Private Identity

'Sharenting' contributes to the "normalisation of a culture of surveillance" (Leaver and Highfield 2018, 43) and represents a major interference with the child's right to privacy and a private identity. In addition, the persistence of a single online identity means that information shared about a child will persist as an inescapable representation of him/her into adulthood (Leaver 2015, 1). Irrespective of the compliance or non-compliance with privacy settings, 'sharenting' creates an indelible footprint in the online arena. The Irish constitution under article 40.3^0 guarantees in its laws 'to respect, and as far as practicable, by its laws to defend and vindicate the personal rights of the citizen'.

The right to privacy was first recognised in this jurisdiction in *McGee v Attorney General*, Walsh J. in the Supreme Court held that 'Article 41 of the Constitution guarantees the husband and wife against……invasion of their privacy by the State.' In *Kennedy and Arnold v Attorney General*, Hamilton P. held that the right to privacy was one of the unenumerated rights recognised by Article 40.3[0] of the Constitution.

The Convention on the Rights of the Child (CRC) under Article 3 which supports the best interests of the child can be regarded as establishing a legal foundation for the right to privacy and imposing an obligation to protect a child's right to privacy (Art.16). It recognises a child's right to privacy stating that, 'no child shall be subjected to arbitrary or unlawful interference with his or her privacy' (Art.16(1)). It supports the 'best interests' of the child's principle and specifies that it is a State's duty to oversee the necessary care and protection of the well-being of a child, acknowledging at the same time the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her. States Parties are obliged to take all appropriate legislative and administrative measures (Art.3(2)).

In addition, the CRC under article 8 undertakes to respect the child's right to preserve his/her identity. The European Convention of Human Rights (ECHR) states that 'everyone has the right to respect for his private and family life, his home and his correspondence' (Art.8).

The protection of privacy is also guaranteed by the Charter of Fundamental Rights of the European Union (Art.8), while the treaty on the Functioning of the EU upholds the right to the protection of personal data (Art.16).The right to privacy was successfully invoked before the European Court of Human Rights (ECtHR) in *Von Hannover v Germany* in an application brought by Princess Caroline of Monaco. She claimed that the German courts had failed to protect her right to privacy following the publication of her family's photographs in several German magazines. The ECtHR employed a balancing act between the applicant's right to privacy (Art.8) and the media's right to freedom of expression (Art.10) under the ECHR.

The ECtHR ruling focused solely on the publication of the photographs, however, this judgment is noteworthy as it implies that Article 8 of the ECHR supports the view that everyone is entitled to a stringent level of privacy protection regardless of his/her status as a public figure.

However, in *Von Hanover* (2), the Courts were not willing to accept that the applicants claim to be 'ordinary private individuals', the relaxation of the terms 'public figure'' and 'debate of general interest'' broadened the scope of a Convention-compliant publication.

'Sharenting' has not, as yet, been analysed by the European Court of Human Rights and in the event of that occurring, it is anticipated that the Court

might attempt to balance the child's right to privacy and the parent's right to freedom of expression, as the publication of photographs is a recognised component of freedom of expression. The status of the child as a member of the public, rather than a figure of public importance, would afford them a greater degree of privacy.

With regard to the prior conduct of the applicant, it was held in *Egeland and Hanseid v Norway* that earlier participation in media activities did not deny the applicant the right to privacy in later situations. In the event of a clash between parental and children's interests, parental interests have the upper hand unless the courts decide otherwise. However, in *Re Z* (A Minor), an injunction was granted by the Court of Appeal to prevent Channel 4 (despite the mother having previously consented) from identifying a child with special educational needs.

Whilst legal guardians are presumed not to present their children in a negative way, interpretation of photographs can be subjective thus providing basis for an argument that privacy has not been breached. The audience size of the publisher is another relevant factor that may be worthy of consideration by the ECtHR. In addition, the privacy settings on the legal guardian's account would be of relevance as the proof of a breach may depend on whether or not the photographs are set to 'public'. The scope of the public domain is ambiguous (Mills 2017, 53). Courts have delivered conflicting judgments as to the thresholds of the 'public' audience, the conflict centres sometimes around the difference between print media and online media. The Northern Ireland High Court in *Martin* contended that the posting of a status on a private Facebook page was destined to the public at large (*Martin and Ors v Gabriele Giambrone P/A*, 2013), whereas in the *Weller* case, the appearance of a photograph on a Facebook archive and on a Tumblr account did not constitute a wide publication (*Weller and Ors v Associated Newspapers Limited*, 2014). The uploading of children's photographs to social media, however, highlights the need for consent. It raises the question as to whether, parents should be able to consent on their child's behalf. Privacy issues are often additionally compounded by the battle between 'relational and individualistic conceptions of identity, ethics and responsibility' (Blum-Ross and Livingstone 2017, 112).

The ruling in *Reklos and Davourlis v Greece* demonstrates that the ECtHR currently considers parents to be capable of such consent on their children's behalf. Thus, because parents assume competence for consenting to taking and disseminating images, they can legitimise their own activities on social media, activities which would amount to a clear breach of privacy if done by a third party without consent. In examining the issue of consent, the ECtHR concluded that: '[a] person's image constitutes one of the chief attributes

of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers' (*Reklos and Davourlis*). The right to protect one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image (*Reklos and Davourlis*). This 'control right' includes the ability to refuse the capture of one's image along with the manner, if any, of the dissemination of the image. It was held that consent is a necessary precondition to the acts of both photography and dissemination.

The court concluded that, if Article 8 of the ECHR was not applied in this manner, 'an essential attribute of personality would be retained in the hands of a third party and the subject matter of the image would have no control over any subsequent use of the image'(*Reklos and Davourlis*).

However, the ECtHR in *Reklos* recognised that, in the absence of consent, the act of photography was an invasion of privacy. This ruling could be applied likewise to children whose images are posted online without consent. In *Von Hannover*, the privacy breach rested solely on the lack of authority to disseminate the photographs, there was no reference to consent to taking the photographs.

The failure to acknowledge the centrality of consent in privacy may lead to privacy infringements. Ortiz maintained that the difficulty of privacy laid in the determination of its boundary and that consent must feature strongly in the whole privacy issue (Ortiz 1989, 92). However, others caution against overreliance on consent and they contend that 'consent and anonymity should not bear, and should never have borne, the entire burden of protecting privacy' (Baracos and Nissenbaum 2014, 33). Consent cannot be expected to be a 'silver bullet' in the protection of privacy. Arguably, practices initially consented for may adjust or change without the necessary adjustment in consent.

Today, individuals online are often presented with a 'binary choice, consent or abandon', the consent requiring one to agree to vague and complex privacy notices written in 'complex legal' language (Cate and Mayer-Schonberger 2013, 67). In practice, this does not represent the ideal way of ensuring the protection of either information privacy or the free flow of information.

Regardless of the merits pertaining to the concept of consent, social media applies a 'take it' or 'leave it' attitude towards consent with connectivity depending on 'take it'. There appears to be a huge disconnect between consent policies and people's aptitudes to read, comprehend and assent to privacy policies. In particular, with regard to the issue of consent in social networks, research shows that people mostly do not read privacy policies, as they tend to be too complicated or too long to read (Obar and Oeldorf-Hirsch 2020, 142). Reading them might not be convenient at the moment of

downloading an app or signing up for an online service. Privacy policies are generally not very appropriate for small screens, some of the apps do not have a privacy policy.

Regardless of whether or not, parents read privacy policies, their knowledge pertaining to the privacy policies remain the same due to the vague terms.

Moreover, privacy processes are complicated and opaque, perhaps the lack of clarity is intentional. This lack of transparency and difficulty of comprehension may be intentional to facilitate the manipulation of the consumer. This deficit information may often be the deciding factor in one's decision to download or not download a particular a

4. The Right to Autonomy and Digital Self-actualisation

The CRC in article 13 stipulates that the

> *'child shall have the right to freedom of expression and that this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.'*

The exercise of this right may be subject to certain restrictions, but 'these shall only be such as are provided by law and are necessary:

> *(a) for respect of the rights or reputations of others; or (b) for the protection of national security or of public order, or of public health or morals.' There is no provision in this article for the parental assumption of this right.*

The online practice of 'sharenting' removes the autonomy of the child and denies them the right to craft their own footprint on a blank online canvas which should be the birth right of every child. The CRC undertakes to uphold the right of the child under article 13 to seek, impart and seek information through any medium of their choice, in other words, the child shall have the right to craft his/her identity on a blank canvas without any input from anyone else.

It is argued that autonomy or self-determination like happiness is 'a matter of degree as the conditions for individual autonomy are diverse' and so much so that it would be difficult to legislate to ensure the explicit guarantee of a 'right to autonomy' (Rouvroy and Poullet 2009, 59). It should be the right and choice of every individual to craft or at least consent to the crafting of his/her online identity.

Children should have the opportunity to control the data and information produced about them so that that they can live an existence predetermined

by them (Rouvroy and Poullet 2009, 51).'Sharenting' has resulted in minors' identity being crafted as a digital tattoo which is difficult to erase. 'Sharenting' represents one of the most initial incursions into the minor's digital identity.

The initial piercing of a minor's identity privacy leaves the path free for other incursions into the minors' identity and exposure to crime and identity theft.

5. The Right to Protection

The CRC under article 19 stipulates that States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence. 'Sharenting' exposes children to potential crime and it renders them voiceless and powerless. The right of the child to protection is recognised as one of the core principles of the GDPR. 'Sharenting' results in the exposure on children in the world media stage. Prior to the advent of social networking, children did not face such extreme exposure and potential safety threats. 'Sharenting' is contributing to the increasing presence of children in the online arena, which is accompanied by additional exposure to additional threats such as datafication and dataveillance and results in them being targeted.

Individuals' decisions and opportunities are shaped by dataveillance, with the voices of children displaced by technology and algorithmic calculations (Lupton and Williamson 2017, 790).

Equally, older children's online behaviour is being tracked by means of cookies and plug-ins (Lievens and Verdoodt 2018, 269). Children are 'contributors to the unpaid digital workforce', they are unaware as to how their personal details are exploited to construct detailed profiles which may be used for a variety of purposes (Lupton and Williamson 2017, 787).

Currently, the data collected on children is used to dictate market direction and business practices, the digital world is a commercial entity built on economic interests (van der Hof 2016, 415). Children live under a giant microscope and are subjected to surveillance and continuous judgment. It is contended that children are understood and portrayed through the algorithmic knowledge that aggregate and analyse them as elements of big data sets (Leaver 2017, 8). Children's behaviours, qualities and bodies are classified into digital data, which is used to make assessments, judgements or inferences about them.

This classifying of children as algorithmic assemblages results, not only, in the overlooking of their complexities, potentialities and opportunities, but children are encouraged to view and compare themselves with others

using these assemblages (Lupton and Williamson 2017, 787). They become the subjects of calculations performed by digital things.

Thus children, calculated and metricized as data traces, are encouraged to assess themselves through the study of their own data (Lupton and Williamson 2017, 787). It is recognised and accepted that the Internet of Things now facilitates the collection of personal information including that of individual's preferences and choices which are used to profile the individual (Rinik 2019, 2).

The right of the child is not considered in the process of datafication. There is, however, consensus that datafication and dataveillance erodes their privacy (Lupton and Williamson 2017, 786). There are now significant ramifications for breaches of people's rights to data privacy, potential privacy harms and security issues arising from the current collection and use of personal information. In addition, there are companies engaged in undercover dataveillance with the result that the 'datafied' individuals are unable to exercise their right to privacy and data protection (van der Hof 2017, 418). Hacking for malicious or cyber-criminal purposes occur regularly, leading to the revelation of individuals' private data. It is argued that 'surveillance appears to be woven into every element of an online and digital society', there is no escaping dataveillance (Leaver 2017, 3).

Even in the absence of personal information, the metadata behind photographs and technologies which facilitate user tagging, automated facial recognition and the accumulation of discrete pieces of information provides significant amounts of personal information (Bessant 2018, 4). Photographs may be altered and re-used on illegal websites. All photographs of children have the potential to be fodder for bullying and ridicule (Bessant 2018, 8).

'Sharenting' represents a serious incursion into the human rights of minors. Social media providers, culpable in their dereliction of duty towards social media users, have frequently been found to be non-compliant with GDPR.

6. Internet Service Providers and Minors and Their Compliance with the GDPR

In recognition of the potential adverse consequences associated with 'sharenting', and despite social media providers' assurances of compliance with the child's best interests, the non-compliance of network providers is widespread and provokes concern. Prior to the introduction of the GDPR, there was little or no regard for the vulnerability of children in Silicon Valley. Despite assurances of compliance and calls by internet service providers for governmental action to assist them to protect consumers' safety and

privacy, social media providers tend to put their own interpretation on the law. They tend to adapt their regulations and have not shown themselves overly compliant with the GDPR. While Facebook tried to comply with the European driven privacy recommendations, their improvements are said to be accompanied by efforts to encourage users to share additional information (Kuczeraway and Coudert 2010, 231). Facebook has been fined for allowing Cambridge Analytica to access and harvest the personal data of 87 million Facebook users (Cadwalladr et al. 2018).

Unlike pre-GDPR existence, Facebook, following a data breach in September 2018 could face a fine of up to 4 percent of its annual global turnover which, based on its past fiscal year, could amount to $1.63 billion. Due to separate attacks, hackers were able to access and take over 50 million users' accounts. The GDPR requires that companies must notify the relevant data protection authority, within 72 hours. However, Facebook was not entirely compliant in that it reported just within the three-day limit and did not share all the pertinent details with the Irish Data Protection Commissioner. Another, unrelated bug had exposed 6.8 million users' private photos to up to 1,500 different applications for nearly two weeks. This bug had been discovered and fixed, yet Facebook did not alert affected users, the public, or authorities for almost three months.

Facebook has tried different strategies to circumvent the intent of the GDPR, such as complying with the timeline set out by the GDPR but omitting crucial details. In addition, Facebook interpreted the GDPR as saying that a company has an unlimited period of time to investigate a breach. Once the investigation is complete, and the company has decided that the breach is 'reportable,' then the three-day time limit kicks in. The French data protection watchdog (CNIL) imposed a GDPR fine (€50 million) on Google, claiming that it failed to comply with the General Data Protection Regulation (GDPR) when Android users set up a new phone and follow Android's on-boarding process. The CNIL concluded that Google failed to comply with the GDPR on the grounds of transparency and consent.

With regard to transparency, essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for the advertisement personalization, are disseminated across several documents, with buttons and links on which it is required to click to access complementary information. The CNIL ruled that Google's wording is deliberately obscure, thereby making it difficult to understand how customers' data is used.

Furthermore, Google's consent flow does not comply with the GDPR according to the CNIL. Google tend to bundle up consent which is illegal under the GDPR. The creation of an account should be separate from the

setting up a device. In the event of signing up to an account, one is asked to 'tick' or 'untick' some settings with no explanation as to the ramifications. Google in asking an individual if they want personalized advertisements fails to clarify that many different services, from YouTube to Google Maps and Google Photo are being referred to and it is not referring to one's Android phone alone.

In addition, Google does not ask for specific and unambiguous consent on the creation of an account, the option to opt out of personalized advertisements is hidden behind a 'more options' link. That option is pre-ticked by default. Finally, by default, Google ticks a box that agrees to the processing of one's information as described above and further explained in the 'Privacy Policy' when an account is created. Broad consent like this is also forbidden under the GDPR.

Evidence reveals that social networking represents a potential threat to minors, the GDPR's exemption of household and personal online activities from any degree of oversight has the potential to expose children to danger and erode their privacy. Social network providers' assurances of oversight do little to allay concerns. On a positive note, the Court of Justice of the European Union (CJEU) has been proactive and has adjudicated that the 'Safe Harbour Framework' was invalid on the grounds that US Legislation did not limit interference with an individual's rights as it failed to identify any objective criteria for determining limitations to the access and use of personal data by public authorities (Schrems 1 Case C-362/14 Commission Decision 2000/520/EC). Furthermore, Advocate General Saugmandsgaard cautiously backed data transfers generally but sharply criticized the EU-US Privacy Shield agreement and called for due diligence and caution in the use of standard contractual clauses (SCC) (Schrems 11 Case C-311/18 December 2019). It is envisaged that these words of caution will strongly influence future policy relating to data transfer.

Conclusion

In recognition of the right of the child to privacy and a private identity, the GDPR was introduced to address the issue of child safety and protection. It introduced a suite of protective measures supporting the rights of the child to privacy and safety. Among such measures are the need for consent to process the data of minor children, the prohibition on the processing of biometric data and the right of children to data portability, erasure and the right to be forgotten. Despite the rationale of the GDPR being in favour of the protection and safeguarding of children's privacy and private identity, it

fails to address the right to privacy and a private identity of children who are the subjects of 'sharenting'.

Furthermore, it neglects to acknowledge the possibility that parents may not be technologically competent to safeguard their children's privacy or that they may not always feel obliged to act in their child's best interests. The use of 'Sharenting' as a means to validate their roles as parents has grown exponentially and has resulted in the online exposure of children's identity with no regard for ramifications such as identity theft, online crime and deprivation of autonomy and the right to self-actualisation.

The GDPR exempts household activities from the Protection constraints imposed on the processing of children's data. This exemption is very broad and there is no attempt to define where parents' rights end and children's rights begin. This identifiable lacuna in the GDPR leaves minor children without any protective provisions for their privacy and private identity. The GDPR under recital 18 tends to favour paternalism, which has problematic consequences for children as rights holders especially their agency and rights to access, information, privacy and participation (Livingstone et al. 2015, 5). Minor children who are the subjects of 'sharenting' have become the forgotten children of the twenty first century.

The discourse around the protection of children from online predators and the freedom of older children to online interaction that is free from parental supervision needs to shift to include the protection of children from 'sharenting' (Sorensen 2016, 156). Parental rights over children need to move away from property-like underpinnings to that of trustees (Sorensen 2016, 176). Some like Sorensen argue that parents should assume the role of trustees over their children's privacy and private identity until such time as they become autonomous individuals, whereas others such as Steinberg advocate parental rights embracing a 'child-centric perspective' (Siibak and Traks 2019, 117).

Irrespective of the role of parents, 'Sharenting' represents a lot of dangers for children, not only are children denied the right to craft their own digital footprint, but they are also denied the right to self-determination. In addition, there is the exposure to online crime resulting from data mining and datafication. The 'omnipresence' of social media sharing leaves our minors in a vulnerable position (Mills 2017, 71). The GDPR offers no succour or support to minors who are the subjects of 'sharenting', this glaring omission of support stems from the fact that there is a strong presumption that parents always act in their child's best interests. However, in the words of Craig Hill, 'parents by their words and actions possess the ability to bless or curse the identities of their children' (Hill 2013).

Acknowledgements

The author accepts full responsibility for any errors and omissions and would like to thank Dr. Connie Healy (Lecturer above the Bar at NUI Galway) for her valuable input.

References

Acquisti, A., Taylor, C., Wagman, L. (2016) 'The Economics of Privacy', *Journal of Economic Literature,* 54(2), 442-492.

Albrecht, J. (2016) 'How the GDPR Will Change the World', *European Data Protection Law Review*, 2(3), 287-289.

Archer, C., Kao, K-T. (2018) 'Mother, baby and Facebook makes three: does social media provide social support for new mothers?', Media International Australia, 168(1), 122-139.

Autenrieth, U. (2018) 'Family photography in a networked age' in Mascheroni, G., Ponte, C., Jorge, A. (eds.), *Digital Parenting. The Challenges for Families in the Digital Age*, Goteborg: Nordicom, 219-231.

Baracos, S., Nissenbaum, H. (2014) 'Computing Ethics: Bid Data's End Run around Procedural Privacy Protections', *Communication of the ACM*, 57(11), 31-33.

Bessant, C. (2014) 'Data protection, safeguarding and the protection of children's privacy: exploring local authority guidance on parental photography at school events', *Information and Communications Technology Law*, 23(3), 256-272.

Bessant, C. (2017) 'Parental rights to publish family photographs versus children's rights to a private life**',** *Entertainment Law Review*, 28(2), 43-46**.**

Bessant, C. (2018) 'Sharenting: balancing the conflicting rights of parents and children' *Communications Law*, 23(1), 7-24.

Bessant, C. (2016) 'Photographs of children in public : the wider significance of Weller v Associated Newspapers', *Entertainment Law Review***,** 27(6), 197-201.

Blum-Ross, A., Livingstone, S. (2017) 'Sharenting', parent blogging and the boundaries of the digital self', *Popular Communication*, 15(2), 110-125.

Brown, D., Pecora, N. (2014) 'Online Data Privacy as a Children's Media Right: Towards Global Policy Principles', *Journal of Children and media*, 8(2), 201-207.

Buttarelli, G.(2016) 'The EU GDPR as a clarion call for a new global digital standard', *International Data Privacy Law*, 6(2), 77-78.

Cate, F.H., Mayer-Schonberger, V. (2013) 'Notice and Consent in a World of big Data', *International Data Privacy Law*, 3(2), 67-73.

Charter of Fundamental rights of the European Union, retrieved from: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed:10/2/2019).

Coccoli, J. (2017) 'The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era', *Peace Human Rights Governance*, 1(2), 223-250.

Corrigan, H., Craciun, G., Powell, A. (2014) 'How Does Target know So Much About Its Customers? Utilizing Customer Analytics to Make Marketing Decisions' *Marketing Education Review*, 24(2), 159-165.

Custers, B., van der Hof, S., Schermer, B., Appelby-Arnold, S., Brockdorff, N. (2013)'Informed consent in Social Media Use - The Gap between User Expectations and EU Personal Data Protection Law', *A Journal of Law and Technology*, 10(4), 435-457.

Data Protection Commissioner -v- Facebook Ireland Ltd & Anor, (2019) IESC 46 (2019).

Donovan, S. (2019) 'The bear is listening: the high cost of smart toys' *RTÉ Brainstorm* NUI Galway, 17 December, 2019, retrieved from: https://www.rte.ie (accessed: 20/12/2019).

Eftekhar, A., Fullwood, C., Morris, N. (2014) 'Capturing personality from Facebook photos and photo-related activities: How much exposure do you need?', *Computers in Human Behaviour*, 37(C), 162-170.

Egeland and Hanseid v Norway Application Nos. 34438/04 (16th April 2009).

European Convention on Human Rights and Fundamental Freedoms, 1950, Retrieved from: https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed: 12/10/2018).

Facebook, 'How does Facebook's face recognition work?', retrieved from: https://www.facebook.com/help/1221755507864081?helpref=faq_content>?helpref=faq_content (accessed: 10/12/2018).

Flanagan, M. (2019) *Photography and The Law. Rights and Restrictions*, London& New York: Routledge.

General Data Protection Regulation (EU) 2016/679, retrieved from: https://gdpr-info.eu/ (accessed:12/10/2018)

Goffman, E. (1959) *The Presentation of Self in Everyday Life*, New York: Doubleday.

Google v Spain C-131/12 (13 May 2014) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Kidron, B. (2018) 'Are children more than the 'click-bait' in the 21st century?' *Communications Law*, 23(1), 25-30.

Kisunaite, A. (2019) 'Children's Rights Protection in the EU: The Need for a Contextual Perspective', *Peace Human Rights Governance*, 3(2), 171-192.

Krotz, F., Hepp, A. (2013) 'A Concretisation of Mediatisation: How "Mediatisation works" and why mediatised worlds are a helpful concept for empirical mediatisation research', *European Journal for the Philosophy of Communication*, 3(2), 119-134.

Kuczerawy, A., Coudert, F. (2010) 'Privacy Settings in Social Networking Sites: Is it fair?, in Fischer-Huber, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (eds.), *Privacy and Identity Management for Life*, Springer Science & Business Media, 231-243.

Leaver, T. (2015) 'Researching the Ends of Identity: Birth and Death on Social Media', *Social Media & Society*, 1(1), 1-2.

Leaver, T., Highfield, T. (2018) 'Visualising the ends of identity: pre-birth and post-death on Instagram', *Information, Communication & Society*, 21(1), 30-45.

Leaver, T. (2017) 'Intimate Surveillance: Normalising Parental Monitoring and Mediation of Infants Online', *Social Media & Society*, 3(2), 1-10.

Lee, D. (2017) 'The five big announcements from Google I/O', BBC News, retrieved from: http://www.bbc.com/news/technology-39958028 (accessed: 20/12/2018).

Lievens, E., Verdoodt, V. (2018) 'Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation', *Computer Law & Security Review*, 34(2), 269-278.

Livingstone, S. (2005)'Mediating the public/private boundary at home: children's use of the Internet for privacy and participation', *Journal of Media Practice*, 6(1), 41-51.

Livingstone, S. (2018) 'Children: a special case for privacy?', *Intermedia*, 46(2), 18-23.

Livingstone, S., O'Neill, B. (2014) 'Children's Rights Online: Challenges, Dilemmas and Emerging Directions', vol .24, in Van der Hof, S., Van den Berg, B. Schermer, B. (eds.), *Minding Minors Wandering the Web:Regulating Online Child Safety*, The Hague: Asser Press, 20-38.

Livingstone, S., Haddon, L. (2009) *Introduction – Kids online: Opportunities and risks for Children*, Bristol: The Policy Press.

Lupton, D., Williamson, B. (2017) 'The datafied child: The dataveillance of children and implications for their rights', *New Media & Society*, 19(5), 780-794.

Macenaite, M. (2016) 'Protecting Children's Privacy online: a critical look to four European self-regulatory initiatives', *European Journal of Law and Technology*, 7(2), 1-26.

Macenaite, M. (2017) 'From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation', *New Media & Society*, 19(5), 765-779.

Macenaite, M., Kosta, E. (2017) 'Consent for processing children's personal detain the EU: following in US footsteps?', *Information & Communications Technology Law*, 26(2), 146-197.

Malik, A., Hiekkanen, K., Nieminen, M. (2016) 'Impact of privacy, trust and user activity on intentions to share Facebook photos', *Journal of Information, Communication and Ethics in Society*, 14(4), 364-382.

Martin and Ors v Gabriele Giambrone P/A, Giambrone & Law, Solicitors & European Lawyers (2013)NIQB 48.

Mascheroni, G. (2018) 'Researching datafied children as data citizens', *Journal of Children & Media*, 12(4), 517-523.

Mills, M. (2017) 'Sharing privately: the effect publication on social media has on expectations of privacy', *Journal of Media Law*, 9(1), 45-71.

Montgomery, K., Chester, J., Milosevic, T. (2017) 'Children's Privacy in the Big DataEra: Research Opportunities', *Paediatrics*, 140(2), 117-121.

Nissenbaum, H. (1998) 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', *Law and Philosophy*, 17(5/6), 559-596.

Nissenbaum, H. (2009) *Privacy in Context: Technology, Policy and the integrity of social life*, California: Standford Law Books.

Nissenbaum, H. (2011) 'A contextual approach to privacy online', *Daedalus Journal of the American Academy of Arts & Sciences*, 140(4), 32-48.

Obar, J., Oeldorf-Hirsch, A. (2020) 'The biggest lie in the Internet: ignoring the privacy policies and terms of service policies of social networking services', *Information, Communication & Society*, 23(1), 128-147.

Ortiz, D.R. (1989) 'Privacy, Autonomy and Consent', *Harvard Journal of Law and Public Policy*, 12(1), 91-97.

Oswald, M., James, H., Nottingham, E. (2016) 'The not-so-secret life of five-year-olds: legal and ethical issues relating to disclosure of information and the depiction of children on broadcast and social media', *Journal of media Law*, 8(2), 198-228.

Palmer, A. 'Facebook reveals bug exposed up to 6.8 million users' unposted photos to apps' (14 December 2018), Daily Mail, retrieved from: http://www.dailymail.co.uk (accessed: 15/12/2018).

Re Z (AMinor) (1996)1 FLR191.

Reklos and Davourlis v Greece, Application Nos. 1234/05 15th January 2005.

Rouvroy, A., Poullet, Y. (2009) 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., Nouwt, S. (eds.), *Reinventing Data Protection*, Amsterdam: Springer.

Schrems 1 Case C-362/14 2000/520/EC.

Schrems 11 Case C-311/18 December 2019.

Siibak, A., Traks, K.(2019) 'The dark sides of sharenting', *Catalan Journal of Communication & Cultural Studies*, 11(1), 115-121.

Skelton, A., Mezmur, B. (2019) 'Technology Changing @ Dizzying Pace: Reflections on Selected Jurisprudence of the UN Committee on the Rights of the Child and Technology', *Peace Human Rights Governance*, 3(3), 275-305.

Sorensen, S. (2016) 'Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights', *Children's Legal Rights Journal*, 36(3), 156-176.

Staksrud, E., Livingstone, S. (2009) 'Children & Online Risk. Powerless Victims or Resourceful Participants?', *Information, Communication & Society*, 12(3), 364-397.

Steinberg, S. (2017) 'Children's Privacy in the age of Social Media', *Emory Law Journal*, 66(4), 839-884.

United Nations Convention on the Rights of the Child 1989, retrieved from: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx (accessed: 12/3/2019).

van der Hof, S. (2016) 'I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World', *Wisconsin Int'l Law Journal*, 34(2), 409-445.

van der Hof, S. (2016) 'Minding Minors Wandering the Web: Regulating Online Child Safety,' *SCRIPTed*, 13, 219.

van der Hof, S., van der Berg, B., Schermer, B. (eds.) (2014) *Minding Minors Wandering the Web: Regulating Online Child Safety*, The Hague: Asser.

Von Hannover v Germany (2004) EMLR379 ; (2005)40EHRR1.

Weller and Ors v Associated Newspapers Limited (2014)EWHC1163 (QB)

Wilson, M. (2019) 'Raising the ideal child? Algorithms, quantification and prediction', *Media, Culture & Society*, 41(5), 620-636.