DEFENDING CHILDREN'S RIGHTS MINDING CHILDREN'S PRIVACY AND DEVELOPMENT IN LIGHT OF THE GENERAL DATA PROTECTION REGULATION

George Bouchagiar
Attorney-at-law, Tutor/Research Fellow on Data Protection/IP,
Ionian University (Kaloheretu 14, Corfu, Greece, 49100)
georgebouchayar@yahoo.gr

Maria Bottis
Associate Professor on Information Law,
Ionian University (Ioannou Theotoki 72, Corfu, Greece, 49100)
botti@otenet.gr

Abstract

The law has always recognized children's special needs for protection. Children are vulnerable also in relation to the processing of their data, since they are less aware of risks emerging from data processing. The new General Data Protection Regulation (General Data Protection Regulation 2016 (EU), GDPR) has strengthened children's safety. Higher transparency standards are now required. Any information offered should be in a clear language that the child can easily understand. The right to be forgotten is reinforced when a child has given her consent to data processing, but later wishes to withdraw this consent. Children's rights and freedoms may override the interests of the controller and could render processing unlawful. Minors below the age of 16 can consent only via a parent. This chapter focuses on challenges posed by the new GDPR (General Data Protection Regulation 2016 (EU)) and on potential benefits for children's rights to data protection.

Keywords: GDPR, children, data protection, consent, right to erasure.

1. Introduction

Children enjoy a fundamental right to freedom of expression (United Nations Convention on the Rights of the Child 1989 (UN), Article 13) and a right to education (United Nations Convention on the Rights of the Child 1989 (UN), Articles 28, 29) as well as a right to development (United Nations Convention on the Rights of the Child 1989 (UN), Article 6) and a right to privacy (United Nations Convention on the Rights of the Child 1989 (UN), Article 16), rights protected constitutionally in most European, and other, countries. As firms and organizations process a huge volume of children's personal data, whose lives have become increasingly datafied (Lupton & Williamson, 2017, p. 781), the interplay and the balancing of these rights has become increasingly strenuous in the current digital world.

Children may benefit from all digital services offered to enhance their creativity, participation, interaction, or self-expression, but they are also threatened by "digital risks" emerging from (to name but a few) cyber-bullying, targeted advertisements or hateful speech (Palfrey, Sacco, & Boyd, 2008, p. 17). Parents tend to, covertly or overtly, monitor children's behavior (Livingstone & Helsper, 2008, p. 589) or control on their online activities. Innovative technologies allow and encourage parents to engage in such monitoring (Family Online Safety Institute, 2011, p. 3-4; Kirwil, 2009).

Existing tools empower parents to set limits with regard to time spent online, content visited, or services offered (Family Online Safety Institute, 2011). Mobile apps, promising "continuous connectivity", are designed for parents to track whereabouts of their children. The so-called "Quantified Self", i.e. any individual engaged in self-tracking of any kind of biological, physical, behavioral, or environmental information (Swan, 2013, p. 85-86), renders bodies transparent and calculable: via an application human behavior, e.g. sleeping patterns or how many steps one walked, may be measured, managed, and monitored even more deeply. However, data distribution on the Internet allows remote-tracking of others' data, which leads to a "Quantified Otherness", in which others are approached through data (Gabriels, 2016, p. 176). Smart applications, such as 1TopSpy (FAQs – 1TopSpy Cell Phone Spy App, 2014), secretly record SMS messages, Call history, Contact list, Web visited history, or Applications usage history, and track GPS location of the phone in real time. The target-phone holder is unaware that the application is installed and, as no response or participation is required, parents may control children without any interaction.

Since technological developments refl ct what society values, such applications can be regarded as leading examples of the contemporary desire for "truth-making machines" (Gregg, 2013, p. 307). Many "tracking-tools", like Life360 (https://www.life360.com/), are offered free of charge. The endless capabilities of digital technology monitoring raise the question of how to better protect children's rights in relation to their data.

2. The GDPR and children's data processing

The Data Protection Directive (DPD, Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 (EU)) did not mention the word "children" and, hence, treated both adults and children equally. However, as children became avid users of technologies (Article 29 Data Protection Working Party, 2013, p. 26), attention was drawn to strengthening their right to personal data protection (Article 29 Data Protection Working Party, 2009, p. 2). After having recognized minors' vulnerability (Article 29 Data Protection Working Party, 2010, p. 17), decision-makers accepted that children are less aware of risks and they, hence, merit specifi protection that should, in particular, apply to use of data for the purposes of marketing or creating profiles (General Data Protection Regulation 2016 (EU), Recital 38). So, higher transparency standards are required and, for instance, any information should be in plain language that children can easily understand (General Data Protection Regulation 2016 (EU), Recital 58, Article 12(1)).

A child is every human being below the age of eighteen years, unless she has acquired legal adulthood before that age (Article 29 Data Protection Working Party, 2009, p. 3; United Nations Convention on the Rights of the Child 1989 (UN), Article 1). But defining a child so broadly could negatively impact older children's rights and, in particular, their ability to access the Internet and express themselves freely (Montgomery & Chester, 2015, p. 289). Indeed, children are in a special situation that could be seen from a static and a dynamic perspective (Article 29 Data Protection Working Party, 2009, p. 3): they are persons who have not yet achieved physical and psychological maturity (static point of view), and they are in the process of developing physically and mentally to become adults (dynamic point of view) (Article 29 Data Protection Working Party, 2009, p. 3). Under the GDPR, the European legislator took such concerns into account and made clear that when "information society's services" are offered "directly" to a child, personal data processing is lawful when the child is at least sixteen years old –and has given consent– while, where the child is below that age, consent must be given by the holder of parental responsibility (General Data Protection Regulation 2016 (EU), Article 8(1)). An "information society's service" is defined as any service normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services (General Data Protection Regulation 2016 (EU), Article 4(25); Directive laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services 2015 (EU), Article 1(1)(b)).

As payment is a condition in this case, one could question whether advertising services, services provided by non-profit e.g. educational) organizations, or in general all "free digital services" (e-mail services etc) are included in the list. Moreover, these "information society's services" are required to be offered "directly" to a child, but it is not very clear

whether these refer to services that are targeted to children (like Facebook's "messenger kids": https://messengerkids.com/) or to those that are offered on a daily basis (such as the very Facebook itself). Further uncertainties concerning harmonization could emerge, as Member States may provide by law for a lower age, provided that it is not below thirteen years (General Data Protection Regulation 2016 (EU), Article 8(1)). Hence, different age thresholds can be set by national laws. Given the complexities of the digital environment, which question parents' capacity to make better decisions than their children (Hof, 2016, p. 434), a high age threshold could pose risks, putting too much responsibility in the hands of those who are not always familiar with technologies. There are no exceptions with regard to parents' consent (unless children's data is processed in the context of preventive or counseling services offered directly to the child; General Data Protection Regulation 2016 (EU), Recital 38), which could lead to excessive parental interference or even breach of children's right to privacy (Hof, 2016, p. 440) and to development: to provide informed consent, a parent should become aware of the child's online activities; to become aware, parents would need to monitor and track minors.

While it is recognized that the right to erasure is crucial, in cases where a child has given her consent, but later –when no longer a child– wishes to waive this consent and remove her data (General Data Protection Regulation 2016 (EU), Recital 65), however, the provision (General Data Protection Regulation 2016 (EU), Article 17) that reinforces the right to erasure makes no reference to children. So, exercising this right may not always be straightforward in practice (Blume, 2015, p. 262).

Although decisions based solely on automated processing should not concern a child (General Data Protection Regulation 2016 (EU),Recital 71), the "profiling article" (General Data Protection Regulation 2016 (EU), Article 22) mentions nothing in relation to the specifi protection that children merit. Additionally, even though the above children's rights and freedoms may override interests pursued by the controller and could, thus, render this processing unlawful (General Data Protection Regulation 2016 (EU), Article 6(1)(f)), how data controllers will undertake balancing tests in practice remains uncertain.

3. Parents' monitoring vs. minors' rights

Raising children with access to the Internet is a –relatively– new phenomenon. One could argue that children, who are not yet "in the maturity of their faculties" (Mill, 1859, 2001, p. 54), could or should be treated paternalistically. To some, parents are the most important guardians of children's welfare, as they are deeply concerned about the impact that technologies may have on minors (Kaiser Foundation, 2004, p. 12; Livingstone & Bober, 2006, p. 93). They would ensure that their children would "jump" into a swimming-pool only after having learnt how to swim (Byron, 2008, p. 107). Similarly, they would ensure that their children would not be harmed in the digital world.

Parental control is, to a large extent, necessary to direct children to adulthood. Some have described this parents-children relation as the "archetype of responsibility" (Jonas, 1984, p. 130). Children, when poorly monitored, may be more likely to express antisocial or criminal behavior (Stattin & Kerr, 2000, p. 1072) and parents' involvement could establish the rules necessary to facilitate communication (Stattin & Kerr, 2000, p. 1082). However, the active role and the participation of minors themselves should also be clearly acknowledged.

Early adolescence can be understood as a stage, in which teenagers strive for autonomy and self-determination, as a transition period to prepare for separation from parents, to become self-reliant. In this phase, minors tend to avoid parental control (Barron, 2014, p. 408) and they want the right to be ignored by those whom they see as being "in their business" (Boyd, 2014, p. 55). So, early teens not only disobey –to negotiate or alter– parents' rules (Fleming, 2005, p. 13) but also make decisions autonomously.

Autonomy, in the context of informational privacy, requires that individuals are "rational project pursuers" (Moore, 2003, p. 215) and choosers (Benn, 1980, p. 60) who steer their course through the world. To be a person, an individual must recognize not just her actual capacity but also her exclusive moral right to shape her destiny by her choices (Reiman, 1976, p. 39).

Although it could be claimed that teens lack this moral autonomy, which mainly refers to adults (Scarre, 1980, p. 123), albeit, children do not turn miraculously into grown up persons. They, thus, need to enjoy certain rights depending on the level of their maturity and the capacity to independently make reasoned choices. As emerging persons, they need to have the right to develop, to turn into autonomous agents. To do so, they need privacy; the ability to see themselves as autonomous, to learn that they are capable of controlling when and by whom the thoughts in their head will be experienced by someone other than themselves, and to learn that they are entitled to such control and that they will not be forced to reveal the contents of their consciousness even if they put such

contents on "paper" (Reiman, 1976, p. 43).
Intimacy is crucial in this context. To be friends or lovers, persons need to be intimate to some degree with each other. There is a need to share information about one's actions, beliefs or emotions that one does not share with everybody and that one has the right not to share with anyone; by granting this right, privacy creates "moral capital" that is "spent" in friendship and love (Gerstein, 1970, p. 89).
In the children-parents relation, the above means that the child should enjoy privacy to exercise the right to development and become intimate with her parents and with others. If a minor were completely disallowed to keep her own secrets or share secrets with those she would wish, she would not be able to create relationships or learn how friendship work and would not be able to develop.

4. A children-friendly interpretation of the GDPR

The GDPR's parental consent prerequisite supports a "paternalistic argument": Parents must protect children from harm as minors face risks online. Information about their online behavior is needed to protect them and, so, monitoring is good to get this information and necessary to give informed consent. Therefore, parents should monitor online activity.
Monitoring, however, as a paternalistic action, intends to remove or restrict the choice of a person (Clarke, 2002, p. 82). When it comes to children's privacy, it would be fair to argue that such practices should not always be acceptable.
Digital risks are in some cases overstated, while monitoring can be ineffective, as one cannot infer someone's beliefs from mere information. Namely, a minor may read a racist text but this does not always mean that she shares the author's views. Moreover, monitoring may harm in other cases, such as where unreasonably conservative parents would completely restrict their minor's freedom, if they found that he was gay. Besides, covert monitoring, if discovered, could undermine trust, while overt monitoring would be a clear message that the parents do not trust their child.
There is, it follows, a need for reciprocity, mutual respect and trust that would encourage minors to become media educated, instead of app monitored. Perhaps, parents and children should engage in democratic negotiations, share online activities, and talk more about the Internet. And, in our view, the GDPR does offer the provisions necessary to render minors beneficiaries of the data-driven reality. The principle of data protection by design and by default (General Data Protection Regulation 2016 (EU), Article 25) could oblige firms to introduce different default settings for children. Since firms should evaluate the risks inherent in data processing and implement measures to mitigate them (General Data

Protection Regulation 2016 (EU), Recital 83), a data protection impact assessment could be conducted (General Data Protection Regulation 2016 (EU), Article 35) when minors' data is processed. While children's data is not included in Recital 91 of the GDPR, however, it could be argued that, in light of Recital 38, carrying out the above assessment would be a good practice. Furthermore, supervisory authorities could very well perform their role as promoters of public awareness (General Data Protection Regulation 2016 (EU), Article 57) and, hence, encourage digital media literacy. Codes of Conduct (General Data Protection Regulation 2016 (EU), Article 40(2)(g)) could also be introduced to efficientl and effectively provide information and make clear how to "formulate" plain language (General Data Protection Regulation 2016 (EU), Article 12(1)).

Lawyers, data scientists, software designers, ethicists and others should all work together to make information understandable. This way, monitoring would very likely be mostly avoided, the use of tracking-applications would most probably be limited for exceptional situations (to serve goals of benevolence), and parents, when wondering whether their child is threatened by the e-world, would ask themselves questions asked in the emergence of an alleged "offline threat": "Does she study less? Did she quit her friends and activities? Has she become antisocial?" If the answer is "no", monitoring is probably unreasonable.

References

Article 29 Data Protection Working Party (2009). Opinion 2/2009 on the protection of children's personal data. Adopted on 11 February 2009.

Article 29 Data Protection Working Party (2010). Opinion 2/2010 on online behavioral advertising. Adopted on 22 June 2010.

Article 29 Data Protection Working Party (2013). Opinion 02/2013 on apps on smart devices. Adopted on 27 February 2013.

Barron, C. M. (2014). 'I had no credit to ring you back': Children's strategies of negotiation and resistance to parental surveillance via mobile phones. Surveillance & Society, 12(3), 401-413. DOI: 10.24908/ss.v12i3.4966

Benn, S. I. (1980). Privacy and respect for persons: A reply. *Australasian Journal of Philosophy,* 58(1), 54-61.

Blume, P. (2015). The Data Subject. *European Data Protection Law Review, 1(*4), 258-264.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. New Haven, London: Yale University Press.

Byron, T. (2008). *Byron Review – Children and New Technology.* Safer Children in a Digital World. The Report of the Byron Review. Nottingham, UK: The Department for Children, Schools and Families, and the Department for Culture, Media and Sport.

Clarke, S. (2002). A definition of paternalism. *Critical Review of International Social and Political Philosophy,* 5(1), 81-91.

Directive laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services 2015 (EU). Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data 1995 (EU). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Family Online Safety Institute (2011). *Who Needs Parental Controls? A Survey Of Awareness, Attitudes, And Use Of Online Parental Controls*. Findings From A National Survey Among Parents. Washington, NY: Hart Research Associates.

FAQs – 1TopSpy Cell Phone Spy App. (2014). Retrieved from http://www.1topspy.com/faq.html.

Fleming, M. (2005). Adolescent Autonomy: Desire, Achievement and Disobeying Parents between Early and Late Adolescence. *Australian Journal of Education and Developmental Psychology, 5, 1-16*.

Gabriels, K. (2016). 'I keep a close watch on this child of mine': A moral critique of other-tracking apps. *Ethics Information Technology, 18*, 175-184. DOI: 10.1007/s10676-016-9405-1

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

Gerstein, R. S. (1970). Privacy and Self-Incrimination. Ethics, 80(2), 87-101.

Gregg, M. (2013). Spouse-busting: Intimacy, adultery, and surveillance technology. *Surveillance & Society, 11*(3), 301-310. DOI: 10.24908/ss.v11i3.4514

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

Jonas, H. (1984). *The Imperative of Responsibility. In search of an ethics for the technological age.* Chicago: The University of Chicago Press.

Kaiser Foundation (2004). *Parents, media and public policy: A Kaiser Family Foundation Survey.* Washington DC: Kaiser Family Foundation

Kirwil, L. (2009). Parental Mediation of Children's Internet Use In Different European Countries. *Journal of Children and Media,* 3(4), 394-409. DOI: 10.1080/17482790903233440

Livingstone, S., & Bober, M. (2006). Regulating the internet at home: Contrasting the perspectives of children and parents. In D. Buckingham & R. Willett (eds), *Digital generations: children, young people and new media* (pp. 93-113). Mahwah, N.J.: Lawrence Erlbaum.

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

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society, 19*(5), 780-794. DOI: 10.1177/1461444816686328

Madison, R. (2014). Life360 *App aims to become leader in family network*. Retrieved from https://utahbusiness.com/

Mill, J. S. (1859, 2001). On Liberty. Kitchener, Ontario, Canada: Batoche Books.

Montgomery, C. K., & Chester, J. (2015). Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework. *European Data Protection Law Review, 1(*4), 277-291.

Moore, A. D. (2003). Privacy: Its Meaning and Value. *American Philosophical Quarterly*, 40(3), 215-227.

Palfrey, J., Sacco, D. T., & Boyd, D. (2008). *Enhancing Child Safety and Online Technologies: Final Report Of The Internet Safety Technical Task Force To The Multi-State Working Group On Social Networking Of State Attorneys General Of The United States*. Cambridge, MA: The Berkman Center for Internet & Society at Harvard University.

Pasquale, F. (2015). The Algorithmic Self. *The Hedgehog Review,* 17(1). Accessed at http://www.iasc-culture.org/THR/THR_article_2015_Spring_Pasquale.php.

Reiman, J. H. (1976). Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs, 6(*1), 26-44.

Scarre, G. (1980). Children and Paternalism. *Philosophy,* 55(211), 117-124.

Stattin, H., & Kerr, M. (2000). Parental Monitoring: A Reinterpretation. *Child Development,* 71(4), 1072–1085.

Swan, M. (2013). The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. *Big Data,* 1(2), 85-99. DOI: 10.1089/big.2012.0002.

United Nations Convention on the Rights of the Child 1989 (UN). UNCRC, United Nations (General Assembly). Convention on the Rights of the Child.