Protecting Children's Privacy in the Era of Big Data

Melike Tanberk

Introduction

Defining the concept of privacy has always been a challenging endeavour, given its multifaceted nature and evolving societal norms. However, the emergence of new technological advancements, particularly in the realms of artificial intelligence and big data, has further complicated the task of delineating a precise and well-defined boundary for privacy.

As we explore privacy, it becomes increasingly evident that our contemporary trajectory with technological advances, if left unchecked, threatens to expose not only ourselves but also our children to unprecedented vulnerability. This path lays the groundwork for a future where generations to come may find themselves beset with the pervasive surveillance web of capitalism (Zuboff, 2019), where their autonomy and liberty diminished. In grappling with the Collingridge Dilemma of Control —the control dilemma when the consequences of technological advancements are not yet evident (Genus & Stirling, 2018), we must earnestly examine the potential consequences, even as we consider whether it may already be too late to forestall those who seek to harness the means of constraining humanity and steering us toward dystopian destinations. In this quest, the protection of privacy emerges as an issue as vital as safeguarding our natural environment, a legacy that we must defend for the benefit of our grandchildren and the generations that will follow.

It is essential to consider children's privacy differently from that of adults, as failing to do so could lead to insufficient protective measures against unwanted intrusions. As we elaborate in subsequent sections, privacy is essentially characterised by one's ability to exercise control over one's personal information. However, children, in their developmental stages, are unable to exercise discretion on their privacy due to their limited capacity to differentiate between what is considered private and what is not (GDPR-Info.eu, n.d.; Montgomery et al., 2017; van Manen & Levering, 1996).

The primary goal of this article is to provide a preliminary perspective on the evolving concept of privacy, particularly in the context of children, within the backdrop of the Big Data era and emerging technologies. Subsequently, the discussion explores the methods and

motivations behind how big data threatens children's privacy. It also addresses the potential consequences, such as the erosion of freedom and dignity for future generations, stemming from the widespread influence of the current risks associated with Big Data.
Finally, in the last section, we explore measures that can be implemented with ethical considerations to circumvent the invasion of children's privacy. This perspective recognises privacy as a negative right, particularly in situations involving children who may not be capable of independently asserting their rights.

What is privacy?

The literature offers a rich tapestry of perspectives on the concept of privacy, and these myriad definitions often converge on the notion of having control and discretion as fundamental to privacy. While these general viewpoints draw attention to the intrinsic connection between privacy and human dignity and freedom, they tend to fall short in providing a comprehensive framework for addressing the privacy rights of specific groups such as children, people with special needs/mental infirmities, and even animals. This shortfall primarily stems from the conventional understanding of privacy as a negative right, wherein individuals possess the active agency to control and exercise their privacy. Schoeman (1984, 2010), for example, articulates privacy as a pivotal facet of human dignity, serving as a safeguard against unwarranted intrusion into personal matters. It represents a claimed entitlement or prerogative, empowering individuals to dictate the disclosure of information pertaining to themselves to others. Decew (1986), from another vantage point, highlights privacy as the capacity to assert authority over information within specific domains, thereby reinforcing the element of control. Petersen (1997) adds depth to this discourse by characterising privacy as a boundary control process, accentuating its role in demarcating personal boundaries.

One of the most comprehensive viewpoints on privacy, especially within the context of individuals who may have limited control over their lives, such as children, can be found in the work of Benn and Gaus (1983). They assert that privacy constitutes a central social concept that permeates our perception of the social world and exerts profound and nuanced effects on social life. It emphasises the intricate interplay between individual autonomy, societal norms, and interpersonal relationships, making privacy a cornerstone of our collective human experience.

The concept of the "inviolate personality" (Bloustein, 1964) is commonly associated with negative rights focused on the idea that an individual possesses an inherent and inviolable realm that should remain untouched by external intrusion, it can also be linked to positive human rights. In fact, privacy encompasses both the right to be left alone (negative right) and the right to have one's privacy actively protected and supported (positive right) (Warren and Brandeis, 1890). In that regard, children should hold a negative right to have their personal information safeguarded, and this requires the implementation and enforcement of data protection laws by governing authorities. This protection is vital for ensuring the preservation of their future autonomy and dignity. Because the main driving force for children that is behind the development of self-awareness, which ultimately contributes to the cultivation of dignity, is the exploration of how different facets of privacy shape a child's inner development (Crepax et al.,2022; Holloway, 2019, van Manen & Levering, 1996, p:125).

How and Why Big Data Endangers Children's Privacy

Firstly, the commodification of personal data raises profound ethical questions in the digital age. Data once considered an innocuous byproduct of our online lives, has evolved into a tradable commodity of immense value (Carissa Veliz, 2019; Shoshana Zuboff, 2019). The allure of this data-driven marketplace, however, beckons not only legitimate enterprises but also those with questionable ethical boundaries. The process involves digitising individuals and reducing them to data points and profiles, which are then monetised as currencies in a vast digital ecosystem. This monetisation revolves around the relentless collection and analysis of personal data from individuals (Brey, 2005; Carissa Veliz, 2019; Crepax et al.,2022; Floridi & Taddeo, 2016; Ienca et al., 2018; O'Neill, 2019; Wu, 2017). As we navigate this new landscape, we must grapple with complex ethical dilemmas surrounding children's data being introduced as commodifiable objects. The application of methods tailored for tracking and profiling, coupled with the continuous evolution of IoT technologies and the introduction of interconnected toys known as IoToys, has brought about a transformation where children are now treated as digital commodities that can be exchanged. Most of these surveillance devices are concealed within items resembling toys and online games (Crepax et al., 2022; Montgomery et al., 2017; Holloway, 2019). These nascent

marketing approaches, including data mining (Buckingham, 2011), effectively position children as both specific consumer targets and marketable assets.

Another factor contributing to the erosion of privacy through data collection is the uncertainty surrounding data ownership. Tech companies and governments frequently collect data from individuals without their consent and, in many cases, without their awareness. The ownership of data is often unclear or ambiguous. (Drexl, 2021; Veliz, 2019). This ambiguity creates a potential for it to be utilised without individuals' consent. This can result in significant privacy violations, encompassing the collection, dissemination, or sale of personal information without the data subject's awareness or control (O'Neill, 2020). This, in turn, gives rise to a related issue - trust. The ambiguity regarding data ownership undermines trust in digital systems and the authorities that endorse them, leading to a lack of absolute authority and accountability (Brey, 2005; Floridi & Taddeo, 2016; O'Neill, 2019). Even consent forms regarding data collection exacerbate the problem by being overly complex, with few people taking the time to thoroughly review their contents, thereby worsening the situation of trust (Crepax et al.,2022, Floridi & Taddeo, 2016; Holloway, 2019; O'Neill, 2020; Panayiotou & Protopapadakis, 2022; Schneble et al., 2021; Veliz, 2021).

Furthermore, the concept of 'sharenting' introduces a complex issue where children's rights to their futures are inadvertently compromised by their parents. 'Sharenting' refers to the practice in which parents share photographs and information about their children on social media (Donovan, 2023). Despite some regulatory measures for minors, such as those outlined by GDPR, they may not fully safeguard these vulnerable children from potential risks arising from their parent's actions, often performed without understanding the future consequences. These parents, whether digitally inexperienced or indifferent to the implications, frequently share their children's photos and data across various online platforms (ibid.). Also, there is the "Network Effect, which emphasises that compromising one person's privacy can have a cascading impact on the privacy of others. For instance, consider a scenario where a photograph taken at a party is shared on social media, inadvertently revealing the identities of individuals who may not have given their consent for such exposure. Similarly, genetic data can unveil not only an individual's information but also that of their family members as a network effect (Carissa Veliz, 2019; Floridi & Taddeo, 2016; Roessler & Mokrosinska, 2013).

Children are now undergoing digitisation even before birth, with prenatal scans and the disclosure of various details such as names, house photos, birthdates, hospital names, and potential health risks. Consequently, by the age of two, a child already possesses a substantial

online presence, and in the United States, this phenomenon affects approximately 90% of children (Donovan, 2023; Wilson, 2019). One notable and recent instance involves the admission made by Elaine Kasket's habit of sharenting. Her personal narrative emphasises the crucial connection between respecting a child's privacy and fostering a healthy parent-child relationship in the digital age (2023).

In addition to the practice of sharenting, there exists another significant challenge in the realm of parental protection of children's privacy. This challenge revolves around the notable generational distinction in the responsibility to safeguard privacy. Those entrusted with this vital responsibility are often categorised as 'digital immigrants.' These individuals have had to navigate the swift and constant advancements in technology, finding themselves in a transitional phase as they seek effective solutions to preserve the privacy of those born into the digital era, commonly referred to as 'digital natives.' Prensky (2001) shed light on this generation gap and emphasised the imperative need to bridge this divide. This issue lies in the dynamic and ever-evolving nature of technology. The challenge is particularly daunting for parents who may not possess a high level of technological literacy, further complicating their efforts to protect their children's privacy. Children, being remarkably adaptable to technology, may actively seek ways to circumvent parental controls or screens specifically designed to restrict their access to certain content or applications (ibid.). Their motivations for doing so are diverse and may include a desire to access entertainment, engage with social media platforms, satisfy their natural curiosity about technology, or assert a growing sense of independence.

The greater danger, however, lies in the event that unless we acknowledge childhood as a stage that warrants strong protection against privacy infringements as an intrinsic entitlement through protective actions, there is a risk that their future will be subject to the influence of tech giants who exercise extensive surveillance techniques to accumulate excessive behavioural data, that is 'Behavioural Surplus'.

'Behavioural Surplus' is a term coined by Shoshana Zuboff (2019) that encompasses the vast reservoirs of data generated as a byproduct of individuals' online activities and digital interactions. This surplus data, often produced without users' full awareness and explicit consent, has become a valuable resource for data-driven businesses and tech giants. Organisations leverage behavioural surplus to develop advanced predictive algorithms and gain insights into user behaviour. By applying cutting-edge data analytics and machine learning techniques, they can identify intricate patterns, trends, and correlations within this data. Behavioural surplus represents the most troubling aspect of the Big Data phenomenon,

as it fosters profiling and a gradual shift toward a world where democracy is weakened thereby, technology elites hold unchallenged power, ultimately eroding democracy (Floridi & Taddeo, 2016; Holloway, 2019; Veliz, 2021; O'Neil, 2017, p.93; Vanacker and Heider, 2018; Fukuyama, 2002, p.218; Zuboff, 2019, p.492).

In the context of Big Data analysis, the individual's privacy takes a back seat to the emerging collective patterns and group profiles. This shift in focus aims to revolutionise techniques for large-scale persuasion and influence, often raising ethical and privacy concerns, as in the case of the Cambridge Analytica scandal, which unfolded in 2018 and involved the unauthorised collection of Facebook user data by the political consulting firm Cambridge Analytica. The firm obtained personal information from millions of Facebook users through a quiz app, which violated Facebook's data policies. This data was then used for targeted political advertising during the 2016 US presidential election (Dwoskin and Romm, 2018). The Cambridge Analytica scandal undoubtedly indicated the critical issues surrounding data privacy, digital manipulation, and the subsequent erosion of democratic principles. In this trajectory, the freedom of many hangs in the balance, primarily because they are highly susceptible to manipulation —a vulnerability that is investigated from the behavioural surplus. This shows that despite the presence of regulations such as the General Data Protection Regulation (GDPR) with the protective mechanisms they offer, including data anonymisation, pseudonymisation, and the 'right to be forgotten', it might not provide comprehensive mitigation against data profiling activities. This is especially problematic when confronting novel privacy areas such as genome maps and pedigree data (Taylor et al., 2017; Floridi & Taddeo, 2016; Ienca et al., 2018b). Even when data is collected for valid and advantageous reasons, like enhancing healthcare or responding to disasters, the inherent pervasiveness and susceptibility of Big Data categorise it as a potential risk (Brey, 2005). Entrusting Big Data to responsible hands also cannot ensure its immunity from potential data breaches by malicious actors with harmful motives (O'Neill, 2009; Vanacker, 2018). For these reasons, sensitive data should be handled, with additional protective measures and ethical considerations, to prevent any potential manipulations or misuse.

Finally, the ethical challenges governments face in addressing privacy intrusions, apart from their being relatively novel, can be linked to a shift in ethical paradigms from a duty-centered framework to a rights-based approach, as argued by Onora O'Neill (2020). O'Neill's perspective suggests that the transition to a rights-based framework weakens the effectiveness of both imperfect and perfect duties since they no longer specify claimants, encompassing duties toward future generations. This shift in ethical norms further

complicates the ethical considerations surrounding privacy issues and highlights the need for new approaches to protect individuals in an evolving digital landscape.

Ethical Considerations and Imperative Measures

The central focus of the privacy issue revolves around the need for a thorough and ethical approach. While granting individuals control over their personal data is a form of digital autonomy, it may not be sufficient for children, given their limited understanding of the importance of privacy. Likewise, protective measures like data anonymisation and pseudonymisation, intended to safeguard identities and sensitive information, often fall short due to the ease of deanonymisation and the persistence of profiling within the realm of big data.

Ensuring transparency and holding tech companies and government agencies accountable for their data practices are of paramount importance. Nevertheless, it is important to remember that even stringent legal protections may not fully secure data within the boundaries of existing regulations. The risk of data breaches remains ever-present, whether from foreign attackers or malicious hackers, as previously mentioned, leaving data vulnerable to cyberattacks. Furthermore, it is worth noting that there might be other jurisdictions or individuals who may operate without ethical constraints, extending their reach beyond conventional boundaries.

Promoting awareness emerges as another suggested approach to curb the excesses of surveillance capitalism (Zuboff, 2019; Veliz, 2021). While it does entail the benefit of maintaining privacy by educating the public about their digital rights, its impact is somewhat diminished when applied to children due to their ongoing developmental phases and their parents’ digital illiteracy.

Irreversible data deletion stands out as a viable and efficient means to shield children's privacy, supported by various sources (Angwin, 2014; Moglen, 2010; O'Hara and Shadbolt, 2014; Zuboff, 2019; Veliz, 2021). Given the potential risks of cyberattacks, the permanent removal of data emerges as a vital measure to protect minors' privacy.

As 'digital immigrants,' adults may sometimes be confounded by 'digital natives', who quickly adapt to technological advancements and may seem self-sufficient. However, what minors might not yet grasp is that history often repeats itself cyclically, with privacy

infringements leading to dire consequences for those targeted, resulting in a loss of individual freedom and personal security.

Technological progress, particularly in the domain of digital technology and the internet, has transformed the way people interact and share information, but the fundamental value of privacy remains unaltered. Protecting this essential human right is imperative, as neglecting it could create an opportunity for surveillance capitalism to establish a global Panopticon —a concept, initially formulated by Jeremy Bentham which envisions an institutional facility designed for surveillance and control (Bentham and Boovic, 2011), where surveillance elites would reap the benefits.

Conclusion

Humanity stands at a pivotal moment in history, facing the discovery of AI technology, akin to the discovery of fire, and its fuel is Big Data. As in the case of fire, this technological landscape presents a dual nature, with the potential for both immense benefits and grave drawbacks. The implications of this situation transcend individual incidents or crimes; they reverberate globally. The catastrophic aftermath of this metaphorical wildfire has the capacity to profoundly disrupt the lives of future generations. In order to avert such a perilous outcome, the current generation is responsible for taking proactive measures and guarding against the potential dangers that lie ahead within big data.

To ensure that our children and grandchildren have the opportunity to live lives marked by freedom, a privilege that should be universally available, we must oppose the grip of surveillance capitalism by protecting minors' privacy. Those surveillance capitalists have been constructing tantalising houses made of sweets, treats, and cookies to lure in our Hansels and Gretels. Their sinister goal is to lead children into these attractive traps, put them in cages and exploit them as a means to their ends. It is our duty to protect their right to privacy in this infosphere.

Word Count: 2,999

References:

- Angwin, J. (2014). *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance.* New York: Henry Holt and Company.

- Bentham, J. & Boovic, M. (2011) *The Panopticon writings*. London: Verso.

- Benn, S.I. and Gaus, G.F., 1983. 'The public and the private: concepts and action'. *Public and private in social life*, 3, pp.297-325.

- Bloustein, E.J. (1964) 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York University Law Review*, 39(6), 962-1003.

- Brey, P. (2005). Freedom and privacy in ambient intelligence. *Ethics and Information Technology*, *7*(3), 157–166. https://doi.org/10.1007/s10676-006-0005-3

- Buckingham, D. (2011) *The Material Child: Growing Up in Consumer Culture*. Cambridge: Polity Press.

- Crepax, T. et al. (2022) 'Information technologies exposing children to privacy risks: Domains and children-specific technical controls'. Computer standards and interfaces. [Online] 82103624–

- Decew, J. W. (1986) *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press.

- Donovan, S. (2023) *There should be recognition and protection of the privacy of children's identity and freedom for them to narrate their own online identity*. *PhD Thesis.* NUI Galway.

- Drexl, J. (2021) 'The (Lack of) Coherence of Data Ownership with the Intellectual Property System,' in Bruun, N., Dinwoodie, G. B., Levin, M., and Ohly, A. (eds) *Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur.* Cambridge: Cambridge University Press (Cambridge Intellectual Property and Information Law), pp. 213–223. doi: 10.1017/9781108688529.025.

- Dwoskin, E. & Romm, T. (2018) 'Facebook's rules for accessing user data lured more than just Cambridge Analytica: The social media giant changes its policies in 2015, but not before apps such as FarmVille and Tinder — and the Obama campaign — took advantage'. *The Washington Post* (Washington, D.C. 1974. Online).

- Floridi, L., & Taddeo, M. (2016). 'What is data ethics?' In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* (Vol. 374, Issue 2083). Royal Society of London. https://doi.org/10.1098/rsta.2016.0360

- Fukuyama, F. (2002) *Our posthuman future : consequences of the biotechnology revolution*. New York: Farrar, Straus and Giroux.

- GDPR-Info.eu. (n.d.). Recital 38 - General Data Protection Regulation (GDPR). Retrieved from https://gdpr-info.eu/recitals/no-38/ (Accessed: 12 September 2023)

- Genus, A., & Stirling, A. (2018). 'Collingridge and the dilemma of control: Towards responsible and accountable innovation'. *Research Policy*, *47*(1), 61–69. https://doi.org/10.1016/j.respol.2017.09.012

- Holloway, D. (2019) 'Surveillance capitalism and children's data: The internet of toys and things for children'. *Media international Australia incorporating Culture & policy*. [Online] 170 (1), 27–36.

- Ienca, M., Ferretti, A., Hurst, S., Puhan, M., Lovis, C., & Vayena, E. (2018a). 'Considerations for ethics review of big data health research: A scoping review'. *PLoS ONE*, *13*(10).

- Kasket, E. (2023) 'A moment that changed me: I stopped posting funny stories about my daughter and she began to trust me again'. *The Guardian.* Available at: https://www.theguardian.com/lifeandstyle/2023/aug/30/a-moment-that-changed-me-i-stopped-posting-funny-stories-about-my-daughter-and-she-began-to-trust-me-again (Accessed: 7 September 2023)

- Moglen, E. (2010). ‘Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing.’ Speech at the Free Software Foundation's Seminar.

- Montgomery, K. C. et al. (2017) ‘Children’s privacy in the big data era: Research opportunities’. *Pediatrics* (Evanston). [Online] 140 (Suppl 2), S117–S121.

- O'Hara, K., & Shadbolt, N. (2014). *The Spy in the Coffee Machine: The End of Privacy As We Know It*. London: Oneworld Publications

- O'Neil, C. (2017) *Weapons of math destruction-how big data increases inequality and threatens democracy*. New York: Allen Lane.

- O’Neill, O. (2009). ‘Ethics for communication?’ *European Journal of Philosophy*, *17*(2), 167–180. https://doi.org/10.1111/j.1468-0378.2009.00346.x

- O’Neill, O. (2019). *Transcript - The Ethics of Communication with Dr. Onora O’Neill - from podcast | Templeton World Charity Foundation, Inc.* https://www.templetonworldcharity.org/transcript-ethics-communication-dr-onora-oneill-podcast
- O’Neill, O. (2020). ‘Trust and accountability in a digital age’. *Philosophy*, *95*(1), 3–17. https://doi.org/10.1017/S0031819119000457

- Panayiotou, A. G., & Protopapadakis, E. D. (2022). ‘Ethical issues concerning the use of commercially available wearables in children’. *JAHR*, *13*(1), 9–22. https://doi.org/10.21860/j.13.1.1

- Petersen, K. B. (1997) *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press.

- Prensky, M. (2001) ‘Digital Natives, Digital Immigrants’. *On the Horizon*, 9(5). MCB University Press.

- Roessler, B., & Mokrosinska, D. (2013). ‘Privacy and social interaction’. *Philosophy and Social Criticism*, *39*(8), 771–791. https://doi.org/10.1177/0191453713494968

- Schneble, C. O., Favaretto, M., Elger, B. S., & Shaw, D. M. (2021). 'Social media terms and conditions and informed consent from children: Ethical analysis'. *JMIR Pediatrics and Parenting*, *4*(2). https://doi.org/10.2196/22281

- Schoeman, F. D. (1984) *Privacy and Social Freedom*. Cambridge University Press.

- Schoeman, F. D. (2010) *Privacy: Philosophical Dimensions*. Cambridge University Press.

- Taylor, L., Floridi, L. and Sloot, B.van der (2017) *Group privacy : new challenges of data technologies*. Dordrecht: Springer.

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

- Warren, S. D., & Brandeis, L. D. (1890) 'The Right to Privacy'. *Harvard Law Review*, 4(5), 193-220.

- Wu, T., 2017. *The attention merchants: How our time and attention are gathered and sold*. London: Atlantic Analysis Corp.

- Vanacker, B. and Heider, D. eds., (2018). *Ethics for a digital age*. New York, NY: Peter Lang.

- van Manen, M., & Levering, B. (1996) *Childhood's Secrets: Intimacy, Privacy, and the Self Reconsidered.* Teachers College Press. ISBN 0-8077-3505-1.

- Veliz. (2019). *Digitization, Surveillance, Colonialism - Liberties*. https://libertiesjournal.com/articles/digitization-surveillance-colonialism/ [Accessed 02 Aug. 2023].

- Veliz, C. (2020) *Privacy is power : why and how you should take back control of your data*. London: Bantam Press.

- Zuboff, S. (2019) *The age of surveillance capitalism : the fight for the future at the new frontier of power.* London: Profile Books.