I AGREE. . . OR DO I? — A RIGHTS-BASED ANALYSIS OF THE LAW ON CHILDREN'S CONSENT IN THE DIGITAL WORLD

SIMONE VAN DER HOF*

* Professor of Law in the Information Society, Center for Law and Digital Technologies, Leiden Law School, Leiden University. I am grateful to my colleagues Bart Custers, Esther Keymolen and Ton Liefaard for their valuable feedback. Many thanks also to the organizers of the WILJ 2016 Symposium 'Stamping privacy's passport: The Role of International Law in Safeguarding Individual Privacy', University of Wisconsin Law School for kindly inviting me to present this paper.

INTRODUCTION

Almost all children are online in the Western World. The Internet has become an intrinsic part of their everyday lives, wherever they are. To use their computer devices, download apps, surf the web, enjoy music and vlogs, post messages on social media, and participate as a citizen in modern society, and so on, children continuously give and give off crumbs and chunks of their own personal data to businesses, governments, and other individuals. In many contexts, sharing personal data is subject to the consent of the person concerned and in more and more situations that person is a minor, i.e. a person who has not yet reached the age of majority. The concept of consent is wrought with issues and as a result, we might question the effectiveness and even fairness of consent as a means for children to exercise privacy and data protection rights in the digital world. In addition, given the growing complexity of personal data processing, we need to consider whether it is necessary to recalibrate the balance between autonomy and protection, which are key in giving meaning to children's rights in theory and practice. Moreover, it is important to develop tools for meaningful and secure participation of children in the digital world that allow them to adequately retain control over their personal data, or at least make more informed choices in their daily digital lives—or "onlives," which is a fitting term given the hyperconnectedness in and of todays' world.[1]

This article analyzes the concept of children's consent in the digital world from the perspective of the rights-based approach as propagated by the UN Convention on the Rights of the Child 1989 (*hereinafter* UN CRC or Convention).[2] The article will particularly analyze the distribution of consent decisions between minors and parents with respect to online processing of personal data through the three conceptual lenses of protection, participation/ emancipation, and development of children to

---

[1] *See* THE ONLIFE MANIFESTO, BEING HUMAN IN A HYPERCONNECTED ERA (Luciano Floridi ed. 2015).

[2] G.A. Res. 44/25, Convention of the Rights of the Child (Nov. 20, 1989).

adulthood, which are fundamental to the rights-based approach of the Convention.[3] Taking this multidimensional perspective towards children's consent and the ways in which it has been regulated in United States and European Union law provides a considerably richer and significantly more balanced view on children's consent in the digital world than merely viewing such issues from the protection paradigm that is currently at the heart of the debate.

The article starts out with briefly characterizing today's data-intensive digital world, in which children and teens grow up, by focusing on the trends of datafication, hyperconnectivity, and commercialization, and the (potential) effects these trends may have on children's lives. Subsequently, in Part II, the article sets out the legal notion of consent and how consent has been regulated in the United States and the European Union. Part III sets out the rights-based approach under the Convention, before analyzing the legal approaches to consent in light of the three conceptual lenses that underpin the rights-based approach. First, children's consent is analyzed through the lens of protection, and addresses whether children need protection and to what extent their parents or caregivers will provide such protection. This part demonstrates various issues that make consent problematic as an effective and fair means of exercising privacy and data protection rights. Second, the law on children's consent is considered through the lens of participation and emancipation. To what extent have the rights of children been sufficiently respected in the law on children's consent? Third, the adequacy of the law on children's consent is tested in terms of the optimal development of children. To what extent and how can children's basic needs to make sound decisions on personal data processing in today's digital world be accommodated? Part IV then presents the conclusions of the analysis and some recommendations for potential ways forward in addressing the challenges raised by the rights-based analysis of children's consent.

I. CHILDREN IN A DATA-INTENSIVE, HYPERCONNECTED AND COMMERCIAL DIGITAL WORLD

Youth of today grow up in a data-intensive digital world that is characterized by a number of trends. These trends impact their lives in ways that can, as yet, only partly or hardly be foreseen. To set the scene

---

[3] Gerison Lansdown, *The Evolving Capacities of the Child*, UNICEF INNOCENTI RESEARCH CENTRE, 3 (2005), http://unicef-irc.org/publications/pdf/evolving-eng.pdf.

for this article's further analysis, this section will briefly address the mutually reinforcing tendencies of datafication, hyperconnectivity, and commercialization, and briefly go over some—actual and potential—consequences thereof.

A. DATAFICATION

The amount of personal data that is processed on the internet has exponentially grown in recent times and will go on to increase rapidly in the future. Basically, three types of data can be distinguished as part of the growing data intensity. First, some of that data is given or published by the individuals themselves. If children open an account to play in the online virtual world Minecraft, they need to register with their e-mail addresses and birth dates, as well as submit payment details to buy the software that actually allows them to enter this blocky online world.[4] Intimate personal information and creative content, such as pictures and videos, are shared on various social media. Such personal data will be given more or less consciously, meaning children can contemplate whether they indeed want to share certain information and whom in their circle of family, friends, and others they want to share it with.

Second, just by being and acting online through computers and mobile devices, such as tablets and smart phones, a lot of personal data is—mostly unconsciously or unknowingly—*given off*.[5] When surfing the web individuals leave digital traces by clicking from link to link in search engines, online stores, on social media, and so on. This is also called behavioral data; how individuals behave on the internet can be meticulously documented by using technologies, such as tracking cookies[6], web beacons[7] and device or browser fingerprinting.[8,9] People also

---

4 *See generally* MINECRAFT, https://minecraft.net/nl/store/minecraft/#register (last visited Oct. 15, 2016).

5 ERVIN GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE,10-46 (1956); B. Van den Berg, The Situated Self: Identity in a World of Ambient Intelligence, 168 (Apr. 23, 2009) (unpublished Ph.D. thesis, Erasmus University of Rotterdam).

6 *See generally HTTP Cookie*, WIKIPEDIA, https://en.wikipedia.org/wiki/HTTP_cookie (last visited Oct. 15, 2016) (definition of a "cookie.").

7 *See Generally*, *Web Beacon*, WIKIPEDIA, https://en.wikipedia.org/wiki/Web_beacon (last visited Oct. 15, 2016).

8 *See Generally Device Fingerprint*, WIKIPEDIA, https://en.wikipedia.org/wiki/Device_fingerprint (last visited Oct. 15, 2016).

9 Tools exist to visualize your tracking and tracing. *See e.g.* PANOPTICLICK, https://panopticlick.eff.org/about (last visited Oct. 15, 2016); *Add-ons*, LIGHTBEAM FOR FIREFOX BY MOZILLA, https://addons.mozilla.org/en-US/firefox/addon/lightbeam/ (last visited Oct. 15,

give out a lot of data that is (potentially) very personal both on the web and on by using apps on mobile devices, such as smart phones. These apps offer a wide range of services that cover many aspects of our professional and personal daily lives, such as communications with family, friends and others, day-to-day schedules and activities, our innermost thoughts, news reading and other habits, exercise and health information, and entertainment preferences. As a smart phone commercial fittingly states about whatever you want to do or are interested in: "There's an app for that."[10] App users are not only sharing data, including personal data, with the app companies, but also—and sometimes too extensively and despite promises to the contrary—with third parties, or when apps are not in use.[11] Data given off—or observed data—does not merely consist of content, i.e. communications, social media posts, pictures and video's et cetera, but also of metadata, i.e. data about data. Metadata includes, for example, meta-information about your smart phone, such as MAC-address, usage, social connections, how often you call whom, when and where, and other location data.[12]

Based on such metadata, individuals can be uniquely identified by their smart phones.[13] This brings us to the third category of data, i.e. inferred data, or new data that is derived from other data. Captured by the buzzword 'big data,' the trend of datafication is augmented by sophisticated and real-time automated data analysis through algorithms.[14] The data given and given off—and other data—are captured, processed, and then analyzed with algorithms, which results in new knowledge consisting of patterns and correlations. Therefore, knowledge about someone can be inferred that was perhaps not disclosed by individuals because

---

2016) (product for purchase which enables the buyer to see "the first and third party sites you interact with on the Web").

[10] *See Sesame Street: There's an App for That* (PBS broadcast Nov. 3, 2010) You will be able to find the relevant clip on Youtube. Sesame Street, *Sesame Street Song: There's an App for That*, YOUTUBE https://www.youtube.com/watch?v=EhkxDIr0y2U (last visited Nov. 11, 2016).

[11] ANTOINE PULTIER ET AL., SINTEF, PRIVACY IN MOBILE APPS: MEASURING PRIVACY RISKS IN MOBILE APPS 9 (2016); FINN LÜTZOW-HOLM MYRSTAD ET AL., FORBURKER RADET, APPFAIL: THREATS TO CONSUMERS IN MOBILE APPS 41-43 (2016), http://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/.

[12] *See* Phillip Branch, *Metadata and the Law: What your Smartphone Really Says About You*, THE CONVERSATION (Mar. 2, 2014), https://theconversation.com/metadata-and-the-law-what-your-smartphone-really-says-about-you-23827.

[13] Yves-Alexandre de Montjoye, et al., *Unique in the Crowd: The Priacy Bounds of Human Mobility*, NATURE.COM (Mar. 25, 2013) http://www.nature.com/articles/srep01376.

[14] CHRISTOPHER STEINER, AUTOMATE THIS, HOW ALGORITHMS CAME TO RULE OUR WORLD 204 (2012).; VIKTOR MAYER-SCHÖNBERGER, & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 78 (Eamon Dolan ed., 2014).

they perceived it as too personal to share online. Based on Facebook "likes," personality traits (openness, intelligence) and personal attributes (gender, sexual orientation, political orientation, ethnic origin) can be predicted with high accuracy, even if the "likes" themselves do not reveal the trait or attribute.[15] In a 2014 Stanford University study, two computer science students found that analyses of telephone metadata produces extremely sensitive information about individuals, such as medical information, political and religious associations, and sexual interests.[16] The researchers contend that their study involved merely simple inferences.[17] Obviously, more advanced data analytics can yield even more sophisticated outcomes. The end of what technologies can do with data in all its colorful varieties and forms, either in collecting, processing, or enhancing it, is nowhere near in sight. Moreover, the datafication trend is amplified by an increasing hyperconnectivity of individuals and artifacts.

B. HYPERCONNECTIVITY

Hyperconnectivity essentially denotes the trend of an increasing number of individuals and artifacts continuously being connected through networked, digital technologies. In a relatively brief period of time, we have come a long way from computers connecting the first people across the network of networks to a world in which each person is digitally connected. In addition, increasingly the physical things that surround us—such as thermostats, television, and washing machines—are able to join us online to increase the efficacy of organizational processes and make our lives more convenient. These interconnected physical objects turn into "smart devices" when they start tracking and predicting our behavior to cater to our preferences and needs (or those of others). The "internet of people" and "internet of things" become more and more intertwined, and even merge when individuals equip themselves with wearables that incorporate electronics and sensors to track their move-

---

[15] Michal Kosinski et al., *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 PROCEEDINGS OF THE NATI'L ACAD. OF SCI. OF THE U.S. 5802-05, 1 (2013).

[16] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POLICY (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

[17] *Id.*

ments, bodily data, and emotional or mental status.[18] Needless to say, the hyperconnectivity of individuals and objects brings about a greater data-intensity than ever before. The internet of things increasingly harbors devices that are particularly meant for children, such as smart toys. In 2015, toy company Mattel started shipping Hello Barbie, a WIFI-enabled smart Barbie doll that records and analyzes children's (and any other) conversations to find out about their interests and preferences (and potentially other things).[19] Eavesdropping on children at play was perceived as a bridge too far and a petition has been launched to "say goodbye to 'Hello Barbie.'"[20]

C. COMMERCIALIZATION

Underlying the previously mentioned tendencies is the commercialization of children's everyday lives. The digital world is a highly commercialized world that is predominantly constructed and scripted by companies to serve their economic interests. A strong motivator behind both datafication and hyperconnectivity, and particularly the combination of both, is to considerably improve businesses' understanding of actual and potential customers in order to better target their products and services and increase profits.[21] Children are important targets for the marketing industry for three reasons: they have (increasingly more) money to spend; children influence family spending; and children are future consumers.[22] Research organizations specialized in marketing to children have developed sophisticated strategies focused on different stages of child development, which already include babies and toddlers.[23] In the digital world, marketing to children has changed considerably as compared to traditional advertising in magazines and on television. As Montgomery, Grier and Dorfman describe:

---

[18] *See e.g.* Nic Fleming, *Know Thyself: The Quantified Self Devotees Who Live by Numbers*, THE GUARDIAN (Dec. 2, 2011) https://www.theguardian.com/science/2011/dec/02/psychology-human-biology.

[19] *Stop Mattel's "Hello Barbie" Eavesdropping Doll*, CAMPAIGN FOR A COMMERCIAL-FREE CHILDHOOD (Feb. 29, 2016), http://www.commercialfreechildhood.org/action/stop-mattel%E2%80%99s-hello-barbie-eavesdropping-doll.

[20] *Id.*

[21] *See e.g.*, Jerry Daykin, *Personalised Marketing at Scale is the Next Big Thing in Digital*, THE GUARDIAN, (Mar. 19, 2015), https://www.theguardian.com/media-network/2015/mar/19/personalised-marketing-digital-future.

[22] PATTI VALKENBURG, SCHERMGAANDE JEUGD: OVER JEUGD EN MEDIA 166 (2014).

[23] *Id.* At 165.

> Unlike television, where children's exposure to commercials is limited to brief intervals during the times when they are viewing the programs, digital marketing is now woven into the fabric of young people's daily experiences, integrated not only into their media content but also into their social and personal relationships. Young people are not just viewing content but also inhabiting media environments where entertainment, communication, and marketing are combined in a seamless stream of compelling sounds and images.[24]

Marketing has increasingly become more integrated in our offline and, particularly, online environments. In addition, the line between information, entertainment, and play versus marketing has blurred. Since individuals can too easily ignore or skip advertising when it is recognizable as such, marketing strategies are focused on hiding commercial messages and manipulating individual persons unconsciously.[25] Advergames are a case in point—advergames include online games that aim to stimulate brand awareness, without necessarily showing the brand or the products that are sold under a particular brand as part of the game.[26] Advergames may involve colorful and fun characters that highly appeal to children and are used in supermarkets to sell food, especially sweets and snacks such as ice cream, cereals, and cookies. Research has shown that commercialization has negative effects on children by inducing materialistic values in children, encouraging negative relations between child and parent, and exacerbating unhealthy lifestyles and health problems (e.g. obesity, eating disorders) for children.[27] It begs the question, how are these emerging invasive and difficult-to-escape marketing practices fair to children.[28]

Commercialization of children's "onlives" is significantly augmented by other modes of manipulation that go with these advanced marketing strategies. Datafication practices are part of a carefully orchestrated game plan, in which internet companies immerse users in interac-

---

[24] Kathryn C. Montgomery et al., *The New Threat of Digital Marketing*, 59 PEDIATRIC CLINICS OF N. AM. 659, 660 (2012).

[25] *See e.g., Mind Control Theories and Techniques Use by Mass Media*, THE VIGILANT CITIZEN (Apr. 28, 2010), http://vigilantcitizen.com/vigilantreport/mind-control-theories-and-techniques-used-by-mass-media/.

[26] AGNES NAIRN & HAIMING HANG, FAMILY AND PARENTING INSTITUTE, ADVERGAMES: IT'S NOT CHILD'S PLAY 5 (2012) http://www.agnesnairn.co.uk/policy_reports/advergames-its-not-childs-play.pdf.

[27] *See* VALKENBURG, *supra* note 22.

[28] ISOLDE SPRENKELS & IRMA VAN DER PLOEG, *Follow the Children! Advergames and the Enactment of Children's Consumer Identity*, *in* MINDING MINORS WANDERING THE WEB, REGULATING ONLINE CHILD SAFETY 173 (Simone van der Hof et al. eds. 2014).

tive digital environments and nudge them to disclose their innermost thoughts and feelings as well as forecast inclinations and contingencies that shed a new light on the ways in which we are attracted to potential objects of interest. Corporate surveillance is the default in many of the apps and online services that children use because it presents the foundation on which most of these companies are built and, hence, their design is tweaked, tuned, and tested meticulously to produce the best results.[29] What at face value seems like an innocent sharing of stories with loved ones to the users is therefore big business to the service providers. Most of the ways in which users are played happens unconsciously and oftentimes invisibly. As Sprenkels and Van der Ploeg write when addressing a particular advergame, "this clever design consists of putting 'reading clues' about fun and play in the foreground while remaining silent on processes, activities and intentions in the background."[30]

Sometimes, such manipulative practices surface in the media and might even result in—often short-lived—public commotion. This happened, for example, when Facebook's secret mood experiment, which had been carried out without the user's informed consent, surfaced in a research paper.[31] Oftentimes, data processing might go beyond our expectations of what we think is necessary or justified. Why, for instance, does the flashlight app on your smartphone need access to your contacts list?[32] And, why is an app still transmitting data when it is not in use?[33] Companies that engage in corporate surveillance and user manipulation have an intrinsic economic interest in carefully keeping the lid on such practices to not undermine their effectiveness or disquiet and alienate users. This leads to what is called "invisible visibility," a term coined by Esther Keymolen.[34] Invisible visibility signifies an increased transparency of individuals to companies and governments in ways that are com-

---

[29] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 21–23 (2015).

[30] Sprenkels & van der Ploeg, *supra* note 28, at 183.

[31] Katy Waldman, *Facebook's Unethical Experiment*, SLATE (June 28, 2014, 5:50 PM), http://www.slate.com/articles/health_and_science/science/2014/06/facebook_unethical_experiment_it_made_news_feeds_happier_or_sadder_to_manipulate.html.

[32] *See* John Leyden, *This Flashlight App Requires: Your Contacts List, Identity, Access to Your Camera. . .*, THE REGISTER (Sep. 11, 2014, 10:56 AM), http://www.theregister.co.uk/2014/09/11/mobile_app_privacy_survey/.

[33] *See* Pultier et. al., *supra* note 11.

[34] Mireille Hildebrandt, *Who is Profiling Who? Invisible Visibility*, in REINVENTING DATA PROTECTION? 239, 240 (S. Gutwirth et al. eds. 2009).

pletely opaque to them.[35] The consequences are a lack of power for individuals to—effectively—exercise their rights, including privacy and data protection rights, and to hold these organizations accountable for their actions.

The developments described in this section will form the backdrop against which the law on children's consent will be scrutinized from a rights-based perspective. First, however, the following sections will address the notion of (children's) consent and the rights-based approach under the UN CRC.

II. THE NOTION OF CONSENT

A. INTRODUCTION

Consent is a crucial concept in law and society and denotes the autonomy of individuals to have control over their lives. To allow individuals the freedom to make decisions about their lives denotes a shift from a paternalistic paradigm to a rights-based paradigm. Beyleveld and Brownsword underline the social importance of the concept when stating:

> [T]hat where a society (and this, it should be emphasised, means any society, English or American, African or Asian, common law or civilian-based) takes individuals and their choices seriously—particularly so, perhaps, where social relationships are framed by a respect for human rights—the concept of consent will come to play a key role in its practical thinking.[36]

The next section will show how consent has two interrelated functions, which are essential in light of the rights-based approach to be discussed in Part IV.1. Subsequently, Part III.3. will set out the particular rules that have been introduced on children's consent privacy and data protection laws in the United States and the European Union.

B. THE DOUBLE ROLE OF CONSENT

Notions of autonomy and freedom are inherent in the concept of consent in two different ways. Consent is a manifestation of an individual's right of freedom under the law, such as human rights law, but con-

---

[35] Simone van der Hof & Esther Keymolen, *Shaping Minors with Major Shifts: Electronic Child Records in the Netherlands*, 15 INFO. POLITY 309, 311 (2010).

[36] DERYCK BEYLEVELD & ROGER BROWNSWORD, CONSENT IN THE LAW 2–3 (2007).

sent also sets in motion the exercise of those rights by individuals and, by doing so, can turn activities that would otherwise be a violation of their rights into lawful ones.[37]

First, consent as a *manifestation of rights* is evidenced by the individual's right to the integrity of the body, which signifies not only the inviolability of the physical body but also the individual freedom to self-determination over one's body.[38] Individuals, for instance, have the freedom to decide about their bodies being pierced, tattooed, enhanced through plastic surgery, or, in more extreme situations, even being inflicted pain or humiliation in sadomasochistic settings. From a privacy and data protection perspective, the notion of consent is embodied in the right to informational self-determination.[39] The right to informational self-determination is a notion that intrinsic to the value of human dignity and the development of the human personality[40]distinctly puts the individual at the center of online activities in which their personal data is processed—including any results of such processing, such as profiles, are used[41]—for whatever purposes. Under the rights to informational self-determination, "a situation that should clearly be avoided was to create feelings to the individuals of complete loss of control over the information that is collected about them."[42]

Privacy epitomizes many different conceptions, one of which is the claim of having control over our personal information by being able to decide who does or does not have access to that information.[43] The right to informational self-determination particularly captures "the authority of the individual to decide himself, on the basis of the idea of

---

[37] *See id.*; *see also* Bart W. Schermer, Bart H.M. Custers & Simone van de Hof, *The Crisis of Consent, How Stronger Legal Protection may Lead to Weaker Consent in Data Protection*, 16 ETHICS & INFO. TECH. 171 (2014).

[38] *See, e.g.*, RUTH A. MILLER, THE LIMITS ON BODILY INTEGRITY 7–8 (2007) (on bodily integrity and consent in sexual relations).

[39] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 BVERFGE 1, 2008 (Ger.) (the German Constitutional Court holding the right to informational self-determination was recognized as a part of a general personal right in the 1983 Population Census case).

[40] *Id.*

[41] *See* Regulation 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), art. 4(4), 2016 O.J. (L 119) 1, 33 [hereinafter GDPR].

[42] ELENI KOSTA, CONSENT IN EUROPEAN DATA PROTECTION LAW 30 (2013).

[43] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM (1970); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

self-determination, when and within what limits information about his private life should be communicated to others," and "that an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-determined.'[44] Although the right to informational self-determination is not yet endorsed as a right in and of itself, it has influenced data protection laws in European countries and augmented the pivotal role of consent therein.[45] Moreover, it has a broader, social dimension that goes beyond the individualist conception of the right as "self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate."[46]

Second, consent is a fundamental legal instrument for *transforming unlawful conduct into lawful conduct*. Consent allows an individual to say "yes" or "no" to an action that impacts them personally and thus exercise their freedom to self-determination. In addition, by saying 'yes' an otherwise unlawful action, that action may even be legalized.[47] For instance, hurting a person is, in principle, not acceptable and can be legally characterized as physical abuse or even attempted murder depending on the severity of the circumstances. A surgeon who operates on a patient, however, is not likely to face such consequences if the patient consented to the operation. In this way, "being hurt" has been transformed from an unlawful action to something perfectly legitimate with the approval of the patient. Under European data protection law, consent is codified as one of the most important grounds for the lawful processing of personal data.[48] Unlawful personal data processing—assuming no other legitimate grounds for personal data processing apply—is transformed into lawful personal data processing through the authorization given by the data subject.[49] Individuals can only provide legally transformative consent when the law recognizes their capacity to do so. The next section will discuss at what age children are deemed legally capable of consenting to the col-

---

[44] Antoinette Rouvroy & Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in REINVENTING DATA PROTECTION? 45, 51 (S. Gutwirth et al. eds. 2009).

[45] *See id.*; *see also* KOSTA, *supra* note 42.

[46] Rouvroy & Poullet, *supra* note 44, at 53.

[47] *See* BEYLEVELD & BROWNSWORD, *supra* note 36; *see also* Schermer et. al., *supra* note 37.

[48] *See* GDPR *supra* note 41, art. 6(1)(a), at 36.

[49] The data subject is an identified or identifiable natural person to whom information relates. *See* GDPR *supra* note 41, art. 4(1), at 33.

lection and use of their personal data in the United States and the European Union.

C. CHILDREN'S CONSENT

The extent to which children can legally provide consent depends on the capacity of children to make decisions for themselves in a given situation. When they have that capacity, their decisions must be respected. If they lack such capacity, the consent of a third party, most notably the person with parental authority, will be required. The child's capacity to consent derives from their level of maturity—do they have the cognitive ability to sufficiently understand their position and, hence, to give consent? In the landmark case of Gillick, the UK House of Lords formulated the capacity to consent as: "a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision".[50]

In Gillick, the House of Lords determined that in those instances where children have that capacity, medical practitioners need indeed to ask the child instead of the parent for consent to treatment.[51] The level of maturity of the child is also reflected in the privacy and data protection laws in the US and the EU. Both the US Children's Online Privacy Protection Act (*hereinafter* COPPA)[52] and the General Data Protection Regulation (*hereinafter* GDPR)[53] in the European Union hold special provisions on children's and parental consent that take into account different ages of children. This section will show how children's and parental consent has been regulated in both these laws. The purpose of this analysis is not to provide a full-blown comparison or a critical assessment of these laws, but to focus on the principal characteristics of children's consent.

1. Children's Online Privacy Protection Act (COPPA)

In 1998, the federal Children's Online Privacy Protection Act (effective as of April 2000) was introduced in the United States. After a review of COPPA by the Federal Trade Commission (FTC) in 2010, COPPA was amended with the new rule taking effect in July 2013. The

---

[50] Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 AC 112 (HL).

[51] *Id.*

[52] Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013).

[53] GDPR *supra* note 41.

rationale for the introduction of COPPA was the increasing internet use of children that enabled marketing companies to compile lists of children's personal information and behavioral data that were subsequently sold to third parties.[54] Interestingly, privacy concerns were not the only driving force behind the introduction of the act; potential online safety risks, such as (online) predators getting their hands on children's personal data, were also perceived as very worrisome after investigative reports demonstrated the ease with which mailing lists consisting of children's personal information could be obtained from marketing companies.[55] COPPA was codified in and has been implemented by 16 C.F.R. Part 312 and violations of the rule are considered unfair or deceptive trade practices under section 5 of the Federal Trade Commission Act.[56]

The COPPA rule stipulates that commercial online service providers must obtain verifiable parental consent[57] before personal information of children is collected, used or disclosed,[58] as well as after material changes have been made to the data processing practices.[59] Children are defined as individuals under the age of 13.[60] The online services must either be directed to children or service providers, and must have actual knowledge that they are collecting personal information from children below 13. Hence, general audience websites or apps must also comply with the rule if they know they are collecting data from children below 13.[61] Parental consent must be *verifiable*, which entails that prior to the collection of personal information of the child, any reasonably effort (taking into account the technological state of the art)[62] must be made to ensure that the parent of the child: (1) is informed of the personal data processing practices by the online service provider; and (2) authorizes

---

[54] *See Children's Online Privacy Protection Act (COPPA)*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/kids/ (last visited Nov. 9, 2016).

[55] *Id.*

[56] *See* 16 C.F.R. § 312.3; Federal Trade Commission Act, 15 U.S.C. § 45 (2014).

[57] 16 C.F.R. § 312.5(c) (for exceptions to parental consent).

[58] Personal information is "individually identifiable information about an individual collected online." 16 C.F.R. § 312.2 (further specifying personal information by providing examples of personal information).

[59] *See* 16 C.F.R. § 312.5(a)(1).

[60] 16 C.F.R. § 312.2.

[61] As a result, children under 13 are often banned from online services. *See e.g., Under 13 Year Olds on Facebook: Why do 5 Million Kids Log in if Facebook Doesn't Want Them to*? REUTERS (Sep. 9, 2012, 6:07 PM), http://www.huffingtonpost.com/2012/09/19/under-13-year-olds-on-facebook_n_1898560.html.

[62] *See* 16 C.F.R. § 312.5(b) (identifying mechanisms for verifiable parental consent).

those practices.[63] Finally, there needs to be an element of choice when it comes to the sharing of personal data with third parties; parents should be able to consent to the collection and use of their child's personal information by the online service provider, without also authorizing the disclosure of that personal information to third parties.[64] Furthermore, the COPPA rule allows parents to refuse the further or future processing of their child's personal information and tell the online service provider to destroy personal information that has been collected so far.[65] Upon such refusal, the online service provider can end any service provided to the child.[66]

B. General Data Protection Regulation

In 2016, the General Data Protection Regulation was adopted[67] by the European Union Council and Parliament to both invigorate respect for the right to personal data protection as a fundamental right,[68] and sustain the development and strengthening of the internal (digital) market through the free movement of personal data.[69] Its predecessor, the Personal Data Protection Directive, did not contain specific provisions on the protection of children's personal data.[70] It was thus up to member states to regulate on their own. As a result, law on the capacity of minors to consent to personal data processing by online service providers imparts quite a diversified picture. The minimum age to consent to personal data processing varies in the European Union—ranging from 14 to 16 years.[71] Moreover, the validity of consent may depend on the circumstances of a particular situation.[72] In some instances, children might be expected to better deal with such decisions than in other times, allowing

---

63 16 C.F.R. § 312.2.

64 16 C.F.R. § 312.5(a)(2).

65 16 C.F.R. § 312.6(a)(2).

66 16 C.F.R. § 312.6(c).

67 Taking effect as of May 2018. GDPR *supra* note 41.

68 Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. (C 364) 1, 10 [hereinafter Charter of Rights].

69 GDPR *supra* note 41, at 1.

70 Directive 95/46, of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31.

71 Terri Dowty & Douwe Korff, *Protecting the Virtual Child: The Law and Children's Consent to Sharing Personal Data*, ARCH (Jan. 2009), http://medconfidential.org/wp-content/uploads/2013/03/Protecting-the-virtual-child.pdf.

72 *See id.*

a more flexible application of legal capacity rules. Obviously, the introduction of the GDPR offered a perfect opportunity to unify the age of majority for the legal capacity of children to consent to online personal data processing across Europe. Remarkably, however, it still allows member states to run their own course in this respect, which means legal diversity in this area may essentially be perpetuated.

In the GDPR, 'consent' is defined as:

> [A]ny freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[73]

The GDPR sets out specific conditions for children's consent in relation to commercial online service providers[74] in article 8.[75] Oddly enough, 'child' is not defined in the GDPR.[76] Although the obvious definition for the word "child" is provided by the UN CRC, omitting the definition from the GDPR is regrettable. With respect to children's consent, the GDPR takes a graduated approach. Children have legal capacity to consent to commercial services offered directly to them when they are at least 16 years old.[77] Below the age of 16, consent must, in those instances, be given or authorized by the holder of parental responsibility over the child. Member states, however, have the possibility to set a lower age for the legal capacity of children to consent to personal data processing, as long as the age is not below 13 years old.[78] Both in the original proposal of the European Commission and the one that was adopted by the European Parliament, the age was set at 13 years old. However, the council then chose to leave it to EU or national laws to determine the age for the legal capacity of minors to consent to personal data processing.

---

[73] GDPR *supra* note 41, art. 4(11), at 34; *see also* GDPR *supra* note 41, art. 7, at 37 (identifying the conditions for consent); *see also* Schermer et. al., *supra note* 37 (on the requirements for valid consent). *See also infra* Section IV.4.1 (further elaborating on the conditions).

[74] Or 'information society services' as they are commonly called in EU law. *See* GDPR *supra* note 41, art. 4(25), at 35.

[75] GDPR *supra* note 41, art. 8, at 37.

[76] An earlier draft of the GDPR did, however, define a 'child' as any person below the age of 18 years. It is unclear why the definition has later been omitted, but it might be due to differences between the legal systems of the member states. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)*, at 43, COM (2012) 11 final (Jan. 25, 2012). *See also* GDPR, *supra* note 41, art. 4, at 33.

[77] GDPR, *supra* note 41, art. 8(1), at 37.

[78] *Id.*

Hence, the provision in the final version of the GDPR clearly appears to be a compromise that came out of the trilogue between Parliament and Council.[79] Consequently, age differences in the EU might unfortunately continue to exist.

III. RIGHTS-BASED ANALYSIS OF CHILDREN'S CONSENT

A. THE RIGHTS-BASED APPROACH UNDER THE UN CRC

The adoption of the UN Convention on the Rights of the Child in November 1989 signified a paradigm shift from a welfare-based approach towards a rights-based approach with respect to children. Children have long been treated as the objects of adult protection rather than as the subjects of (human) rights and the UN CRC has not only put forward a holistic rights-based approach, but, in doing so, also has given children a voice and, therefore, a confirmed—albeit still a minor—position in society. The recognition of children as rights holders in and of themselves—rather than "mere" persons in need of protection through child-specific measures—forms the foundational rationale of the UN CRC.[80]

The rights-based approach is particularly rooted in the general principles of the CRC, the purpose of which is to guide the interpretation of the rights of the child in particular situations. The next section will briefly set out these principles. Subsequently, Section IV.3. introduces the three conceptual lenses that more specifically embody this rights-based approach, and will be used as analytical frames for exploring children's consent in light of the challenges posed by the digital world.

---

[79] A trilogue is an informal negotiation between representatives of the European Parliament and the European Council of Ministers with the aim of reaching an overall agreement on any differences that have arisen between Parliament and Council during the legislative procedure. *See* Fabio Franchino & Camilla Mariotto, *Explaining Negotiations in the Conciliation Committee*, 14 EUR. UNION POL. 345, 348 (2013).

[80] TON LIEFAARD, DEPRIVATION OF LIBERTY OF CHILDREN IN LIGHT OF INTERNATIONAL HUMAN RIGHTS LAW AND STANDARDS 28 (2008).

B. GENERAL PRINCIPLES

The UN CRC is based on four fundamental principles that are distinguished as such by the UN Committee on the Rights of the Child,[81] and must be taken into account in the interpretation and the implementation of the (other) rights of the child.[82] These four pillars are the principle of non-discrimination (article 2), the right to life and development (article 6), the right to be heard (article 12) and the best interest of the child (article 3).

The principle of *non-discrimination* entails an obligation for State Parties to "respect and ensure the rights set forth in the convention to each child within their jurisdiction without discrimination of any kind."[83] The principle does not imply that all children need to be treated identically.[84] Indeed, different cases may require different remedies to fulfill the rights of a child. For example, children that for particular reasons are more vulnerable to online risks than others, may need more care and support than children of a similar age that are better capable to navigate the intricacies of the digital world. Hence, state parties must "identify individual children and groups of children the recognition and realization of whose rights may demand special measures."[85]

Still, however, the same rights would apply to each of them and their specific situations—albeit with likely different implementations. Corporate surveillance that is augmented by datafication and hyperconnectivity (see Part I) unmistakably touches upon issues of (non-)discrimination, given that the—invisible—underlying processes of data processing and knowledge creation enable social sorting, i.e. systematically categorizing and classifying individuals for purposes of identification or risk assessment.[86] Social sorting can create and reinforce social differences, for instance, by excluding the economically deprived from commercial services or by targeting certain minority groups in society

---

[81] *See* Comm. on the Rights of the Child, General Comment No. 5 (2003) on General Measures of Implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, para. 6), ¶12, U.N. Doc. CRC/GC/2003/5 (Nov. 27, 2003).

[82] LIEFAARD, *supra* note 80, at 69.

[83] Comm. on the Rights of the Child, *supra* note 81, at ¶12.

[84] Both the principles of interpretation laid down in articles 3(1) and 5 UN CRC allow room for diversity. *See* Convention on the Rights of the Child, *supra* note 2, at arts. 3(1), 5.

[85] Comm. on the Rights of the Child, *supra* note 81, at ¶12.

[86] DAVID LYON, SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND AUTOMATED DISCRIMINATION (2002) [hereinafter LYON, SURVEILLANCE AS SOCIAL SORTING]; DAVID LYON, SURVEILLANCE AFTER SNOWDEN (2015) [hereinafter LYON, SURVEILLANCE AFTER SNOWDEN].

with heightened police or intelligence monitoring.[87] Undoubtedly, social sorting can have an effect on children's lives, either directly, when children are at risk or perceived as risks to society,[88] or indirectly through their parents or others close to them as well.

The child's *right to life*[89] puts forward an obligation of state parties to guarantee, amongst others, a child's optimal development. A term that according to the CRC Committee, must be "interpret[ed] in its broadest sense as a holistic concept, embracing the child's physical, mental, spiritual, moral, psychological and social development."[90] Personal development arguably also includes the right to (informational) self-determination (or control over personal information that constructs and determines their (digital) identities) and, hence, is related to the right to privacy. Interestingly enough, in their seminal article, Warren and Brandeis have connected the right to life to their conception of privacy stating, "[N]ow the right to life has come to mean the right to enjoy life—the right to be let alone."[91] Still other conceptions of privacy have an impact on the development of a child's self or personal identity by allowing them the freedom to manage (limit or allow) access to the self which, for instance, allows children to create their own spaces in which their thoughts, opinions and identities can unfold without the prying eyes of their parents or others.[92] The right to privacy, however, also encompasses the right to protection of the integrity of personality, both in terms of respecting a person's individuality and reputation,[93] as well as acknowledging and respecting their capacity to choose (to decide or act in a certain way) for themselves.[94] Moreover, privacy allows children to have social relationships of different natures by being more intimate with some than others, which can again be conducive to both the construction

---

87 *See* LYON, SURVEILLANCE AS SOCIAL SORTING, *supra* note 86.

88 Van der Hof & Keymolen, *supra* note 35 at 320.

89 The right to live encompasses survival and healthy development and, therefore, denotes more than the right to live as such. *See* Convention on the Rights of the Child, *supra* note 2, at art. 6; *see also* discussion on development *infra* Section IV.3.

90 Comm. on the Rights of the Child, *supra* note 81, at ¶12.

91 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

92 *See* SOLOVE, *supra* note 43, at 79, 99.

93 *See* Convention on the Rights of the Child, *supra* note 2, at art. 16.

94 *See* SOLOVE, *supra* note 43, at 85.

and expression of a child's identity.[95] For example, privacy (or private spaces) are paramount to the evolving sexual identity of children.[96]

The child's *right to be heard* not only includes a substantive right of children who are capable of forming views to express those views freely, but also acknowledges that the views of children must be taken into account for decision-making to be in line with the UN CRC.[97] The right to be heard underlies children's participation in their decision-making and a free and open society more generally. Relatedly, the right to be heard is intrinsically connected to the right to privacy, given that the protection of privacy creates a space for individuals to read, think, and discuss ideas without any form of (corporate, government or any other form of) surveillance. This is what Richards calls intellectual privacy,[98] a conception of privacy which has become imperative—and increasingly less obvious—in the age of digital surveillance, given that before: "The state, market, and our social contacts could not monitor our thoughts, our reading habits, and our private conversations, at least not in an efficient, comprehensive, and unobtrusive way."[99]

Clearly, all that has changed in today's world. Moreover, the right to be heard evidently is much related to the right to life and development, given that they can mutually reinforce each other.

Finally, the *best interest of the child* forms one of the fundamental values of the UN CRC enshrined particularly in article 3, which states, "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*"* (article 3).

The principle is held deliberately vague in the Convention—and no definition has been given in the UN CRC—in order to allow for diversified and tailor-made implementations of the concept.[100] As the CRC Committee states in its General Comment dedicated to this principle:

---

[95] *See* SOLOVE, *supra* note 43, at 85.

[96] Alisdair A. Gillespie, *Adolescents, Sexting and Human Rights*, 13 HUM. RTS. L. REV. 623, 624–25 (2013).

[97] AISLING PARKES, CHILDREN AND INTERNATIONAL HUMAN RIGHTS LAW: THE RIGHT OF THE CHILD TO BE HEARD 2 (2013).

[98] NEIL M. RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); *See also* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393 (2014).

[99] RICHARDS, *supra* note 98, at 96.

[100] Karin Arts, *Twenty-Five Years of the United Nations Convention on the Rights of the Child: Achievements and Challenges*, 61 NETH. INT'L L. REV. 267, 279 (2014).

> The concept of the child's best interests is complex and its content must be determined on a case-by-case basis. . . . Accordingly, the concept of the child's best interests is flexible and adaptable. It should be adjusted and defined on an individual basis, according to the specific situation of the child or children concerned, taking into consideration their personal context, situation and needs.[101]

Consequently, the best interest principle is flexible enough to adjust to novel developments, but at the same time provides little guidance on how to ensure children's best interests in particular situations. Therefore, it is at risk of being easily neglected, overlooked, or outright ignored, particularly in a digital reality that is characterized by other—notably commercial and government—interests that are much more powerful and run counter to the interests of children. What is more, online child protection measures can be perceived as "covert efforts to promote the state's power to survey, censor, or even criminalize private citizens' acts" and, hence, might be considered unfavorably.[102]

C. THREE CONCEPTUAL FRAMEWORKS: PROTECTION, EMANCIPATION AND PARTICIPATION, AND DEVELOPMENT

The rights-based approach of the UN CRC provides a fundamental basis when applied rigorously to any measure or action concerning a child. This approach as encapsulated by the four fundamental pillars of the CRC is embedded in the conceptual frameworks of development, participation or emancipation, and protection.[103] These frameworks will be used as the lenses for the further analysis of children's consent in order to ensure a balanced approach towards addressing data protection issues involving children. This section will briefly introduce each of these frameworks.

First, *protection* is an important objective of the UN CRC in light of children's vulnerable position in society. Although children's rights law has shifted from taking a needs-based approach to a rights-based approach with the adoption of the UN CRC, protecting children

---

[101] 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).

[102] Sonia Livingstone & Brian O'Neill, *Children's Rights Online: Challenges, Dilemmas, and Emerging Directions*, *in* MINDING MINORS WANDERING THE WEB 19, 21 (Simone van der Hof et al. eds., 2014).

[103] *See* GERISON LANSDOWN, UNICEF INNOCENTI RES. CTR., THE EVOLVING CAPACITIES OF THE CHILD 15 (2005), http://unicef-irc.org/publications/pdf/evolving-eng.pdf.

against harm naturally is still an essential objective of the Convention and its Optional Protocols.[104] Children are recognized as rights holders, yet the UN CRC also acknowledges that children are human beings in development that may have special needs given their lack of experience and maturity. Article 19 of the UN CRC provides more generally:

> States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.[105]

More specific protective rights are laid down in other provisions of the UN CRC.[106] Although generally seen as a participation right, the child right to privacy also provides a protection right to children. Article 16 provides:

> 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
>
> 2. The child has the right to the protection of the law against such interference or attacks.[107]

Moreover, the UN CRC recognizes a protection right with respect to the economic exploitation of children, which might be relevant in light of the commercialization tendency describes previously (see section II.3.). Article 32 (1) provides:

> States Parties recognize the right of the child to be protected from economic exploitation and from performing any work that is likely to be hazardous or to interfere with the child's education, or to be harmful to the child's health or physical, mental, spiritual, moral or social development.[108]

---

[104] See United Nations, Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, preamble, opened for signature May 25, 2000, T.I.A.S. No. 13094, 2173 U.N.T.S 236 (entered into force Feb. 12 2002); United Nations, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, preamble, opened for signature May 25, 2000, T.I.A.S. No. 13095, 2171 U.N.T.S. 247 (entered into force on Jan. 18, 2002).

[105] Convention on the Rights of the Child, *supra* note 2, at art. 19.

[106] *See* Convention on the Rights of the Child, *supra* note 2, at arts. 32, 37, 38, 40.

[107] Convention on the Rights of the Child, *supra* note 2, at art. 16.

[108] Convention on the Rights of the Child, *supra* note 2, at art. 32(1).

Although the article focuses particularly on child labor, treating children as the product rather than the customer[109] when offering them online services can arguably be perceived as a form of economic exploitation as well.

Second, *emancipation and participation* entail respecting children's rights in order for them to develop their capacities and grow up to be fully competent and responsible adults. Emancipation more particularly denotes "the act or fact of gaining equal rights or full social or economic opportunities for a particular group."[110] Participation signifies the fact of taking part or being part of something. Clearly, emancipation and participation are mutually reinforcing. Allowing children to develop their capacities by having their own space in which to enjoy their rights and freedoms creates more and more opportunities for participation in social life. Therefore, by taking those chances children are becoming wiser and more capable of performing actions autonomously. While growing up, children surely but slowly gain more freedom to exercise their rights independently until at the age of majority when the law recognizes them as fully capable natural persons. The UN CRC recognizes the importance of emancipation and participation most notably in the right to be heard, as one of the general principles of the UN CRC. Furthermore and as already elaborated in the previous section, recognizing the children's right to privacy and other (related) rights, such as the right to information and the right to play, substantially contributes to the emancipation and participation of children in society, and increasingly happens in a world constructed and mediated by digital technologies.

Third, pursuant to the UN CRC, the optimal *development* of children—in view of their evolving personal autonomy and capacities—must be supported by providing them with the basic needs that will fulfill their rights.[111] Most notably, a significant part of childhood must be dedicated to providing education to children for them to gradually become self-sufficient, independent, and self-reliant. Importantly, development must not just focus on specific children's spaces, such as playgrounds,

---

[109] Based on the phrase "If you're not paying for it, you're the product" that is often used in relation to free social media, such as Facebook, LinkedIn, Google and Twitter, the business models of which basically entail capitalizing on the user's personal data. *See* blue_beetle, Comment to *User-Driven Discontent*, METAFILTER (Aug. 26, 2010, 1:41 PM), http://www.metafilter.com/95152/Userdriven-discontent#3256046.

[110] *Liberation*, DICTIONARY.COM, http://www.dictionary.com/browse/liberation (last visited Oct. 20, 2016).

[111] LANSDOWN, *supra* note 103, at 15.

and their relations with other children, but should also factor in navigating broader (offline and online) environments and relations with adults (and others).[112] Developing spaces for children online is particularly important, given that the digital world is inherently focused on grown-up users and dominated by other interests than those of children—if at all recognized—as well as values that do not necessarily align with children's rights. Consequently, "real" children's spaces are increasingly disappearing when their worlds become progressively technologically mediated, which brings about new and difficult challenges to the optimized development of children.

Each of the three conceptual frameworks must be considered in light of the evolving capacities of the child.[113] The protective framework is actually based on these evolving capacities, considering that children might need protection because they are still humans in development and, hence, vulnerable in particular ways. However, it also takes note of the fact that children are indeed maturing while growing up and, therefore, the levels of protection can be different at various ages. Moreover, emancipation and participation rights need to be respected increasingly more while children are becoming older and wiser, entailing also that parents need to take a step—or several ones—back and give their children space to decide for themselves. Finally, the development perspective should ensure that children are provided the knowledge and instruments to strengthen their position in society, both in childhood and emerging adulthood, so they can truly flourish as human beings—now and in the future. In conclusion, all three frameworks—although essential in and of themselves—are mutually dependent (i.e. providing a comprehensive approach) and dynamically constituted subject to particular circumstances and developments in children's lives and society more generally.

D. RIGHTS-BASED APPROACH AND CHILDREN'S CONSENT IN DATA PROTECTION LAW

This section now turns to the rights-based analysis of the children's and parental consent provisions, as have been put forward by COPPA and GDPR (see section III.3.). The three conceptual lenses set out in the previous section will be used to perform that analysis: first the

---

[112] LANSDOWN, *supra* note 103, at 19.
[113] LANSDOWN, *supra* note 103, at 15.

conceptual lens of protection, second emancipation and participation, and finally development.

1. First conceptual lens — Protection

Protection of children is the rationale for parental consent provisions in data protection law. Datafication—i.e. the collection, processing, and use of exponentially increasing amounts of data—impacts adults and children in similar ways. Moreover, data processing practices often entail manipulative and evocative methods that can be hard to see through for individuals. Children are perceived as particularly vulnerable in light of these developments and practices.[114] The GDPR thus states:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.[115]

The questions raised by the parental consent provisions in terms of protection are twofold. First, are children indeed more vulnerable, given the data processing practices on the internet and the suggestive strategies used by businesses? Second, is the assumption that parents are more capable of making decisions than their children a fair one? The next two sections will address both these questions to determine whether COPPA and GDPR, in fact, achieve their purposes of adequately protecting children.

a. First assumption: children are vulnerable

Children are recognized as rights holders under human rights law, yet also have a distinctive position given that they are not yet fully developed and matured. In other words, they may be vulnerable in ways that adults are not and, therefore, protection that is specifically focused

---

[114] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, MODERNISIERUNG *DES* DATENSCHUTZRECHTS [MODERNIZATION OF PRIVACY LAW], BUNDESMINISTERIUMS DES INNERN [FED. MINISTRY OF THE INTERIOR] 95 (2001), http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile.=publicationFile.

[115] GDPR, *supra* note 41, at 7.

on children is legitimate or even imperative. The age at which children are deemed competent can vary widely as a result of the economic, social, and cultural circumstances in which children live. Moreover, there are different, competing theories in developmental psychology about the development of children and their capacities.[116] What is important here is to find out whether there is any evidence on the extent to which children are (not) competent to consent to the processing of personal data, and whether this is in line with the rules adopted by the COPPA and the GDPR. Taking COPPA as an example: is there a magical switch in the child's brain that turns him or her into a competent person to consent at the age of 13? Indeed, adolescence is seen as a period in the child's development, starting at age twelve, in which the general cognitive capabilities improve and become on a par with those of adults. As Hamilton states: "General cognitive capacity—i.e., the abilities to process information, understand and reason from facts, and assess and appreciate the nature of a given situation—improves into mid-adolescence. By age sixteen, these basic cognitive abilities are mature."[117]

Despite their cognitive capabilities and depending on the context in which they need to make decisions, however, adolescents are still more likely to engage in irrational and risky behavior compared to adults. Adolescents tend to put more weight on benefits than risks and are more inclined to make *bad* decisions in situations that are "emotionally charged and pressured", and take well into their twenties to fully mature, socially and emotionally.[118]

Decisions on consenting to personal data processing practices, for instance when opening a social media account or downloading an app, are not likely to be *emotionally charged* or subject to peer pressure,[119] and, therefore, children from 12 years on (or even younger) may be able to make competent decisions if they are genuinely and fully informed about what is at stake. Children's decision-making competence

---

[116] LANSDOWN, *supra* note 103, at 16.

[117] Vivian E. Hamilton, *Immature Citizens and the State*, 2010 BYU L. REV. 1055, 1109 (2010).

[118] *Id.* at 1110, 1118.

[119] Peer pressure can of course play a role in the decision to sign up for online services. *See* Andrew Watts, *A Teenager's View on Social Media*, BACKCHANNEL (Jan. 2, 2015), https://backchannel.com/a-teenagers-view-on-social-media-1df945c09ac6 ("[I]f you don't have Facebook, that's . . . weird. . . . Weird because of the social pressure behind the question, 'Everyone has Facebook, why don't you?'"); *see also* Grace C. Huang et al., *The Interplay of Friendship Networks and Social Networking Sites: Longitudinal Analysis of Selection and Influence Effects on Adolescent Smoking and Alcohol Use*, 104 AM. J. PUB. HEALTH 51, 57 (2014) (discussing the impact of social media on smoking and alcohol use).

tends to be underestimated and cannot be assessed properly without having a close look at their everyday lives. Although these are exceptional events, young children are found to be capable of making difficult medical decisions, some of them including matters of life and death.[120]

However, the capacity to consent to online data processing practices cannot be considered independent of the child's understanding of the underlying commercial interests and calculating processes, and the immediate or future consequences thereof for their lives. As Montgomery observes:

> Most users, who are focused on their social experiences in the online environment, are likely to remain largely uninformed about the nature and extent of commercial surveillance on social networking platforms. These practices have already been woven inextricably into the fabric of the new media culture, operating with very little transparency or public accountability. The breadth and depth of information currently generated through these new data collection and measurement tools are unprecedented, and promise to become even more extensive in the near future. . . . Though young people possess the tools and skills for navigating the social media environment, they lack some of the critical capacities needed for responding effectively to the marketing and data collection apparatus. In the highly commercialized social media landscape, the very features that resonate so strongly with adolescent needs—for identity, peer relationships, and autonomy—also expose them to techniques that may be particularly manipulative and unfair to this age group.[121]

Although we might stretch her observations beyond adolescence (see the next section), it is likely to be true that most of the intricacies and impact of data processing practices are beyond their comprehension because they are—technologically, economically, and socially—complex, not intended to be conspicuous and—at least as far as the consequences are concerned—not readily obvious or—as yet—even unknown. A study involving Dutch, Greek, and Polish teens between the ages of 11-18 found that a majority had never heard of online profiling, as a result of which they were not able to form a solid opinion on whether online profiling was something positive or negative.[122]

---

[120] Priscilla Alderson, *Young Children's Health Care Rights and Consent*, *in* THE NEW HANDBOOK OF CHILDREN'S RIGHTS, COMPARATIVE POLICY AND PRACTICE, 155, 158 (Bob Franklin ed., 2nd ed. 2002).

[121] Kathryn C. Montgomery, *Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications*, 39 TELECOMM. POL'Y 771, 777 (2015).

[122] Simone van der Hof, *Online Profiling of Children in Europe a legal perspective*, *in* DYNAMIC IDENTITY WORKSHOP 156 (2015).

b. Second assumption: parents are more capable of making decisions

The notion of consent is essential as a legal instrument in today's data-intensive digital world in order for individuals to retain control over their data and, hence, their "onlives." Consent as a legal instrument to protect and empower individuals, however, is proving increasingly problematic, and, consequently, questions about the (lack of) effectiveness and fairness of consent as a legal instrument are being raised.[123] There are several reasons why consent is severely challenged as an effective legal concept in today's digital society, as a result of which it is doubtful that parents are actually more capable of making decisions that pertain to personal data practices than their children.

In order to be able to adequately exercise the power to consent to data processing practices and ensure consent is legitimately given, consent needs to fulfill a number of essential requirements.[124] These requirements can also be found in the definition of consent in the GDPR: "[A]ny freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[125]

This definition consists of components that need to safeguard the rights of the individual and ensure that the transformation of conduct from unlawful to lawful happens in a legally acceptable manner. Consent must be *freely given*, signifying the autonomous position of the individual in the context of personal data processing. Freely given contains an element of choice; either choosing to have personal data processed or not or choosing the conditions for such processing. Obviously, mostly there is no choice, other than to opt for *not* using an app or service, given that privacy policies are based on a take-it-or-leave-it basis. Parents and children might have the option to tweak their privacy settings but those changes normally do not affect the default position of corporate surveillance. Consent must be *specific*, which entails parents saying "yes" to clearly defined actions.[126] In order to be able to do so, however, parents

---

[123] *See* Schermer et al., *supra* note 37, at 172.
[124] Schermer et al., *supra* note 37, at 132.
[125] *See* GDPR, *supra* note 41, art. 4(11).
[126] Schermer et al., *supra* note 37 at 173–74.

clearly need to have substantial *information* about the details of data processing practices.

For several reasons, parents are likely to lack such information and, hence, consent is seldom specific. Research shows that people mostly do not read privacy policies.[127] People find them too complicated or too long to read.[128] Reading them might not be convenient at the moment of downloading an app or signing up for an online service. Privacy policies are generally not very appropriate for small screens. And about 40% of the apps do not have a privacy policy.[129] Even if parents did read them, they might be none the wiser, given that data processing practices are often disclosed in rather vague terms. Moreover, the processes behind the screen are complicated and intentionally opaque, bringing us back to the notion of 'invisible visibility.' Not only are the processes by which individuals become transparent opaque, big data companies do not necessarily have an interest in making those processes more transparent as it would undermine their strategies of consumer manipulation (see section II.3). Such strategies might, however, be exactly what consumers want to know before deciding on whether to use an app or online service. This is also implied by the findings from a recent study into the privacy and information involving US adults.[130] In this study, respondents have shared their concerns about third-party data sharing of companies, the use of personal data for ambiguous and invasive purposes, and data security.[131] Respondents also labeled profiling as 'creepy,' 'stalking,' and 'big brother.'[132] Finally, consent must be *unambiguous*, which means that parents must overtly act to consent (for example, clicking the box saying "confirm") or at least consent must be inferred from their actions (for ex-

---

[127] *See* Irene Pollach, *What's Wrong with Online Privacy Policies?*, 50 COMM. OF THE ACM 9, 103–08 (2007). *See also* Daniel J. Solove, *Privacy Self-management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884 (2013).

[128] *See* Pollach, *supra* note 127, at 104.

[129] John Koetsier, *40% of Top-selling Smartphone Apps Have No Privacy Policy*, FORBES (Mar. 24,2016) http://www.forbes.com/sites/johnkoetsier/2016/03/24/40-of-top-selling-smartphone-apps-have-no-privacy-policy/#38dce4705005.

[130] *See* Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, PEW RESEARCH CENTER (Jan. 2016) http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[131] *Id.*

[132] *Id;* Concerns with respect to personal data sharing are often phrased in terms of privacy, however, it is also important to see the bigger picture, which also includes issues of non-discrimination, freedom of expression, freedom of information, and autonomy. *See e.g.*, Bart H. M. Custers, Toon Calders, Bart W. Schermer & Tal Zarsky, *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases*, 3 STUD. IN APPLIED PHIL., EPISTEMOLOGY AND RATIONAL ETHICS (2013); Richards, *supra* note 98.

ample, clicking through after a message saying "your name and e-mail address will be stored" is displayed). Obviously, it is questionable whether the act by which consent is given, which in itself can indeed be unambiguous, actually amounts to consent as a normatively transformative action.[133]

2. Second conceptual lens — Emancipation and participation

Where protection has been at the forefront of the children's and parental consent provisions in COPPA and the GDPR, emancipation and participation are implicitly factored in through recognizing the evolving capacities of children under 18. The principles of the evolving capacities and the best interest of the child, however, denote that values of freedom and autonomy must be meticulously balanced with their need for protection against risk and harm. Admittedly, the interpretation of these principles is not an easy matter and depends very much on the circumstances of a situation as well as concrete weight attached to each of the interests involved in the balancing act. Nonetheless, explicitly focusing on what is actually in the best interest of the child (as opposed to the interests of others) adds interesting perspectives to the equation that may otherwise be omitted.

From a participation and emancipation perspective, the parental consent provisions in COPPA and the GDPR can, remarkably enough, be perceived as rather problematic in terms of the privacy rights of children. The paternalistic approach underlying these provisions raises tensions between parents and children in terms of securing private spaces unbeknownst to parents. Social media are, for instance, not only a venue for teens to socialize with their peers but also to escape from their parents.[134] One of the meanings of privacy for children entails having privacy from their parents or—in other words—absence from parents, which is a condition that already surfaces in younger children well before they become teens.[135] The problem with COPPA and the GDPR is, however, that the scope of these laws is restricted in two important ways that can negative-

---

[133] *See* Schermer et al., *supra* note 37.

[134] danah boyd, Taken Out of Context: American Teen Sociality in Networked Publics (Ph.D. dissertation, University of California-Berkeley) 12 (2008), http://www.danah.org/papers/TakenOutOfContext.pdf; DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS (2014).

[135] Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759 (2011).

ly impact the privacy of children in relation to their parents. First, these laws apply only to the relations between individuals and organizations (such as companies) and interpersonal relationships—such as between parents and children—are exempted from or at least not included in their application.[136] Second, these laws regulate *control over* personal information and not the privacy implications of *access to* the lives of children, which can be effected by giving parents control over their children's personal data.[137] What is more, parental consent requirements might actually generate or encourage over-extensive parental surveillance.[138] These legal confinements, therefore, paradoxically engender a lack of suitably recognizing children's rights in order to protect their rights. In the GDPR, the potentially sensitive relationship between parent and child may have been a consideration in making an exemption to the parental consent rule *in the context of preventive or counselling services offered directly to a child*.[139] This exemption is mentioned only in the considerations of the Regulation, yet has not found its way to the actual provisions, most notably article 8, of the GDPR, which makes its status uncertain. Arguably though, the exemption does not in any way seem relevant to children's "onlives" as discussed here and hence, it is doubtful whether privacy *from* parents has been part of the considerations when drafting the provision. Moreover, recognizing the evolving capacities of the child in setting age limits in both COPPA and GDPR may imply a sensitivity to the child's right to privacy *vis a vis* their parents. Instead of being concerned with privacy breaches within parent-child relations, however, this recognition also acknowledges the increasing maturity of the child while it grows up and of the child's ability to make his or her own decisions from a certain age.

Moreover, some might argue that parental consent does not necessarily entail parental access to children's "onlives" and, hence, emancipation and participation rights can still be exercised outside parental scrutiny. After parental consent has been given to the online service provider, children can move on by themselves on online platforms they have signed up to. Privacy from parents, however, also entails being able to go places your parents don't know about and requiring parents to say OK at

---

[136] *See* 16 C.F.R. § 312 (2012); *see also* GDPR, *supra* 41, at art. 2(c).

[137] *See generally* Shmueli & Blecher-Prigat, *supra* note 136 (making a full distinction).

[138] Simone van def Hof, *No Child's Play: Online Data Protection for Children, in* MINDING MINORS WANDERING THE WEB: REGULATING ONLINE CHILD SAFETY 127 (Simone van der Hof et al. eds., 2014).

[139] *See* GDPR, *supra* 41, at 9.

every entrance point of a digital space children want to enter potentially increases parental surveillance and essentially violates their emancipation rights. What is more, parents might even install a password for the child and have access to the account at any point in time. In reality, children can obviously easily work around all this by not even involving parents when signing up for an online service, since most online service providers do not check whether parental consent is necessary or provided.[140] But the point is that this should nonetheless have been taken into consideration when drafting these rules. Online service providers' practices may not stay this lenient or indifferent, when the stakes—e.g. through stronger enforcement of the rules—are getting higher.

3. Third conceptual lens — Development

The development perspective denotes that children must be provided with the basic necessities to allow them to optimally flourish and grow into self-sufficient, independent, and self-reliant individuals. Growing up in modern society demands new and more sophisticated skills as a consequence of the tendencies of datafication, hyperconnectivity, and commercialization described previously. Such proficiency is also a prerequisite to adequately and fairly exercise the capacity to consent to the extent possible given the fact that exercising autonomy in a data-intense world is innately problematic nowadays. Both COPPA and the GDPR contain provisions on notification and information disclosure, requiring online service providers to communicate their data processing practices with respect to children in a clear, understandable, and unambiguous manner.[141] In section IV.4.1., however, we have seen that information disclosure requirements do not (adequately) instruct internet users on the commercial (or other) data processing practices, and, hence, is one of the causes for why consent as a legal requirement in privacy and data protection law fails entirely in effectively protecting them.

Notwithstanding other difficulties with consent, *informed* consent would *at least* call for profound and comprehensive tutoring and coaching children *and* their parents in understanding and navigating the tendencies of datafication, hyperconnectivity, and commercialization,

---

[140] Instead, US online services providers prohibit children under 13 (the age set by COPP) to access their online services, as a result of which children lie about their age in order to open an account anyway. *See* Madden et al., PEW RESEARCH CENTER, *Teens, Social Media, & Privacy*, 76-77 (2013).

[141] *See* 16 C.F.R. § 312.4; GDPR, *supra* note 41, at art. 12.

their, actual and potential, impact on them as individuals and society more in general, and the instruments available to take—in as far possible—alternative routes in their onlives from the ones that are economically dictated. In other words, children must be challenged to reflect on what it means to be a digital citizen and consumer, how internet governance and economics operate and, thus, influence society, and how to make fair and versed decisions that are in line with your thoughts, beliefs and sentiments, and ensure protection of your rights. The digital world is a different world with a dynamic of its own, and unless you have some understanding of what it means to live in it, you won't be able to take matters in your own hands or, at least, grasp the consequences of your choices. In their report, the Canadian Public Interest Advocacy Centre asserts:

> [We] found that most children found it necessary to limit providing their private information online to other individuals, but these same participants did not perceive there to be many potential risks associated with providing personal information in public online spaces or to website administrators or corporations they consider to be safe, such as Facebook, Webkinz and YouTube. Children and teenagers appear to see the online world as an extension of the offline world, rather than a separate space with different rules.[142]

Moreover, digital citizenship is so much more than understanding how to push the right buttons. Much emphasis is currently put on teaching children to code, which certainly has great merits in showing them that the digital world is not set in stone and can be manipulated and designed differently depending on your preferences, values, or interests. At some point, however, tinkering with technology must be associated with external, social, and economical, effects that greatly determine technological innovation and human lives. This is a daunting task to be sure and entails recalibrating what constitutes optimal development in a world more and more dominantly mediated by technology.

IV. CONCLUSION

This article has set out to scrutinize the protection offered to children under the rules on children's consent in the United States and the European Union privacy and data protection law in light of the rights-

---

[142] PUBLIC INTEREST ADVOCACY CENTRE, *Submission to the Government Consultation on A Digital Economy Strategy for Canada* (July 2010), http://www.combattrelepourriel.gc.ca/eic/site/028.nsf/eng/00217*1.html#p3.2.3*.

based approach of the UN CRC. The analysis shows that not only are children not properly protected under these provisions, but also the rules actually clash with other children's rights. Basically, two overall problems can be identified that need to be addressed in order to establish an adequate legal framework that, on the one hand, does justice to fundamental rights and values, and, on the other hand, can realistically provide protection of these rights and values.

First, the holistic nature of children's rights demands that other perspectives are factored in when implementing protective mechanisms in the law. Obviously, protecting children and their personal data is increasingly more important in modern society; however, privacy and data protection law loses sight of the importance of emancipation, participation and the development of children to find a healthy balance with respect to the protection paradigm. A too paternalistic approach can curtail children's participation and emancipation rights in unfair ways. Parents definitely have important roles in guiding children, including the responsibility of raising awareness of the challenges of the internet and shielding them from online harm. Even so, new technologies also have a tendency to raise irrational fears and concerns—what are called technopanics[143]—that can lead to overprotective measures by parents, which unnecessarily reduce children's opportunities for online participation, effecting their right to be heard, their right to play, and their rights to information and association. Furthermore, their right to privacy calls for the recognition of having private spaces away from or unbeknownst to parents. Involving parents in children's entrance to the digital world through privacy and data protection laws essentially contradicts such a right and negatively impacts its practical implementation. Moreover, by failing to effectively take into account the development paradigm, children are deprived of the knowledge and instruments to grasp what it means to live in an increasingly data-intense, hyperconnected, and commercialized world and how that world can be navigated according to their preferences, values, and beliefs. Development rights—even if implemented in a meaningful way—are not likely to resolve the current deficiencies in privacy and data protection law, but to some degree give children a more empowered position to cope with the intricacies of digital society. More generally, we might even question whether the ages set

---

[143] Adam Thierer, *A Framework for Responding to Online Safety Risks*, *in* 24 Minding minors wandering the web: Regulating online child safety Information technology & law (Simone van der Hof et al., eds., 2014).

by privacy and data protection law are in keeping with the actual capacities of children as compared to adults. Based on developmental psychology theories, children under 13 (COPPA) or 16 (GDPR) might actually be as capable, or as incapable given the context, as their parents in making decisions about data processing practices, but this is a matter for further research.

Second, the current rules are no testimony to the protection of children's—or anyone else's for that matter—personal data being taken sufficiently seriously. They focus too much on procedural safeguards—notice and consent—to the detriment of a fundamental assessment of data processing practices in terms of fairness. Agency of individuals, including children, remains important in the digital age and much more—or even a different approach—is needed than mere consent and information disclosure to empower them. Obviously, information disclosure rules are an attractive way of regulating for many stakeholders as it is the *path of least resistance*, given that they both support the free market principle and intend to promote consumer autonomy and empowerment.[144] Nonetheless, consent—which typically can be a powerful "tool" in accomplishing self-determination—in the privacy and data protection context only relays the illusion of autonomy because most of what it aims to regulate or achieve is in reality beyond our control. Much of what happens under the hood of digital society and the ways in which it can potentially impact human lives is, oftentimes deliberately, invisible to us and too complicated to understand just like that. Nor can we determine to what extent data processing practices lead to reasonable and legitimate results—or influence them if they do not. The effects of privacy intrusions are usually incremental and the impact may not be readily perceptible.[145] Moreover, the tendencies discussed here do not merely bring about privacy and data protection issues but also implicate other fundamental rights, values, and principles, such as the right to non-discrimination,[146] the right to freedom of expression,[147] the right to per-

---

[144] OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 146 (2016). This is also the underlying rationale of the GDPR which aims to both facilitate the free flow of data and the protection of the rights of individuals. *See generally* GDPR, *supra* note 41.

[145] Solove, *supra* note 43 at 33.

[146] LYON, SURVEILLANCE AS SOCIAL SORTING, *supra* note 86.

[147] *See* Richards, *supra* note 98.

sonal development, the presumption of innocence,[148] the principle of legal certainty, and the principle of contractual freedom.

Although corporate surveillance is currently a default setting in the way many businesses operate, it does not need to be. In the longer term, it might actually turn out to be counterproductive. In the post-Snowden era, more Americans are concerned about their privacy and the loss of control over personal information and are looking for ways to protect themselves.[149] Not just the internet as such but a secure internet may become a basic necessity for individuals, in that it would allow them to interact without being observed by those who are not explicitly invited. Novel decentralized and encryption technologies, such as blockchain might lead the way towards a shift from corporate surveillance towards secure online services that are more in accordance with privacy and other expectations of individuals, both young and old.[150]

---

[148] Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption, How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 70 (2013).

[149] Mary Madden et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (Nov. 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

[150] *See* Wikipedia, *Blockchain (Database)*, https://en.wikipedia.org/wiki/Blockchain_(database) (last visited Oct. 20, 2016). Guy Zyskind, Oz Nathan & Alex Pentland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, *in* IEEE SECURITY AND PRIVACY WORKSHOPS (2015), http://web.media.mit.edu/~guyzys/data/ZNP15.pdf.