CHILDREN AND DATA PROTECTION FROM THE PERSPECTIVE OF CHILDREN'S RIGHTS - SOME DIFFICULT DILEMMAS UNDER THE GENERAL DATA PROTECTION REGULATION

Thorbeckecolleges

Voordrachten gehouden in het kader van de uitwisseling tussen
de juridische faculteiten te Gent en te Leiden

Faculteit Rechtsgeleerdheid
Rijksuniversiteit Leiden

Thorbeckecollege 43

Children and data protection from the perspective of children's rights - Some difficult dilemmas under the General Data Protection Regulation

Voordracht gehouden aan de Universiteit te Leiden
Faculteit Rechtsgeleerdheid
op 20 april 2018

door

Prof. Simone van der Hof

Hoogleraar Recht en de Informatiemaatschappij, Centrum voor Recht en Digitale Technologie, Universiteit Leiden

Verantwoordelijke uitgever: Paul De Ridder

Ragheno Business Park
Motstraat 30
2800 Mechelen

Klantenservice:
Motstraat 30
2800 Mechelen
Tel.: 015 78 76 00
klant.BE@wolterskluwer.com
www.wolterskluwer.be

D/2018/2664/457
ISBN: 978-94-03-00581-2
BP/GANDTOR-BI18001

TABLE OF CONTENTS

1. Introduction

Assume you have 5-year-old daughter who is playing football with a friend on a nearby playground. Around them is a group of people who write down in a notebook what the children do — Do they play with each other? Whom else do they play with? Are they talented football players? Are they interested in other games? These people are always there, nobody knows who they are and what information they collect and for what purposes. Would you as a parent be happy with this situation? Of course not. And yet in the digital world, the constant monitoring, measurement and analysis of the behaviour of children is the norm. And not only of children, of course. The recent Facebook/Cambridge Analytica scandal[1] has made two things very clear. First, it bears witness to the enormous economic, social and political value of our personal data. Secondly, the scandal shows how intrusively our mind is manipulated with the help of behavioural marketing to nudge us into spending money — even when we do not need anything — and how through micro-targeting our vote can be pushed in a certain direction.

However, we must realise very well that this scandal is not just about Facebook and Cambridge Analytica. What is called surveillance capitalism[2] is the basis of almost all apps and online services that we use on our computers, tablets and smartphones. Based on the use of our smartphones, our lives can be mapped in great detail: where we live, work, who our friends, family and children are, who

1. Facebook fined for data breaches in Cambridge Analytica scandal, The Guardia, 11 July 2018, https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal (last visited 23 July 2018).
2. S. Zuboff, Big other: surveillance capitalism and the prospects of an information civilization, J Inf Technol (2015) 30: 75. https://doi.org/10.1057/jit.2015.5.

our partner or lover is, our day-to-day activities and even our medical condition and sexual preferences remain no secret. Google knows what we think when we use their search engine. Thousands of so-called data traders make billions of dollars of off our data and hence our identities — which might lead to comparisons with slavery.[3] And some of my students presenting on the economic exploitation of children in class pointed at a new form of child labour by calling children "facebook workers".[4]

Applications of artificial intelligence and big data analytics are becoming more and more sophisticated in analysing data and a combination of these developments increasingly influences the lives of individuals ever more radically. It is crucial that there are sufficient effective safeguards that optimally protect the rights and freedoms of individuals in a datafied digital world. Children should not be forgotten, because their lives are already imbued with digital technology from birth. In Belgium[5] and The Netherlands[6] a vast majority of children are online daily and their data is collected, used and shared by toys, baby surveillance cameras, games, children's e-books, digital learning systems, social media and video-sharing apps and so on and so forth.

If we actually want to protect the privacy and more specifically the personal data of children in a datafied digital world then it is necessary to take a holistic perspective in

3. A. Balkan, Wir alle sind Cyborgs, Zeit Online, 7 March 2016, https://www.zeit.de/digital/mobil/2016-03/digitalisierung-big-data-soziale-netzwerke-ueberwachung-umgang-digital-denken (last visited 23 July 2018).
4. In the combined course on Digital Child Rights for the advanced masters programmes Law and Digital Technologies and International Children's Rights at Leiden Law School (class 2017-2018).
5. Apestaartjaren, De digitale wereld van kinderen en jongeren, Mediaraven, Mediawijs, IMEC-MICT Universiteit Gent, mei 2018.
6. Monitor Jeugd en Media 2017, Kennisnet, 2017.

the development and implementation of regulations that aim to achieve such protection. A holistic perspective, moreover, that must incorporate different dimensions. I will briefly explain what I mean by this.

One dimension essentially starts from a more general children's rights approach, factoring in all relevant children's rights and adequately balancing protection and freedom children. The aim is to achieve adequate protection of children without unduly impacting their freedom rights, the outcome of which may differ depending on the age and maturity of children.

The *second dimension* is more specific and domain related and pertains to the data protection framework promulgated by the General Data Protection Regulation (hereafter GPDR) which has entered into force on 25 May 2018.[7] An innovative element in the GDPR is that it incorporates special attention for the protection of children and their personal data.[8] The protection offered by the GDPR is an important step forward in the datafied digital world, but such augmented protection means that we must not merely focus on the provisions in which the interests of children are in so many words addressed but take into account the large set of rights and responsibilities of the GDPR — if you process personal data of children than you have to exercise extra care regardless of whether children are explicitly mentioned.[9] This is both in the spirit

7. Regulation (EU) 2016/679 of the European Parliament and 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) OJ L 119/1, 4.5. 2016.
8. See Recital 38, GDPR.
9. Van der Hof, S., Lievens, L. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR, Communications Law, Vol. 3, No. 1 2018.

of the GDPR and the interest of the child as laid down in Article 3[10] of the UN Convention on the Rights of the Child (hereafter UN CRC),[11] one one of the fundamental principles guiding the interpretation of any other measure that impacts children, including the GDPR.

I will come back to both these dimensions later on in this book, essentially arguing that the GDPR can be problematic from a children's rights perspective and how a more integrated data protection strategy can mitigate or prevent some of the negative effects of datafication. First, however, let's dive into the world of data in order to set the scene for any further deliberations.

2. Datafication[12]

The developments I have sketched in my introduction are part and parcel of a phenomenon called datafication which has been described by Austrian scholar Mayer-Schönberger and American author Cukier in their book Big Data as turning a social phenomenon such as online behaviour into a quantified format which can be recorded and analysed. But what kind of data do we mean when speaking of a datafied world.[13] The key notion that triggers

10. Subsection 1 reads as follows: "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration." See also Comm. on the Rights of the Child, General Comment no. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (art. 3, para. 1), 32, U.N. Doc. CRC/C/GC/14 (May 29, 2013).
11. Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with article 49.
12. This section is based on: Van der Hof, S. I agree or do I? A rights-based analysis of the law on children's consent in the digital world, 34 Wis. Int'l L.J. 409 2017.
13. Mayer-Schönberger, V., Cukier, K. *Big data: A revolution that will transform how we live, work, and think.* Boston: Houghton Mifflin Harcourt 2013.

the protection of the GDPR is 'personal data', which means "any information relating to an identified or identifiable natural person".[14] But the picture of datafication becomes clearer when we categorise data according to the interests of data companies and internet platforms. To gain more insight into this, it is useful to distinguish between three types of data.[15]

First, there is the data that we provide or publish ourselves — or what can be called data given. These include personal details such as name and e-mail address that we need to submit when opening an account on social media and content such as personal status and interests, messages and pictures that we post on our online social media profiles. We may actually make conscious choices, and many people probably do, when sharing such data, for example to develop a certain kind of identity or because we do not want to disclose intimate personal information.

Ironically, however, this is not the kind of data that necessarily interests data companies most. Rather they seem keener on the second type of data, which is data given off or more often referred to as metadata. Data companies collect what is called behavioural data. Behavioural data are the data crumbs that we, as a modern Hansel and Gretel, scatter through the digital world and are being picked up, stored and processed by websites, apps and data traders. Metadata makes us perfectly identifiable; the way we use a browser or smartphone is unique for each person. The Washington Post revealed that more than 50% of Google Play Store apps offered in the Designed

14. See Article 4 (1) GDPR.
15. See Van der Hof (2017), *supra*.

for family's section targeted children under 13, sending such potential sensitive data given off, including device serial numbers (which allow continues tracking), location data, contact information to third party advertisers and data analytics companies.[16]

This brings me to the third category of data, which are the inferred data or inferred knowledge is actually a more striking term. The first two categories of data — the data given and the data given off — are the raw materials for manufacturing this type of knowledge. This is what is also called Big Data[17]. Data given and data given off are crunched by algorithms to find patterns and correlations that allow to make predictions about people. Remarkably, data that seems trivial at face value can potentially reveal very sensitive information about a person as a 2013 study demonstrates — personality, gender, sexual orientation, political orientation and ethnic origin can be predicted with high accuracy from someone's Facebook likes even if such Likes do not in and of themselves reveal that information.[18] Intimate information that we are not likely to consciously share on social media can nonetheless be inferred from the digital footprints that we leave behind in the datafied digital world and turned into profiles that paint us a certain type of person we according to the system are likely to be. Inferred data are not necessarily presenting the truth, given that they are based on

16. We tested apps for children. Half failed to protect their data, July 2018, https://www.washingtonpost.com/news/the-switch/wp/2017/07/27/we-tested-apps-for-children-half-failed-to-protect-their-data/ (last visited 23 July 2018).
17. Gandomi, A., Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2014.10.007.
18. M Kosinski, D Stillwell, T Graepel, Private traits and Attributes are Predictable from Digital Records of Human Behaviour, Proceedings of the Nat'l Acad. of Sci. of the U.S., Vol. 110, No. 15, 5802–5805 (2013).

correlations, not causation.[19] Inferred data are what Mayer-Schönberger and Cukier mean by datafication, this is the type of knowledge that is central to the Facebook/Cambridge Analytica scandal and these are the datafication processes that are completely invisible[20] to us.

3. The GDPR and protection of children

In a datafied world it is important that adequate safeguards are in place to protect individuals and society as a whole against negative effects, such as incorrect data or profiling errors, as well as against unjustified or harmful exclusion and discrimination of people.[21] These guarantees are necessary to keep a grip on your life. You may not have anything to hide but it is no one's business to know that as a quote on one of Loesjes poster aptly states.[22] And of course we all have many things to hide; intimate or embarrassing or just private things we share with some but not others or keep entirely to ourselves.[23] It is called being human. And even if you have something to hide, it does not mean that we can simply set aside citizen's rights.

The GDPR aims to provide such safeguards by defining individual rights and data processing responsibilities and providing adequate tools to enforce these safeguards

19. Hildebrandt, M. (2013). Slaves to Big Data. Or Are We? *IDP Revista de Internet Derecho y Política*. https://doi.org/10.7238/idp.v0i17.1977.
20. Also called black boxes by Frank Pasquale in his book The Black Box Society, Harvard University Press, 2015.
21. Schermer, B.W., Risks of Profiling and the Limits of Data Protection Law, in: Custers, B., Calders T., Schermer, B. Zarsky, T., Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases (Studies in Applied Philosophy, Epistemology and Rational Ethics), Springer, 2013.
22. See https://www.loesje.nl/posters/nl1210_0/ (in Dutch); for more information on Loesje http://www.loesje.org (both last visited 23 July 2018). Loesje
23. See also Martijn, M., Tokmetzis, D., Je hebt wél iets te verbergen, Over het levensbelang van privacy, De Correspondent, 2016.

which are based on general data protection principles[24]. Although the data protection framework is basically a continuation of principles and partly also rules that have already been in place since the mid-1990s, there are a number of important changes, even regulatory innovations. One of those changes is the specific focus on the protection of children's personal data.

Children are entitled to specific protection with regard to their personal data, as they are probably less aware of the risks, consequences and safeguards involved and of their rights with regard to the processing of personal data, as stated by recital 38 of the GDPR. This specific protection is particularly relevant when children's personal data are used for marketing purposes or for the preparation of personality or user profiles — which falls in my third category of data, namely that of inferred data. But also, when services are directly provided to children.[25] Many digital services therefore fall directly into one or more of the most worrying categories and amongst them many that are being used by children, such as Snapchat, Instagram, WhatsApp, YouTube and so on. By the way, the GDPR does not define what a 'child' is which might seem like an important issue if you wish to single out this group for special treatment. But it leaves room to make the case for adopting the most accepted definition in the UN CRC. Hence, I would argue that under the GDRP a child is a person under 18.[26]

The GDPR has incorporated several child protection mechanisms, but the most important and, at the same time, most controversial is the requirement of parental

24. See article 5, GDPR for the data protection principles.
25. All: recital 38, GDPR.
26. See also Van der Hof, Lievens (2017) *supra*.

consent for commercial online services. I will briefly explain first what the provision entails and then why it is problematic.

Article 8 of the GDPR[27] which regulates the age of digital consent stipulates that children can consent to the processing of their personal data by commercial online services from the age of 16. Below the age of 16 parental consent is required. In principle, because member states can tweak the age of digital consent by lowering it to anywhere between 16 and 13. As a result a patchwork of different ages of digital consent is now emerging across the European Union which is particularly unfortunate for data companies that need to comply with the provision.[28]

The provision has already given rise to quite a number of questions even well before the GDPR entering into force,[29] the answer to which seem to be emerging slowly

27. Article 8 (Conditions applicable to child's consent in relation to information society services) reads as follows:
"1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child."
28. Milkaite, I., Lievens, E., GDPR: updated state of play of the age of consent across the EU, June 2018, https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751 (last visited 23 July 2018).
29. See e.g. Better Internet for Kids, The General Data Protection Regulation and Children's Rights: questions and answers for legislators, DPAs, Industry, Education, Stakeholders and Civil Society, Roundtable report, European Schoolnet, Ghent University, KU Leuven, EU Commission, Brussels: 23 June 2017, https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2018677 (last visited 23 July 2018).

but surely. For instance, online commercial services must be offered directly to a child. What does that mean? Must services be accessible to children, used by them or even popular among children? It seems that services evidently offered to 18 and older are excluded. The provision also requires verification of age and parental consent — but when is verification adequate? It seems clear that depending on the risk involved more security may be necessary and just providing a birth date as is now required on many social media platforms will not be sufficient verification.[30]

Although the provision — despite its ambiguities — initially sounds rather straightforward, it might, however, be highly problematic given that it has the potential to negatively impact children's rights. To explain this further I will shift the perspective to the rights-based approach.

4. The impact on children's rights

First a very brief introduction into the rights-based approach under the UN CRC. The UN CRC is not a mere a catalogue of rights but takes a holistic approach towards children's rights by recognising and merging three dimensions.[31] First, children are recognised as human beings in development with special needs. Children must be supported in protecting their rights, particularly against harm. E.g. right to protection against physical and mental violence.[32] Second, emancipation & participation perspective demands that we respect children's rights and

30. Article 29 Working Party, data protection working party, Guidelines on Consent under Regulation 2016/679, WP259, 29 november 2017, p. 24.
31. Lansdown, G., The Evolving Capacities of the Child, UNICEF Innocenti Research Centre, 3 (2005), http://unicef-irc.org/publications/pdf/evolving-eng.pdf.
32. See e.g. articles 19 and 34, UN CRC.

freedoms in order to encourage them to participate in society and grow into mature and independent citizens. E.g. privacy[33], freedom of information and expression[34], play[35], association[36], right to be heard[37]. Third, the perspective of development requires fulfilling children's rights by providing them with the means to optimally develop themselves and support physical, social and emotional well-being of children (right to education[38]). Adequately uniting these three perspectives is a great challenge and one that the GDPR has not been able to live up to entirely with the age of digital consent. What is more, each of these perspectives is problematic in situations in which the GDPR leaves the protection of the personal data of children up to the discretion of the parent. I will show you what I mean by focusing on each of these perspectives respectively.

A. Protection

The GDPR aims to protect children's specifically and this is an important improvement in the European data protection framework. However, the protection seems fragmented and mostly to be found in the requirement of parental consent. The basic idea behind the notion of consent is that we are in control over the processing of our personal data. Control then essentially means that we are in the driving seat when deciding on who can have and use our personal data for specific purposes. The notion of

33. Article 16, UN CRC; see also articles 7, 8 and 24, Charter of Fundamental Rights of the European Union, OJ C 364/01, 18.12.2000.
34. Articles 13 and 17, UN CRC.
35. Article 31, UN CRC.
36. Article 15, UN CRC.
37. Article 12, UN CRC.
38. Articles 28 and 29, UN CRC.

control pertains to the right to informational self-determination[39], which although not recognised as a right in and of itself has nonetheless greatly influenced data protection laws in Europe.[40] Unless data protection law offers another lawful ground for processing, consent — given the requirements for consent are met — transforms an in itself unlawful activity into a lawful one.[41]

However wonderful it sounds to be in control over the processing of your personal data, if the recent Facebook/ Cambridge Analytica has hopefully once and for all made one thing very clear is that being in control in the datafied digital world is an illusion and being given the capacity by law to say 'yes' or 'no' does not change that one bit in the current state of affairs. We cannot be part of the datafied digital world, at least not when surveillance capitalism is the dominant business model, and stay in control over our personal data.[42] This basically means that if children subscribe to apps and online services that are built on the model of surveillance capitalism, datafication will be an inherent part of the deal and there is not much anyone, including parents and children themselves, can do about it.

What is more, many people seem to perceive control as making conscious choices about the data they publish online, i.e. my first category of data — data given — but are not or less aware of the data collection and use behind the

39. Originally formulated by the Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 65 BVERFGE 1, 2008 (Ger.) (Population Census case).
40. Kosta, E. Consent in European data protection law. Dissertation KU Leuven, Martinus Nijhoff Publishers 2013.
41. Schermer, B.W., Custers, B., Van der Hof, S. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. Ethics Inf Technol (2014) 16:171–182.
42. Van der Hof (2017), *supra*; Van der Hof, Lievens (2017), *supra*.

screen, i.e. both other categories of data — data given off and inferred data — nor are they aware how intrusive data practices may impact individual lives. Such practices are seldom or not at all disclosed in privacy policies and to be sure online services may not even be aware themselves of the practices by third party trackers in their apps or on their websites. In conclusion: parental consent is not likely to lead to improved protection of children's personal data, given that consent does not actually give us control over our personal data in the datafied digital world and parents may very well lack awareness about the risks and consequences as well.[43]

B. Participation and emancipation

We will now turn our attention to the second perspective of the UN CRC: participation and emancipation. And I will start by showing you some quotes of children. They are the result of a recent Dutch study amongst teens:[44]

If I have to get permission from my parents, I'm going to lie that I'm 16 years old, because it harms my privacy! (Cas, 11)

Teach, are you kidding? 16 years old? What kind of lawmaker is that? Don't they understand we really need our privacy?! (student from Rotterdam, 14)

If you have to ask your parents for permission in every case, you don't have a private life anymore. And it's also discrimination (which is forbidden in Holland!) if your parents don't give permission and other parents do give another kid their permission. (Lieke, 11)

43. Van der Hof (2017), *supra;* see also Schermer, Custers, Van der Hof (2014), *supra*.
44. Kwantes, E., Experts v.s. youth & more findings, Report for ECP/SIC Netherlands, 15 December 2017 (on file with the author); see also https://www.youtube.com/watch?v=di3o4ez_wXY (in Dutch) (last visited 23 July 2018).

My private life will be harmed, because I would have to ask everything to my parents, and will not have the possibility to explore and search for myself. (Jens, 11)

Need I say more. These children clearly perceive parental consent as parental surveillance. And note that most of them are 11 years old, which is still under the minimum age of digital age of consent of 13 in article 8 of the GDPR. Part of participation and emancipation, especially when children grow older, is having your own spaces where parents are absent. These spaces can be bed rooms, public spaces where children hang out, being at one's friend's house, but increasingly also include online spaces, such social media, messenger apps, gaming environments and other online communities. Children and especially teens do not necessarily want their parents to know what their favourite digital hangouts are — or at least not each and every one of them. There may also be very particular circumstances in which they want explore the internet without parental supervision, for instance when looking for sensitive information related to sexual orientation and sexuality more generally or finding like-minded people when you are in a situation that is socially or emotionally challenging. That is not to say though that children do not recognise the importance of parental advice when you do want it, as these quotes from the same study[45] show:

The parental consent will make sure your parents know if something is (going) wrong, and they can help you out. 12 is old enough though. (Bram, 11)

Because your parents have to give their consent, I will be better cared of by them. (Gitte, 11)

45. Kwantes (201), *supra*.

Ideally, however, parental guidance should not be dependent on a legal requirement of parental consent; rather parents need to be involved irrespective of laws.[46]

Besides the need for privacy from parents, article 8, GDPR may also impact on their participation and emancipation rights in other ways. Children under the age of digital consent are not allowed on online platforms so these companies do not have to comply with age verification and parental consent requirements. In theory that is because in practice most online platforms do not actually check the age of their users. As a result, children under the age of digital consent can be avid users, but are not recognised as children. Of course, this can lead to safety because their protections rights are not adequately observed. These platforms do not have an incentive to take these children into account, for example by taking protective measures tailored to them, because they violate the general conditions and should not be there in the first place. Norwegian scholar Elisabeth Staksrud very strikingly speaks of children as illegal digital aliens.[47]

However, there is also a participation issue here because as soon as the platform discovers that you have lied about your age, your account and thus all your content will be mercilessly removed.[48] Basically, hours of hard work in creating music videos on Musical.ly or vlogs on YouTube can go up in thin air just like that. But suppose platform

46. See also articles 5 and 18, UN CRC.
47. Staksrud, E. Children in the Online World, Risks, Regulation and Rights, Ashgate, 2013, p.156.
48. See, for instance, Facebook and Instagram change to crack down on underage children, Techcrunch, 19 July 2018, https://techcrunch.com/2018/07/19/facebok-under-13/?utm_campaign=Revue%20newsletter&utm_medium=Newsletter&utm_source=The%20Interface; WhatsApp plans to ban under-16s. The mystery is how, The Guardian, 26 April 2018, https://www.theguardian.com/commentisfree/2018/apr/26/whatsapp-plans-to-ban-under-16s-the-mystery-is-how.

policies remain as they are and age verification is taken seriously, then the likely consequence will be that children under the age of digital consent will effectively be banned from many platforms that play an important role in their lives right now. Paradoxically enough, these online services are mostly based on the surveillance capitalism business model and thus exactly the ones we may want to protect children from.

All in all, greater protection for children under the GDPR can inversely impact their participation and emancipation rights, such as their right to access to media[49], freedom of expression[50], their right to play[51], to association[52] and to personal development[53].

C. Development

The datafied digital world is an inherently commercial world. Real children's spaces are few and far between — at least the ones popular among children — and even those may be dominated by surveillance capitalism. The development perspective entails that children grow up into self-sufficient, independent and self-reliant children.[54] Growing up in a datafied digital world, however, requires new and more sophisticated knowledge and skills to be able to make informed choices.

The GDPR to a certain extent accommodates transparency by requiring data controllers to fill their customers in on

49. See article 17, UN CRC.
50. See article 13, UN CRC.
51. See article 31, UN CRC.
52. See article 15, UN CRC.
53. See article 6, UN CRC.
54. Lansdown (2005), *supra*.

data processing practices,[55] but as I have pointed out earlier such information disclosures rarely result in people actually being informed. The reason is not only that information such as provided in privacy policies is inadequate, but the extent and consequences of data processing practices can only be grasped if you understand the underlying dynamics of surveillance capitalism. To confer that kind of knowledge is very difficult, because the way the datafied digital world is scripted to harvest as much of our data as possible is invisible to us. My colleague and philosopher of technology Esther Keymolen has coined the concept Invisible Visibility for this phenomenon: we become increasingly more transparent to data companies (and governments for that matter) but in ways that are completely invisible to us.[56]

It is quite telling even with the Facebook/Cambridge Analytica scandal all over the media, we still hear people say that as long as they are careful with what they publish online they do not need to be too worried. This is only one type of data we reveal, yet our behavioural and inferred data of which we may not be equally aware that it is being harvested is much more valuable. These surveillance practices are everywhere even if we do not see them. In the wake of the Facebook scandal, the Dutch media disclosed that many medical insurance firms and some hospitals have Facebook pixels embedded in their websites, allowing Facebook to gather data on the types of medical

55. Article 12, GDPR, providing that companies must "provide any information […] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *in particular for any information addressed specifically to a child*." (italics by the author)
56. See Van der Hof, S. , Keymolen, E.L.O. Shaping Minors with Major Shifts: Electronic Child Records in the Netherlands. 15 Info. Polity 309, 311 (2010).

information website visitors are interested in.[57] These are websites that people may actually trust as being privacy friendly.

The development perspective requires that we educate children how the datafied digital world is socially, economically and technologically constructed, which is knowledge that goes beyond teaching them the digital skills to use digital media and produce content in a safe and constructive way. Similarly, when teaching children about democracy we teach them how the system works, what checks and balances are in place, what underlying interests influence the political system and so on. Digital citizenship requires that children understand surveillance capitalism, the consequences and risks of profiling and the ways in which our minds are constantly manipulated into revealing more data. And most importantly, a crucial lesson includes raising awareness that the digital world is a constructed world and, thus, can be constructed differently. The values embedded in the technology are not set in stone but different choices can be made. Tracking people is not a given in the nature of the internet, rather it has become the predominant feature of many online platforms that have been built on top of the network of networks. Those platforms can be constructed in ways that do not make them tools of surveillance.[58] Which brings me to the final part of my narrative.

57. Verzekeraars sturen surfgedrag naar Facebook, ook van medische pagina's, https://nos.nl/artikel/2226902-verzekeraars-sturen-surfgedrag-naar-facebook-ook-van-medische-pagina-s.html (last visited 23 July 2018).
58. See all: Van der Hof (2017), *supra*.

5. A holistic approach to the protection of children's personal data

It is probably in our human DNA to cling to the right to informational self-determination that is underlying the notion of consent as the key to the processing of personal data in many instances. Hence, I would not want to argue for abolishing consent as a lawful ground under the GDPR and I guess Thorbecke — the man in whose honour I have written this work — would have agreed. Therefore, it is important to think carefully about how to construct consent processes in ways that face the challenges I have put forward so far. However, if you take consent as the entry point for improving the protection of children's data, the results are likely to be insufficient or not adequate at all, given that the most challenging issue of all is surveillance capitalism.

This is where the second dimension of the holistic approach becomes crucial. The basic idea is that from the outset and throughout the whole development of digital services, data protection principles and risk assessment must become a structural part of the system. This is not a novel idea, nor is it optional under the GDPR; it is part and parcel of the responsibilities of any organisation that processes personal data. However, these responsibilities have not — or not clearly at least — been formulated with children in mind, which is probably why they have not received attention in relation to children.[59] Yet, both the best interest of the child and the explicit emphasis on child protection in the GDPR provide strong arguments for a child-specific implementation of responsibilities of

59. See for an exploration of this approach: Van der Hof, Lievens (2017), *supra*.

internet platforms. I will give one example to illustrate this approach.

One of the most prominent principles in the GDPR — a regulatory innovation even — is the principle of data protection by design.[60] This principle requires that data controllers effectively implement data protection principles into the design of data processing systems. Clearly, such a strategy shifts responsibility from parents and children to protect themselves from data controllers. It may intrinsically augment the protection of individuals and their personal information and mitigate some of the problems with consent. At the heart of privacy by design is the data minimisation principle, which entails that only data are processed that are necessary for the purpose of the processing.[61] Companies, therefore, need to carefully select what data are really necessary to provide a certain service and not go beyond those data and, preferably, wherever

60. See Article 25, GDPR (Data protection by design and by default), which states:
    "1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
    2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
    […]"
61. See Article 5(1)(c), GDPR.

possible pseudonimise[62] any data that they do collect, i.e. ensure that the data can no longer be attributed to a specific person.

But privacy by design goes beyond mere data minimisation. It holds opportunities to make control over personal data an innate part of data processing practices and to enforce the stricter rules with respect children that exist for transparency of data practices,[63] online profiling of children,[64] marketing targeted at children and the right to start with a clean slate once you come of age.[65] Important to note is also that no age restrictions are set for privacy by design, nor is it limited to online commercial services. As a result, such protections are likely to apply to any child under 18 and certainly to other services, including those used in youth-care, medical and school settings. Besides privacy by design, the GDPR provides other instruments such as data protection impact assessments[66] and codes of conducts[67] that are likely to contribute to the protection of children's privacy.[68]

We think these instruments might actually mitigate some of the challenges in the protection of children and balance control over children's personal data with other children's interest and rights. However, in order to achieve

62. See Article 4(5), GDPR; pseudonimisation means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."
63. Articles 12-14, GDPR.
64. Article 22, GDPR; see also Recital 71.
65. See Article 17, GDPR ('right to be forgotten'); see also Recital 65.
66. Article 35, GDPR.
67. Article 40, GDPR.
68. See further Van der Hof, Lievens (2017), *supra*.

that goal these instruments need to be implemented with children, children's interests and perceptions, and children's rights in mind. To find out what works for children is particularly essential and calls for more research. What are children's privacy expectations in the digital world? How can we explain data practices and their rights to them in a meaningful way, taking different ages into account? And how do we address particularly vulnerable children? A child-centred approach would be in the spirit of the GDPR and data protection as a fundamental right,[69] the aim of which is to protect the autonomy and dignity of all human beings, including children. But it entails going beyond the GDPR as a mere checklist for compliance. To take it even a step further, I argue that if we are able to get it right for children, it might be used as a benchmark for adequately protecting adults as well.

6. Closing words

The Facebook scandal has been a wake-up call for many people, but it does not mean the dynamics of the datafied digital world will change— at least not over night. Platforms built on surveillance capitalism cannot easily, or at all, change their tactics. Great hope is projected on the entry into force of the GDPR to at least improve protection. The extraterritorial nature[70] of the rules and the high fines[71] that can be imposed on companies give the GDPR teeth that were sorely missing under the laws we had so far. But in order to protect children in line with their rights under the most successful international treaty ever adopted, the UN CRC, it is crucial to go beyond mere compliance with the GDPR and even to go beyond the

69. See Articles 8 and 24, Charter of Fundamental Rights of the European Union.
70. See Article 3, GDPR.
71. See Article 83, GDPR.

data protection framework as such. Social media are not the problem, surveillance capitalism is. Online services and platforms play an important part in children's participation, emancipation and development. Together with children we need to reflect upon the digital world in ways that would take their interests, expectations and rights seriously. In my inaugural lecture in 2013,[72] I called for spaces of empowerment for children in line with philosopher Michael Walzer's spheres of justice.[73] For these spaces to be just and for humans to be able flourish in them, abstract rights must be translated into real everyday experiences and expectations of people, says philosopher of law Julie Cohen.[74] I would add that children's voices must not be forgotten. Today we hear voices calling for public digital spaces where people gather and communicate free from commercial surveillance. Spaces that are essential for children as well, just like the playground in the beginning of my talk — but without the notebooks and the prying eyes. Spaces that recognise human dignity, the fundamental rights to privacy and data protection, the GDPR — and especially its principle of privacy by design — but also the rights and principles put forward by the UN CRC. Spaces of empowerment that may even be in the spirit of Thorbecke. He lived in times very different from the ones we live in now but he saw the impact of technology — machines in his case — on the people — especially in terms of inequalities and some benefiting

72. Van der Hof, S., Digitale kinderrechten: balanceren tussen autonomie en bescherming, Inaugural lecture, Leiden University, 2013.
73. Walzer, M., Spheres of justice: A Defense Of Pluralism And Equality, Basic Books, 1984.
74. Cohen, J., Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press, 2012.

more from technology than others.[75] Indeed topics that are still relevant today and go at the heart of humanness and how to preserve human dignity in technologically turbulent times, including the dignity of children. These issues have never been more important than now and will only continue to gain in significance in the future.

75. Thorbecke, J.R., Verhandeling over den invloed der machines op het samenstel der maatschappelijke en burgerlijke betrekkingen, Gent, 1830, text available at: http://home.planet.nl/~dmjanssen1960/Invloed_der_Machines.html (last visited 23 July 2018).