Philos. Technol. (2011) 24:411–418
DOI 10.1007/s13347-011-0034-7

SPECIAL ISSUE

Beware of the Virtual Doll: ISPs and the Protection of Personal Data of Minors

Daniel Nagel

Received: 11 March 2011 / Accepted: 30 May 2011 / Published online: 8 June 2011
© Springer-Verlag 2011

Abstract Once upon a time, they managed to bring Neverland into the bedrooms; they were seen as the heroes of a new era. However, as heroes always tend to walk a fine line between good and evil, it does not come as a surprise that a decade later the perception has dramatically changed; the fairy tale turned into a nightmare. Are Internet Service Providers (ISPs) no more than data-guzzling monsters that need to be tamed? In November, the European Commission published a "Comprehensive approach on personal data protection in the European Union" which seems to nod approval. The approach seeks to strengthen the individual's rights regarding the use of data by ISPs. The Commission notes that children deserve specific protection in this context due to the fact that their awareness of risks and consequences is usually underdeveloped. Both a general principle of transparent processing and specific obligations for data controllers regarding the type of information to be provided and the modalities for providing it had to be taken into account. Not only legal but also self-regulatory initiatives should contribute to a better enforcement of data protection rules. This approach is both applauded and heavily criticized by the European Data Protection Supervisor. In particular, he argues that children's particular interests have not been sufficiently addressed presenting a long list of suggestions for improvement including specific provisions against behavioral advertising, the exclusion of some data categories, an age threshold or special requirements on the issue of informed consent and a reinforcement of data controllers' accountability. Is there really a need for a new magic formula? This paper reviews the current options for addressing the challenges of the use of personal data of minors by ISPs.

Keywords Data protection · Information technologies · Rights of minors · Ethical liability of ISPs

D. Nagel (✉)
BRP Renaud & Partner, Königstrasse 28,
70173 Stuttgart, Germany
e-mail: Daniel.Nagel@brp.de
URL: www.brp.de

1 Introduction

The fact that internet services pose special challenges when the users are minors is not new. A 2007 survey noted that children appear to be extremely familiar with the internet. Learning to use the internet is, for them, almost "self-evident" (European Commission 2007). Hence, it might be seen as surprising that neither Directive 95/46/EC nor the recent Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions provides for a special regulation on the protection of data of minors. This is even more surprising when current figures of internet usage are taken into account. If recent statistics can be trusted, more than 75% of the population of North America and more than half of the population of Europe use the internet.[1] As these numbers even consider people that are not yet or are no longer capable of using internet devices, it is obvious that there are huge numbers of minors online. This is confirmed by many surveys which show that a vast majority of minors have access to the internet at home, mostly through broadband connections or via mobile phones. The times when the internet was a purely adult domain—in terms of a predominant scientific content—have long passed. Minors are said to use the internet regularly and frequently.[2] This increase in use is heavily influenced by the developments and innovations of the so-called digital age which led to a supply of an incredibly vast variety of internet services. Social networks play an increasingly important role, e.g., about half of U.S. teens used Facebook in 2009 (Nielsen 2009). Nevertheless, other services are also able to record regular use by minors.[3]

The Communication of the Commission makes it clear that the Commission sees a need for improving the current standards of data protection. Nevertheless, its approach leaves many back doors open and does not provide for specific measures that the specific rights of minors to be enforced in practice. However, as the internet heavily influences social behavior and the future development of children there is a need to fill this gap both from a pedagogic and a legal point of view. Internet Service Providers (ISPs) will have to carry a part of this burden by equipping themselves with a shareable and sustainable information ethics.

2 The Current Data Protection Framework

Within Europe, the protection of personal data is mainly based on 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. This directive represented a milestone in the quest for achieving a harmonized protection of personal data that does not halt at national borders. Thus, for the first time there was a uniform approach in addressing the issue of a movement of data that could no longer be kept within national boundaries due

[1] Cf. http://www.internetworldstats.com/stats.htm
[2] Ibid.
[3] Google is still among the most frequently used services by children (Nielsen 2009).

to technological developments such as, in particular, the possibility to communicate and transfer information electronically.

In addition, Directive 95/46/EC represented a landmark for data protection activists in many European Member States where the issue had been dealt with rather reluctantly so far. Despite the fact that the Commission chose the form of a directive which meant that it did not take immediate direct effect in the EU15, the wording did not leave much room for deviation in the implementing legislation adopted by the Member States and thereby provided for a certain level of protection in all of the Member States.[4] The directive highlighted that "whereas data-processing systems are designed to serve man; whereas they must whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals."

Thus, the protection of the right to privacy was put at the heart of the directive. This was also emphasized within the introductory remarks of the directive as regards the relationship between data subjects and data controllers. The Commission noted that if the controller failed to respect the rights of data subjects, national legislation had to provide for a judicial remedy. In addition, any damage which a person might suffer as a result of unlawful processing must be compensated for by the controller. The latter only allows for an exception if the controller is able to prove that he/she is not responsible for the damage. The burden of proof, hence, lies with the controller. To put it in other words, the controller is automatically deemed liable unless he/she is able to show that the liability lies with the data subject or that there is a case of force majeure, which puts the data subject at a procedural advantage.

The articles of the directive contain a clear guidance on the treatment of personal data. Article 6 of the directive provides for a fair and lawful processing of data and Article 7 of the directive enshrines the principle of the necessity of a prior consent of the data subject to any collection, storage, or use of data. Only very exceptional and enumerated cases allow for a processing without the explicit consent of the data subject. These exceptions have in common that they contain the necessity to show a legitimate justification for not having the data subject explicitly agree thereto.

The directive does not differentiate between adults and minors. The same level of protection is applied irrespective of the age of the data subject. The challenge posed by the fact that children may not be able to understand the consequences of a disclosure of personal data and thus to declare an informed consent is addressed in most Member States via the regulation on the capacity to contract. Apart from that, the law does not allow for a two-tiered approach. This might be seen as surprising as it is not unusual for the directive to employ a double standard; the directive acknowledges that sensitive data calls for a special protection. Article 8 of the directive explicitly provides that Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Most components of this special category are the

[4] As they were obliged to comply with its objective, cf. Art.32: "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption."

result of securing the full effectiveness of fundamental rights such as the freedom of worship or the freedom of speech. There is no reason why the data of minors who are not yet capable of coming to an informed opinion should not constitute a category that needs special protection, too. However, the Commission obviously was convinced that there is no need for a special protection.

Nevertheless, the current level of protection in conjunction with the application of the respective national rules on the capacity to contract offer at least a general basic protection: personal data of minors cannot be deliberately collected and the data subject or his or her legal guardian has the right to object to data processing or to request that the information is rectified, erased, or blocked.

3 The New *Approach* by the Commission

Arguably, Directive 95/46/EC has some serious flaws which call for improvement,[5] and—despite its young age—it can already be seen as a relic of the early days of the information age. Fortunately, this has not gone unnoticed. The Commission notes that the rapid technological developments and globalization have profoundly changed the world around us and brought new challenges for the protection of personal data (European Commission 2010). The technological development of the means to collect, store, and process data entails the necessity to not only rethink the concept of privacy or the definition of personal data in general but also to establish a comprehensive approach that is able to adapt to and embrace a new gamut of data that might evolve in the near future. The call for the establishment of a habeas data is hence not surprising (EGE 2005),[6] as only a clear concept eliminates insecurities on both the side of the data subject and the side of data processors.

The Commission requests, in its new approach, that data subjects are well and clearly informed in a transparent way via introducing a general principle of transparent processing. The information should be easily accessible and easy to understand. The Commission argues that this specifically applied to children. Apart from that, the concept does not name any specific additional measures for the protection of children.

This is heavily criticized by the European Data Protection Supervisor (European Data Protection Supervisor 2011). The need for a specific protection of children in specific circumstances because of their vulnerability and in order to prevent legal uncertainty had not been recognized by the Commission. The EDPS suggests additional provisions specifically addressed to the collection and further processing of children's data. These provisions should include an improvement and adaptation of information requirements, a specific protection against behavioral advertising, a strong purpose limitation as regards children's data, the prohibition of the collection of certain categories of data, the introduction of an age threshold, and the establishment of rules on how to authenticate the age of a data subject.

[5] For example, the differences in the interpretation of personal data in the relationship EU–US, the lack of uniformity in interpreting cross-border issues or the fact that there is a weak second level protection (i.e., as soon as a data subject has been tricked into consenting once he literally loses control over his data)

[6] Or the ownership-based interpretation of informational privacy by Luciano Floridi (Floridi 2005)

Furthermore, the general form of the new approach is seen as crucial; the approach currently provides for the introduction of a new directive. The choice of this very legal instrument allows for deviating interpretations by Member States. Even though this might be caused by an attempt to find a compromise between differing perceptions of certain aspects of the approach, it, at the same time, weakens its possible impact and thus the political message.

Thus, it is clear that the Communication does not improve the legal protection of privacy rights of minors. While the form of protection is debatable, it is clear that there is a regulatory vacuum that needs to be filled in some way in order to overcome uncertainty and in order to find a sustainable approach for the treatment of data of minors.

4 Is There a Need for a Higher Level of Protection

If the current framework and the new approach of the Commission are compared to the opinion of the European Data Protection Supervisor, the impression can be gained that there is a need to improve the level of protection as regards the protection of personal data of minors by introducing new legal standards. However, it can be doubted whether such an improvement should and can be achieved from a purely legal starting point. The use of internet services by minors is not only a sign that children quickly adapt to technological innovations and thus will be able to further developments in the future but also entails challenges that have to be taken seriously. Any measure, hence, has to take the ambivalent nature of the use of internet services by children into account. In other words, it has to be considered that the use of internet services by children is a double-edged sword. On the one hand, it offers many possibilities that past generations were denied access to. A minor is able to connect with friends and relatives that live far away at any time, to share and exchange thoughts with a peer group a hundred times the size of his grandfather's and access more information than ever. The mere presence of a computer with an internet connection turns a children's room into a library that easily dwarfs the information available in local libraries. On the other hand, these possibilities also entail a lot of challenges and risks. Children are able to access unfiltered information on any subject. This induced some commentators to make sinister predictions reaching from less serious social implications to a loss of youth (Cheon 2005; Anderson et al. 2003). In addition, there is also a spin-off on the passive side: if a minor uses internet services they will use the minor—the use of internet services often includes a collection of details such as names, addresses, gender, ethnicity, language, special needs or interests, date of birth, and telephone numbers. These details have a measurable economic value and are thus very likely to be shared, sold, or stored by many actors. Such "passive" processing of personal data in turn not only influences the present lives of children, e.g., via behavioral advertising, but also their future lives as the internet does not forget.[7] Thus, any data that has ever been collected might be accessed some time in the future by somebody with an interest

[7] Which still stirs up a lot of dust cf., e.g., the discussion on a right to forget (Goméz 2011; Nagel and Weimann 2011)

that might not have been present at the time of the collection.[8] In addition, children can be influenced more easily. Neuroscientists and educationalists taught us that thought patterns of an adult to which new information is compared and against which its content is weighed are far more distinctive and developed than patterns of a child (Gardener 1983). Finally, the use of internet services by minors also carries imminent dangers from a criminal perspective. Technological possibilities such as automated data linkage, e.g., the name, age, and gender to domicile via a Google maps application, exposes minors to risks that usually have not been thought of when the service was made available.

It is hardly possible to counter all these different challenges legally without creating an impediment to the beneficial use of internet services. In addition, such legislation might also influence fields not intended by the legislator as, e.g., from a legal perspective the verification of the fact whether a data subject is a minor either includes data collection or profiling or is hardly possible without limiting access for adults as well.[9] Furthermore, any increase in protection is a push on a slippery slope to a nanny state and thus might finally even curtail fundamental rights such as the freedom of speech or the freedom of information.[10]

Hence, it can be argued that while the suggestions of the European Data Protection Supervisor look good on paper, it is questionable whether they can be realized in practice via a legal instrument. On the other hand, there is no necessity to find a purely legal solution. Firstly, there already is a basic level of legal protection for personal data of minors. Secondly, the power of national legislation stops at political borders, whereas the internet does not. Hence, a flexible and uniform approach by ISPs might be better tailored to address many challenges arising out of the use of internet services by junior surfers.

5 Future Challenges

Notwithstanding this criticism as regards the proposed means of implementing new measures to achieve a better protection of personal data of minors, an important lesson can be learned from the suggestions of the European Data Protection Supervisor: any new data protection approach—irrespective of its form—needs to consider the specific challenges that arise out of the use of internet services by children. The approach needs to consider that data subjects and in particular underage data subjects need to be comprehensively informed about the collection of data and their rights in a transparent and clear way. The mere presence of the right to informational self-determination under Directive 95/46/EC does not automatically

[8] Cf., e.g., the strong tendency of employers to browse social networks for additional information on applicants

[9] Cf., however, in this respect, the research on nonintrusive technological developments to identify minors online which might even overcome the vicious circle of specific data protection without prior data collection in the near future (such privacy enhancing technologies have been and still are the focus of research of various projects, e.g., the Privacy and Identity Management for Europe project PRIME)

[10] Cf., e.g., the fate of the Child Online Protection Act (1998) in the US which was finally "declared" unconstitutional on the basis of these very issues as the Supreme Court refused to hear the US Government's last appeal against respective lower court rulings in 2009

include a conclusive public awareness thereof (Lodge 2010). This is all the more true when minors are involved. Hence, it is important to ensure that underage data subjects are taken by the hand and not only led through the glitter world of internet services but also through the jungle of data collection. In this context, it might even be considered that ISPs could implement preventative measures.[11]

Furthermore, there needs to be some sort of protection from behavioral advertising when the data subject is underage. It is true that it is not easy to guess the age of an internet user if no data is entered. However, automated monitoring and profiling systems that are used for behavioral advertising could be programmed to not function when the profiling leads to the assumption that the user might be a minor.[12]

Finally, ISPs could establish codes of conduct on using children's data when it is obvious to them that the data of minors are involved. This could include the automatic deletion of certain categories of data or the implementation of an impact assessment test before transferring that data to third parties. Such codes could also consider the issue whether an age threshold can be used to improve the online security of children and how it could best be implemented.

In addition to these suggestions from the legal sphere, there is the need to also consider the use of the internet by children from other perspectives.[13] Only a multidisciplinary approach will be able to provide a sustainable guideline. It is true that ISPs cannot fill the gap left by a lack of supervision or education on their own. They can, however, support educational or other measures to lighten the load caused by complex technological innovations. There are, e.g., fascinating pilot schemes underway which combine educational theories and internet services.[14] The time to further such processes is now.

Thus, there is no need for a new magic formula. However, the grimoire where it can be found in needs some dusting and a hero of the new era to (re)open it.

References

Anderson, C.A., Berkowitz, L., Donnerstein, E., Huesmann, L.R., Johnson, J.D., Malamuth, D.L.N.M., Wartella, E. (2003). The influence of media violence on youth, *Psychological Science in the public interest*, *4*(3), 81–110.

Cheon, H. J. (2005). Children's exposure to negative internet content: effects of family context. *Journal of Broadcasting & Electronic Media, 49*, 488–509.

European Commission. (2007). *Safer internet for children. Qualitative Study in 29 European Countries, Summary Report May 2007*. France: Eurobarometer.

[11] Such as, e.g., the automatic full selection of all protective "privacy options" within social networks if the birth date indicates that the user is not an adult; in addition, current schemes as, e.g., the Google Family Safety Center which enables users to have pages filtered, could be extended to include data collection-sensitive filters

[12] For example, if the user shows a high interest in certain online games or videos that are usually accessed by children

[13] For example, from a pedagogic perspective: Should children be addressees and recipients of digital communication at all, and if so, to which extent?

[14] Cf., e.g., the pilot scheme "schoolbook" which is about to start at some German schools and mirrors internet services (such as social networks) on a closed platform where it is possible for teachers and pupils to interact and for the "internet" to forget

European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—a comprehensive approach on personal data protection in the European Union*. Brussels: COM.

European Data Protection Supervisor (2011) Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—a comprehensive approach on personal data protection in the European Union. Brussels: European Data Protection Supervisor.

European Group on Ethics in Science and New Technologies (EGE). (2005). *Ethical aspects of ICT implants in the human body: opinion presented to the Commission by the European Group on Ethics*. Brussels: European Commission.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology, 7*, 185–200.

Gardener, H. (1983). *Frames of mind: the theory of multiple intelligences*. New York: Basic Books.

Gómez, R. G. (2011). *Quiero que Internet se olvide de mì*. Madrid: El País.

Lodge, J. (2010). *Quantum surveillance and 'shared secrets': a biometric step too far?* Brussels: CEPS Liberty and Security in Europe.

Nagel, D. & Weimann, T. (2011) Streit um das Recht auf digitales Vergessen, Legal Tribune Online, 9 May.

Nielsen. (2009). *How teens use Media. A Nielsen report on the myths and realities of teen media trends*. New York: The Nielsen Company.

The European Parliament and the Council of the European Union. (1995). 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. *Official Journal L, 281*, 0031–0050.