**Please note that this is the authors’ accepted manuscript. Do not cite.**

**The publisher’s version can be found at:**

[**https://link.springer.com/article/10.1007%2Fs00146-021-01314-w**](https://link.springer.com/article/10.1007/s00146-021-01314-w)

**Title**

Hey, Google, Leave Those Kids Alone: Against Hypernudging Children in The Age of Big Data

**Authors**

Correspondence author: Mr James Smith, Department of Philosophy (Stellenbosch University), School for Data Science and Computational Thinking (Stellenbosch University), james@ridgetop.co.za

Co-author: Dr Tanya de Villiers-Botha, tdev@sun.ac.za, Department of Philosophy (Stellenbosch University).

**Acknowledgments**

James Smith is grateful to the School for Data Science and Computational Thinking at Stellenbosch University for their generous bursary which has enabled him to pursue his postgraduate studies.

**Abstract**

Children continue to be overlooked as a topic of concern in discussions around the ethical use of people’s data and information. Where children are the subject of such discussions, the focus is often primarily on privacy concerns and consent relating to the use of their data. This paper highlights the unique challenges children face when it comes to online interferences with their decision making, primarily due to their vulnerability, impressionability, the increased likelihood of disclosing personal information online, and their developmental capacities. These traits allow for practices such as hypernudging to be executed on them more accurately and with more serious consequences, specifically by potentially undermining their autonomy. We argue that children are autonomous agents in the making and thus require additional special protections to ensure that the development of their autonomy is safeguarded. This means that measures should be taken to prohibit most forms of hypernudging children and thus ensure that they are protected from this powerful technique of digital manipulation.

**Keywords**

Data Ethics, Big Data, Autonomy, Children, Hypernudging, Historical Account of Autonomy, Digital Manipulation

**Declarations**

Funding: Not applicable

Conflicts of interest: Not applicable

Availability of data and material: Not applicable

Code availability: Not applicable

Authors’ contributions: Not applicable

Ethics approval: Not applicable

Consent to participate: Not applicable

Consent for publication: Not applicable

## **Introduction**

According to the International Data Corporation (2020), to date, more than 59 zettabytes of data has been produced in the world, with the bulk of it being produced online. One third of all internet users are children and the generations of children being born today will be the first to live their entire lives in the age of Big Data (Berman and Albright, 2017: 9).[[1]](#footnote-2) Children are becoming more involved in the data cycle[[2]](#footnote-3), as they interact more with social media platforms, web browsers, and smart devices in the Internet of Things (Berman and Albright, 2017: 9). The practices of Big Data mean that searches a child makes on a web browser, like Google, or secrets they share with their smart toy, like Hello Barbie, are processed to reveal (potentially sensitive) information about them (see Holloway and Green, 2016; Berman and Albright, 2017; Chaudron *et al.*, 2017). This means that more data is now being gathered on children than ever before. The exact consequences of this practice are still unknown; however, given the vulnerabilities of children, it is important to identify and limit Big Data practices that could negatively impact them from the outset.

The capabilities of Big Data analytics are growing exponentially, whilst ethical considerations concerning Big Data are lagging behind (McAfee and Brynjolfsson, 2012: 4; Mittelstadt and Floridi, 2016: 304). Even more worryingly, ethical concerns relating to children in the data cycle have largely been overlooked (see Berman and Albright, 2017; Montgomery, Chester, and Milosevic, 2017). This is particularly troubling considering that children are vulnerable members of society and thus require special consideration and protection.

This paper extends the discussion on the ethical use of Big Data to children. Specifically, we argue that hypernudging, a Big Data-driven technique of decision interference, has the potential to unethically undermine crucial processes of autonomy development in children if used inappropriately. Hypernudging, when aimed at children, affects their decision-making processes early on in their development, thereby potentially affecting the way in which their capacity for autonomous decision-making develops and hence will function throughout their lives. Consequently, we argue that strong measures are needed to ensure that hypernudging is only used on children where it is clear that they will benefit from such interference. An example here may be using hypernudging to guide a depressed child to speak with their parents about their feelings. However, in instances where the benefits of hypernudging a child are not clear and significant, it should be deemed illegitimate and should not be allowed.[[3]](#footnote-4)

To make our case, we firstly lay some groundwork by addressing questions that may arise around children’s autonomy in general. We will be using an historical conception of autonomy, based on the work of Christman (1991)[[4]](#footnote-5), which emphasises how the desires, values, and emotions we develop throughout our lives have a direct, long-term impact on the decisions we make. This means that for our decisions to be deemed authentically autonomous, the development of such desires, values, and emotions needs to be as free from illegitimate interference as the act of deciding itself (see Christman, 2006). Once we have presented a general historical account of autonomy, we will give a brief description of hypernudging and its reliance on Big Data. Thereafter, we will argue that, due to its substantial interference in children’s development phase, hypernudging holds particular danger for children’s autonomy. Hence, we will argue that even where children currently do enjoy special protection in terms of data-related practices, such as under the General Data Protection Regulation in the European Union and the Protection of Personal Information Act in South Africa, such protections are insufficient, given the unique vulnerability of children and given that such protections generally focus primarily on protecting children’s privacy rather than their autonomy.

## **Autonomy and Children**

In line with various theorists on autonomy influenced by the modernist humanist tradition, we understand being autonomous, at its most basic, as being self-governed (see e.g., Dworkin 1988; Arneson 1991; Mele 1995; Christman 1991, 2020). To be self-governed means that one is directed by one’s authentic self, that is, one is moved to make decisions and act based on desires, conditions, and considerations that are authentically one’s own. For desires, values, and considerations (reasons) to be authentically one’s own, these need to develop or arise without undue influence from others.[[5]](#footnote-6) In addition, to be autonomous, in this basic sense, requires that one is responsible for one’s actions.[[6]](#footnote-7) In other words, one needs to somehow initiate one’s decisions and actions to be “responsible” for them in this sense in that they are the result of one’s “own command”. One’s actions need to be under one’s own control so that if this control were absent, one would not have taken the decision or executed the action.[[7]](#footnote-8) Hence, an autonomous person is a person who is responsible for their actions and whose decisions to act are based on authentic desires and considerations. Although the concept of “autonomy” is much-contested, autonomy as such is often considered to be a cornerstone of many moral and legal rights and responsibilities and as a precondition for a functioning liberal democracy (e.g., Dworkin 1988; Grafanaki, 2017: 811; Christman, 2020: 2-3). Myriad societal, moral, and political structures are predicated on the idea that people are able to choose and act autonomously. Consequently, as the most cursory glance at the applied ethics literature will confirm, the violation of autonomy in various contexts is often taken to be unethical. Similarly, we will assume that autonomy is valuable and merits protection and that unjustified violations of autonomy are unethical.

An influential contemporary approach to autonomy is an historicist one, where exercising one’s autonomy is conceived of in diachronic terms. It is argued that one’s historical development affects the decisions that one makes in such a way that this development itself also needs to meet certain criteria in order to ensure that one can exercise authentic autonomy (see e.g. Fischer and Ravizza (1988); Arneson 1991; Christman 1991, 2020; Mele 1995; Cohen 2000; Cave 2007).[[8]](#footnote-9) While the details of the various historical approaches to autonomy differ, the general argument is that one’s decisions are inevitably influenced by the values, desires, traits and emotions that one develops and embraces both as a child and throughout one’s lifetime. These are the factors that move one to make a decision in the first place. Hence, while it certainly is the case that autonomous decisions need to be free from illegitimate interference at the time that one makes them, the historical factors that move one to make a decision in the first place need to be free from illegitimate interference as well.[[9]](#footnote-10)

We find this general historical approach to autonomy compelling.[[10]](#footnote-11) While it clearly is the case that decisions made under duress cannot be deemed autonomous, it also seems right to hold that decisions made on the basis of values, desires, traits, and emotions that one has been manipulated or coerced into holding cannot be deemed autonomous either. Consider the case of S who was raised in an isolated cult since infancy. It seems plausible to suggest that any decisions that S makes are necessarily influenced by the worldview that she has been inculcated with since childhood. If her circumstances were such that she was never exposed to any ideas, values, practices, etc. that contradict those of the cult, any decision that she makes to endorse the values and ideas of the cult can hardly be described as an autonomous choice. S has had no opportunity to even conceive of alternative options, let alone evaluate their appeal. Clearly, people need to develop desires, values, and emotions, as well as tastes and preferences, before they can choose between anything (see Fischer and Ravizza 1988; Christman 1991; Mele 1995; Cohen 2000; Cave 2007). From infancy, people have experiences and encounter information that shape their worldview, and their desires, values, and emotions along with it. If a person visits an abattoir as a child and thereafter no longer desires to eat meat, and they keep this desire into adulthood, each time they decide to not eat meat, their decision is at least partly informed by a desire they formed in childhood. Following Grafanaki (2017: 812), we can gloss all the aspects of one’s history that have an impact on one’s decisions as part of the “exploration phase” of that decision. This encompasses one’s desires, values, and emotions and so forth that contribute to that particular decision. On an historical view of autonomy, to illegitimately interfere with this exploration phase is to undermine the autonomy of the decision that an agent makes just as much as interfering at the moment the decision is being made (call the latter the “application phase”). Hence, authentically autonomous decisions need to be free from illegitimate interference at both the exploration and the application phases.

Note that we are employing a weak sense of “authenticity” here, where the requirement is that the values, desires, and emotions that influence one’s decision to act, as well as the decision itself are *relatively* free from interference (see Cohen, 2000: 1424).[[11]](#footnote-12) “Relative” implies that there is leeway for some interference without it necessarily undermining the authenticity of a decision. Hence, one may act on the advice of a doctor, for example, who may strongly advise a given course of treatment for a life-threatening illness. Having a life-threatening illness and being urged by an expert to take a certain course of action significantly curtails one’s options and seemingly forces one’s hand to some extent. Nevertheless, deciding to opt for the treatment can still plausibly be described as an authentically autonomous decision. It is also important to note that interfering in someone’s autonomy is not always illegitimate. In most societies, drivers do not have the autonomy to drive recklessly and endanger the lives of others. It is relatively uncontroversial to hold that interference into citizens’ autonomy is necessary in certain instances in order for society to function. Hence, autonomy can be understood as a non-absolute value that needs to be weighed up against other relevant values rather than being upheld at all costs.

We will assume that interference becomes illegitimate i) when someone is restricted, for unjustifiable reasons, from developing certain desires, values, and emotions, or ii) when someone is unjustifiably restricted from performing certain actions. We suggest that the following two broad categories exemplify justifiable reasons for restricting someone from developing certain desires, values, or emotions or from performing certain actions:

1. When the well-being of others or the primary values of society can reasonably be said to be threatened if that person’s autonomy is not restricted.[[12]](#footnote-13) An example here would be imprisoning a convicted criminal.
2. If restricting the person’s autonomy can reasonably be said to be in the best interest of that person. This means that the interference should have some immediate or long-term benefit to the functioning or well-being of the person being interfered with. Preventing a mentally ill person from harming herself would be an example here.

In addition to having justifiable reasons for restricting someone’s autonomy, interference in autonomy can only be legitimate when it is undertaken by relevant and accountable parties. Hence, only those who have been mandated by society to interfere with the autonomy of others in a specific way can legitimately carry out such interference. The state is mandated to restrict the autonomy of a murderer because they are mandated with protecting their citizens from harm. Parents and guardians (and to some extent teachers and other authorities) are mandated with protecting and nurturing their children and they can restrict the autonomy of their children accordingly. Such interferences are constrained by mandates and by law, and parties interfering in the autonomy of others are nevertheless accountable for such interferences. They must be able to provide reasons for performing certain actions or making certain decisions in this regard and are also held responsible for the consequences of those actions or decisions (Lanzing, 2019: 563). When detaining a murderer, the state can (and should) be held accountable for any restrictions on the murderer’s autonomy that they do impose. Hence, whereas interference in autonomy is not always illegitimate, such interference can only be legitimate when it is done on the basis of justified reasons and by the appropriate parties who can be held to account for their interference.

From the above it should be clear that an historical conception of autonomy entails that, in a society that values autonomy, people should not only be relatively free from interference when making decisions, but they should also be relatively free to explore and experiment with a wide variety of desires, values, and emotions throughout their lifetimes and adopt those desires, values, and emotions that resonate most with them.

Of course, children[[13]](#footnote-14) are a special case in that paternalism towards their development and actions is not only tolerated, but expected.[[14]](#footnote-15) In fact, children’s status as autonomous agents is sometimes questioned (see Giesinger 2019). Given their limited rational competencies, it is argued that they cannot be left to their own devices and their parents and/or caretakers are expected to override their children’s decisions in as far as it is required to keep them safe and to facilitate their healthy development. For our purposes, it is important to emphasise that legitimate paternalism constitutes interference with someone’s autonomy *with that person’s end in mind* (see Dworkin 1988). In other words, paternalism is meant to be to benefit the person whose autonomy is being undermined. And even in such instances, the violation of autonomy is not always justified. For example, as children grow and their cognitive capabilities develop, they gain greater levels of “local autonomy”, making overly paternalistic interference with their choices unjustified (see Feinberg 1986). Moreover, such interference must be carried out by appropriate parties and under appropriate circumstances in order to be legitimate.

The details of children’s development into fully autonomous agents does not concern us here. What is important for our purposes is that the historical conception of autonomy sketched above entails that children are in a unique position in that they are still developing into fully-fledged autonomous agents. Hence, our claim is that children’s “autonomy-profile” differs from that of competent adults in that they are especially receptive and thus vulnerable in the exploration phase of autonomy. They are still forming the basis for their desires, emotions, beliefs, and general worldviews that will continue to affect their decisions throughout their lives. Hence, we are chiefly concerned with how interference through hypernudging affects this exploration phase of autonomy, as this is where we believe children are uniquely vulnerable. Essentially, our argument is that hypernudging potentially inhibits their development into authentic autonomous agents, thus negatively affecting them to an even greater extent than adults subjected to hypernudging. As such, children require unique protections in this regard.

**Vulnerability**

The unique position of children when it comes to their developing autonomy is compounded by their overall vulnerability. Children are generally considered to be dependent members of society because they are especially vulnerable.[[15]](#footnote-16) To be vulnerable is to be susceptible to harm, which Giesinger (2019) suggests we should understand on two levels. On the first level, to be vulnerable means to be in danger of being harmed at all. On the second level, to be vulnerable means to be unable to avoid being harmed. All human beings are vulnerable to some extent, and every human will fall under each of these levels to some degree. Nevertheless, children are especially vulnerable as a result of their heightened susceptibility on both levels of vulnerability (Giesinger, 2019: 219-220). On the first level, children are in more danger of being harmed at all because any harm that a child incurs harms them both on an immediate and developmental basis. For example, both adults and children share the potential to be harmed by starvation. Nevertheless, when an adult suffers from starvation, it affects them mostly on an immediate basis (pain, exhaustion, susceptibility to disease, and so on). When a child suffers starvation, they are affected on the same immediate basis as adults, but also on a development basis. The developmental basis accounts for the fact that the child will be physically, mentally, and emotionally impeded by their starving and that will have knock-on effects that will follow them throughout their lives (Giesinger, 2019: 220). The same goes for other harms.

On the second level of vulnerability, children are also more vulnerable than adults in their inability to avoid being harmed. Children do not yet have the cognitive, emotional, moral, or practical capacities to avert harms in the way that adults do (Giesinger, 2019). They do not understand the dangers of different situations that they should avoid, and once in these situations, they are less capable of getting out of them. In addition, children do not have the means to avoid certain harmful situations. For example, they lack the capacity to partake in financially compensatory work, at least the kinds of work that could support them financially whilst optimising their development (*ibid*.). This inability to avoid harms, coupled with the susceptibility to be more harmed in any harmful circumstances, is what makes children dependent members of society.

The vulnerability and dependence of children is the basis for their special status in the world. It is what causes societies to set up social arrangements to ensure that parties do not take advantage of children’s vulnerabilities (Dixon and Nussbaum, 2012; Giesinger, 2019). These arrangements include special rights and laws for children, as well as grants, orphanages, schools, feeding schemes, and the like, which can all be seen as the mechanisms that practically ameliorate the special vulnerabilities of children. From the above it should be clear that children occupy a unique position, which transfers to their relationship with Big Data practices as well. Not only are children uniquely vulnerable when it comes to the potentially pernicious effects of hypernudging, but society also already recognises the unique vulnerabilities of children and implements various measures in order to protect children from such harms. The remainder of this paper applies this background to the dangers children face when it comes to illegitimate hypernudging. We conclude that more drastic measures are needed to protect children against this practice.

## **Big Data and Children**

The practices of what has come to be known as “Big Data” has come under the spotlight for various reasons (e.g., Mittelstadt and Floridi, 2015). In this paper we are primarily concerned with the way in which massive data sets are used to influence behaviour. Once data becomes information, it has an economic value (Yeung, 2017). For example, the dominant information technology companies such as Google and Facebook use the large volumes of data that they have access to through their various platforms in order to develop targeted content and targeted advertising. [[16]](#footnote-17) In addition, other companies, governments, individuals and so forth acquire this data or insights gleaned from it for various purposes. This includes targeted advertising, product improvement and tracking, amongst others (Floridi, 2015; Floridi & Taddeo, 2016; Shaw, 2016; Panger 2016; Grafanaki, 2017; Susser, Roessler and Nissenbaum, 2019; Veliz, 2020). Much of this practice is aimed at some form of behaviour modification—the aim is to get consumers to spend more time on certain platforms (and hence to have more opportunity to expose them to advertising and to gather more data on them, which allows for better-tailored content that keeps them on the platform longer) and/or to expose consumers to as much targeted advertising as possible (Véliz, 2020). The assumption is that the better targeted advertisements are, the better the chances that the consumers will click on those advertisements and buy the advertised products. In order to better target content and advertisements large amounts of data are gathered on individual web users, which allows for the creation of their “data doubles” (Grafanaki, 2017). A data double is a digital version of a web user that represents their current behaviour, preferences, desires, emotional states, and cognitive weaknesses (Grafanaki, 2017; Susser, Roessler and Nissenbaum, 2019). Advertisements and other internet content are then created, curated, and delivered in accordance with the insights revealed by these doubles so as to be maximally effective. Essentially, who we are and what drives us, according to the information that Big Data has on us, determines what we see on the internet, both in terms of content and advertisements.

It has been estimated that at least one in three internet users are below the age of sixteen (Berman and Albright, 2017). Children being born today will be the first to be part of the data cycle throughout their entire lives. Some children will even be part of the data cycle before they are born.[[17]](#footnote-18) In addition, children are being exposed to more and more web-connected devices and services, such as smart toys and YouTube Kids. Coupled with rapid and exponential growth in the power of modern computational systems, this will significantly improve the accuracy of data doubles on people in general, and on children in particular. This means that people are at greater risk of being influenced online *as children* and *as adults*. This is concerning in two ways. Firstly, it means that Big Data barons will have greater insights into the behaviour and susceptibilities of children at critical periods in their personal development (Berman and Albright, 2017: 16). Children could be digitally influenced during these times to adopt different desires, values, and emotions that could influence their decisions around political and social issues, as they grow older. This could give the barons, and by extension the people who use their services for advertising, the ability to influence people’s voting and purchasing behaviour to swing elections and increase revenue.[[18]](#footnote-19) Secondly, with considerably more information on people by the time they reach adulthood, companies will be able to influence the behaviour of adults online (and, arguably, offline) with far more accuracy.

Being part of the data cycle exposes children to the same kinds of online interference as adults. Moreover, children are uniquely vulnerable to online interference for two reasons. Firstly, they are more likely to provide personal information to smart devices and web services without fully comprehending the potential consequences (Chung and Grimes, 2006). This allows companies to generate more accurate data doubles of them. Secondly, children are more easily manipulated and indoctrinated than adults[[19]](#footnote-20) as well as more impressionable, impulsive, and experience more frequently fluctuating emotions (see Montgomery, Chester, and Milosevic, 2017; and Gorshkova, Robaina-Calderin and Martin-Santana, 2020). All these traits of children make them far more at risk to online decision interference (and hence manipulation) than adults.

A powerful form of decision interference in this context consists in hypernudging. We will give a brief explanation of what this practice entails before discussing its possible pernicious effects on children.

## **How to Hypernudge**

Hypernudging is the practice of online decision “guidance” that uses information about the susceptibilities and preferences of an individual to try and alter their decision making in the context of Big Data. The term derives from the concept of nudging, popularised by Thaler and Sunstein (2008) with their pioneering work in the field of behavioural economics. Nudging is a design-based approach to altering the behaviour of people without overtly limiting their options or changing the economic incentives of the options available to them. This is achieved using knowledge of people’s heuristics and cognitive biases, the shortcuts the brain takes to save time and effort in the decision-making process[[20]](#footnote-21) (see Kahneman, 2011).

Hypernudging shares a lot of characteristics with regular nudging. It still aims to alter the decisions of a person unconsciously; however, it occurs online and, crucially, on an individual, targeted level, using dynamic, data-driven means to alter a person’s choice architecture, and it potentially occurs across a variety of platforms, as a given party can easily place specific targeted advertisements across the internet (Simons & Gosh, 2020). This means that unlike regular nudges, hypernudges are tailored to alter an individual’s decisions based on their *personal* preferences, biases, and susceptibilities, making hypernudging far more subtle and effective than nudging (Yeung, 2017). For example, data analysis can reveal the times of day a person is more likely to make an online purchase. Companies can then hypernudge a person to purchase their products at the time of day that this hypernudge will be most effective. Such nudges can also be ubiquitous, following someone as they navigate the internet. Sætra (2019: 1) argues that hypernudges are too powerful to be deemed nudges at all and describes them as “shoves” instead. The features that give hypernudging this increased potency can be narrowed down to *personalistation* and *dynamicity*.

The dynamic feature of hypernudging is related to the velocity feature of Big Data. Hypernudges can be adjusted in accordance with real-time changes in the preferences of an individual. This means that hypernudges can be continuously updated to optimise their influence over a particular person. The dynamic feature of hypernudging is seen in how Facebook uses data from its platform to track the real-time moods and feelings of its users (Lanzing, 2019). This real-time information can be used to microtarget content and advertisements to people who are feeling a particular way at a particular time. Moreover, these advertisements can be adjusted as changes are detected in the moods and emotions of the target. Cambridge Analytica used similar processes when hypernudging voters in the 2016 US Elections. The company microtargeted advertisements to people based on their psychometric profiles. Depending on the user’s real-time engagement with the advertisement, it would be tweaked until the optimal formula for persuasion as identified (Véliz, 2020).This example of behaviour being altered in accordance with real-time information displays the dynamicity of hypernudging. It is not difficult to imagine similar kinds of decision interference being conducted via platforms such as “YouTube Kids”[[21]](#footnote-22) or the proposed “Instagram Kids”, projects that pose significant ethical concern for the well-being of children in the age of Big Data (BBC, 2021). It is important to note that targeted advertising need not be restricted to clearly identified advertisements but can be integrated into the actual content of videos and other material on the internet.

Hypernudging can also take place via other products aimed at children through the Internet of Things. Introduced in 2015 and now discontinued, Hello Barbie is a smart toy that uses pre-programmed responses to hypernudge children to share private information about themselves and their families, which is recorded via the toy’s microphone and then analysed (see Walker, 2015; McReynolds *et al.*, 2017; Steeves, 2020). The toy uses build-in games to “learn” about the child and their circumstances and then uses this knowledge to elicit further information about the child and their family (Steeves, 2020). For example, one game involves the child telling the doll which shops in a fictional town their family members would be most likely to operate. If the child responds that their dad would like to work at the pet shop, then the doll questions the child further, “which animals are his favourite”. This information about the child and their family is used not only to encourage the child to form a bond with the doll but also to inform the dialogue going forward with the aim of persuading the child to share even further information and to encourage the child to consume more Barbie-related products (Steeves, 2020). This example represents how the personalisation of nudges can be used to influence children not only to disclose sensitive information about themselves and their families, but to affect their feelings and behaviour towards their toys and potentially their consumption choices in the future.

It is clear that hypernudging is often effective. Tollon (2021) highlights the capabilities that Big Data-backed hypernudging has to influence people’s behaviours, which subsequently could affect their values. He notes the YouTube AutoPlay algorithm as an example of this due to its tendency to recommend conspiratorial content, which has been shown to nudge viewers to use the platform for longer, thus generating more advertising revenue (Tollon, 2021). Of course, the consequences of this nudging are people potentially having their values informed by epistemically problematic content, which can lead to problematic decisions and behaviours.

The alarming implications of online “value mediation”, especially regarding children and teenagers, are seen in the involvement of Cambridge Analytica in the 2010 Trinidad and Tobago general election. In 2010, Cambridge Analytica created a political marketing campaign directed specifically towards the youth in Trinidad and Tobago (*BBC*, 2018; Digital, Culture, Media and Sport Committee, 2019; Hilder, 2019). The firm used Big Data and social media to gain insights into the behaviours and preferences of the youth to develop and execute a campaign that did not support a particular candidate, but rather sought to make voting unpopular with the young people. This included the creation of anti-voting music, dances, and videos that were targeted at people in the country within a certain age group. Cambridge Analytica’s insights had revealed that the young supporters of the United National Congress would be less influenced by the anti-voting campaign than the young supporters of the People’s National Congress. Purportedly, this resulted in a higher turnout for the United National Congress, which is thought to have tipped the election in the party’s favour. This is one of many examples where technology has seemingly been used to affect the values people adopt. It is not unreasonable to imagine this example of hypernudging being used to manipulate the political orientation of children at a younger age, and for a longer period of time.[[22]](#footnote-23)

## **Leave Those Kids Alone**

A number of ethical concerns have been raised around both nudging and hypernudging (Yeung, 2017). The concern that hypernudging can be deceptive is effectively a concern about autonomy in that hypernudges can distort the capacity of people to make authentic decisions. The undermining of autonomy associated with hypernudging is even greater cause for concern when it comes to children.

Arguably, any decision that a person makes where hypernudging has been present in either the exploration phase or the application phase of that decision could potentially fail to be authentically autonomous. This need not necessarily be wrong since, as already discussed, autonomy is a non-absolute value. Nevertheless, it can become problematic when the reasons for employing such hypernudging are illegitimate. As touched upon above, hypernudges have been shown to be capable of subtly changing the desires, values, and emotions of people overtime, a feature which can be used to interfere with decision-making for any number of illegitimate reasons. Hypernudging has been used to alter political expressions[[23]](#footnote-24), alter people’s moods[[24]](#footnote-25), and influence product purchases[[25]](#footnote-26). All of these examples involved deliberate interferences in the authentic construction of desires, values, and emotions, which ultimately guide decision making. That being said, a case may be made that adults, as mature autonomous agents, are not entirely susceptible to hypernudges and do not necessarily have their autonomy undermined by being subjected to these. Presumably, at the very least, adults can choose to avoid environments in which hypernudges take place or counter the effects of hypernudging through critical reflection. Some scholars are optimistic about hypernudging and the opportunities it presents. Mills (2019), for example, believes that hypernudging holds the potential to significantly improve people’s behaviour around health and finance. He suggests that these benefits of hypernudging should not be overlooked when assessing whether or not it is a permissible means of decision guidance.

Nevertheless, even if we accept such arguments, it remains the case that children, in particular, require more stringent protections against such decision interference, given their unique vulnerabilities when it comes to autonomy. For one, children are more likely to divulge personal information, and they are less likely to understand that their decisions are being interfered with in the first place. Moreover, children are generally more impressionable than adults and less likely to be able to extricate themselves from manipulative contexts. In addition to their immediate vulnerability, hypernudging also threatens to undermine the autonomy of children to an even greater extent than that of adults in that it disproportionately affects the exploration phase of their decision making, both now and into the future. As we have seen, the desires, values, and emotions a person develops as a child potentially influence the decisions they make throughout their lives. Hence, children being hypernudged today are not only more susceptible to hypernudges as children but are in danger of failing to develop into authentically autonomous adults, at least with regard to some aspects of their lives.

As seen above, modern technology and Big Data have provided a direct line to the attention of children through a wide variety of web-connected devices and online platforms (also see Keymolen & Van der Hof, 2019). YouTube Kids and Netflix Kids are already well-established, and Instagram Kids is in the pipeline (Kelly, 2021). Furthermore, children are using web browsers like Google far more frequently. If motivated, the companies behind these platforms could persuade a child to adopt a particular political orientation over time, even less intrusively than was the case with Cambridge Analytica in Trinidad and Tobago. Techniques like filtering search results and social media content and targeted advertisements could ensure that a child is never given adequate exposure to opinions and information that do not support a particular political or ideological orientation. This would mediate their values by improving access to certain information, whilst restricting other information. This is an example of direct, illegitimate interference in self-construction. These scenarios of value-mediation in children remain possible as long as the practices of Big Data organisations are allowed to go unchecked.

That is not to say that hypernudging children is never permissible. As discussed above, restricting autonomy may be legitimate if society or those being restricted can plausibly be said to benefit from the restriction and if it were to be carried out by the appropriate, accountable parties. These conditions do not apply in the case of most commercial hypernudges targeting children, nor in instances where hypernudging is aimed at influencing the worldview of children for particular political purposes. Arguably, the aim in such instances is to increase profit or political sway and not to benefit those children or society in general. Moreover, the parties involved are generally not mandated to engage in such interference. There is also a general lack of accountability for the purposes, methods and results of such hypernudging. Clearly hypernudging in these cases consist in illegitimate interferences with children’s autonomy.

A case can be made that there are instances where hypernudging children could be legitimate, such as hypernudging a child showing signs of depression in their online behaviour to speak to their parents or find help through other means. Here interfering is clearly to the child’s benefit. Nevertheless, we argue that even if a private company that harvests data for commercial reasons can identify depressed behaviour in adolescent users of its platform as a result, it should not be permitted to intervene through hypernudging in its own capacity, as it is not mandated to do so and cannot be held properly accountable.[[26]](#footnote-27) Hence, even if there are legitimate instances of hypernudging children, private companies are not the appropriate parties for carrying out such hypernudging. Only accountable parties that are mandated with looking after the welfare of the children involved should be allowed to interfere with their decision making in this way. In addition, given the significant impact that exposure to hypernudging could have on children and their development, we would argue that even in cases where such nudging is undertaken by legitimate parties and to the benefit of the child, a cost-benefit analysis should be undertaken in order to show that the potential benefits are sufficient to outweigh the costs of potential loss of autonomy.

## **Current Protections**

It may be argued that in at least some instances, children already have special protection against the practises of Big Data in the form of legislation such as the European Union’s General Data Protection Regulation (GDPR), as well as South Africa’s Protection of Personal Information Act (POPIA) (Protection of Personal Information Act 34/35; General Data Protection Regulation 8/6), for example. Nevertheless, these protections are often inadequate in protecting children against autonomy-related harms stemming from maleficent forms of online decision interference. This is partly due to the primary focus of such legislation being on protecting the values of privacy and consent when it comes to obtaining and processing data on children. For example, POPIA allows for the processing of children’s “personal information which has deliberately been made public by the child with the consent of a competent person” (Protection of Personal Information Act, 35e). Article 8 GDPR requires parental consent to be obtained for the processing of children’s data in relation to “information society services” offered directly to children under a certain age. Here, once privacy concerns have been addressed, children’s data could still potentially be used for the purposes of hypernudging, despite the special legal protections afforded to them in terms of privacy. We argue that autonomy protection needs to be a specific area of focus of such legislation and that the possibility of parents and guardians consenting to the use of children’s data for commercial purposes should be circumscribed so as to prohibit commercial (and politically related) hypernudging.

Given the power of hypernudges and heightened vulnerability of children, measures should be put in place to ensure that hypernudging children is clearly regulated. We are persuaded by the idea that children should be given a “clean data slate”, a proposal that bans all private and public storage of data on children up to a certain age (Renda, 2020: 664). Hypernudges cannot be produced without the vast datasets Big Data barons compile on their users. Therefore, this clean data slate should ensure that no child can be digitally manipulated through hypernudging. Nevertheless, we concede that there are instances where children are benefitted from having their data collected and stored and that hypernudging them may sometimes be legitimate. Hence, legislation should be put in place that not only safeguards their privacy and integrity but also their autonomy.

A possible objection to our argument is that *any* case of hypernudging could be legitimate if adequate notice is given by the choice architect before the hypernudging occurs and if consent is given. This would mean that the hypernudged party essentially waives their right to autonomy in exchange for another benefit, such as using a web service for free, for example. However, children, especially younger children, are not in a position to give *informed* consent in this regard. There are questions around even adults’ capacity to give meaningful informed consent in this context (e.g. Solove, 2013: 1881)[[27]](#footnote-28). Van der Hof (2017: 132) argues that children *and* adults would require intensive tutoring in the processes of datafication and the fundamental impact it could have on their lives and autonomy to be able to give informed consent regarding these processes. Nevertheless, for the sake of argument, we can concede that adults can legitimately consent to being deceived through hypernudging. Does this imply that adults can consent to their children’s being hypernudged in exchange for given benefits? Not on our view, since allowing such interferences with children’s autonomy still needs to be shown to be of benefit to the child in order to be legitimate. And one would be hard-pressed to identify benefits from commercial hypernudging that outweigh the potential costs that the child would bear as a result of loss of autonomy, given their unique risks in this regard.

## **Conclusion**

Hypernudging undermines autonomy, and this has especially negative implications for the development of autonomy in children. An historicist approach to autonomy stresses that a person’s desires, values, and emotions are what move them to make decisions in the first place. This means that for a decision to be deemed authentically autonomous, these traits in a person need to be as free from illegitimate interference as the act of deciding itself. Since people start developing these traits as children, it is essential that children are protected from illegitimate interference in their exploration and experimentation with different desires, values, and emotions.

Hypernudging is deceptive as it intentionally seeks to bypass the rational capacities of a person or to restrict their choice architecture in an effort to affect their decision making in a particular way. And while it might be possible to make a case for adults giving informed consent to being hypernudged, the same cannot be said for children. Furthermore, hypernudging children is more cause for concern than hypernudging adults given the heightened vulnerability and the possible long-term impact the practice may have on their autonomy. Hence, hypernudging children should only be allowed to the extent that the benefits *to them* can plausibly be said to outweigh the costs that they will bear and legislation should be developed that protects children accordingly.

## **References**

Arneson, Richard, 1991. “Autonomy and Preference Formation,” in Jules Coleman and Allen Buchanan (eds.), In Harm’s Way: Essays in Honor of Joel Feinberg, Cambridge: Cambridge University Press, pp. 42–73.

BBC News. 2018. *Cambridge Analytica-linked firm 'boasted of poll interference'*. [online] Available at: <https://www.bbc.com/news/uk-43528219> [Accessed 8 June 2021].

BBC News. 2021. *Instagram for kids paused after backlash*. [online] Available at: <https://www.bbc.com/news/technology-58707753> [Accessed 28 September 2021].

Berman, G. and Albright, K. (2017) *Children and the Data Cycle: Rights and Ethics in a Big Data World*, *Innocenti Working Paper 2017-05,*. Florence. doi: 10.13140/RG.2.2.20603.52008.

Brighouse, H. and Swift, A. (2014) *Family Values: The Ethics of Parent-Child Relationships*. Princeton & Oxford: Princeton University Press.

Carolan, M. (2018) ‘Big data and food retail: Nudging out citizens by creating dependent consumers’, *Geoforum*. Elsevier, 90(December 2017), pp. 142–150. doi: 10.1016/j.geoforum.2018.02.006.

Cave, E. (2007). What's Wrong with Motive Manipulation? *Ethical Theory and Moral Practice,* *10*(2), 129-144.

Chaudron, S. *et al.* (2017) *Kaleidoscope on the Internet of Toys: Safety, security, privacy and societal insights*. doi: 10.2788/05383.

Chen, W. and Quan-Haase, A. (2020) ‘Big Data Ethics and Politics: Toward New Understandings’, *Social Science Computer Review*, 38(1), pp. 3–9. doi: 10.1177/0894439318810734.

Christman, J. (1991). Autonomy and Personal History. *Canadian Journal of Philosophy,* *21*(1), pp. 1-24.

Christman, J. (2006) ‘Relational Autonomy and the Social Dynamics of Paternalism’, *Ethical Theory and Moral Practice*, 17(3), pp. 369–382. doi: 10.1007/s.

Christman, J. (2020) *Autonomy in Moral and Political Philosophy*, *Stanford Encyclopedia of Philosophy*. doi: 10.5860/choice.41sup-0181.

Chung, G. and Grimes, S. M. (2005) ‘Data Mining the Kids: Surveillance and Market Research Strategies in Children’s Online Games’, *Canadian Journal of Communication*, 30(4), pp. 527–548. doi: 10.22230/cjc.2005v30n4a1525.

Cohen, J. E. (2000) ‘Examined Lives: Informational Privacy and the Subject as Object’, *Georgetown Law Faculty Publications and Other Works*, pp. 1373–1438. doi: 10.4324/9781351154161-12.

House of Commons Digital, Culture, Media and Sport Committee (2018) ‘Disinformation and ‘fake news’: Interim Report’, Fifth Report of Session 2017–19. Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm> [Accessed 15 June 2021]

House of Commons Digital, Culture, Media and Sport Committee (2019) ‘Disinformation and 'fake news': Final Report’, Eighth Report of Session 2017–19. Available at: < https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm> [Accessed 15 June 2021]

Dixon, R. and Nussbaum, M.C. (2012) “Children’s Rights and a Capabilities Approach: The Question of Special Priority” Cornell Law Review 97(3), pp. 549-594. Available at: http://scholarship.law.cornell.edu/clr/vol97/iss3/3

Dworkin, G. (1988) *The Theory and Practice of Autonomy*. Cambridge: Cambridge University Press.

Fairs, M., 2018. *Eindhoven pioneers use of scent and light to "influence the behaviour of people" in crowds*. [online] Dezeen.com. Available at: <https://www.dezeen.com/2018/01/04/design-terrorism-talk-eindhoven-pioneers-use-scent-light-influence-behaviour-people-in-crowds/> [Accessed 10 June 2021].

Feinberg, J. (1986) *The Moral Limits of the Criminal Law: Harm to Self*. Oxford: Oxford University Press.

Fischer, J.M. and Ravizza, M. (1988) *Responsibility and Control. A Theory of Moral Responsibility*. Cambridge: Cambridge University Press.

Floridi, L. (ed.) (2015) *Introduction*, *The Onlife Manifesto: Being Human in a Hyperconnected Era*. Springer. doi: 10.1007/978-3-319-04093-6\_21.

Floridi, L. and Taddeo, M. (2016) ‘What is Data Ethics?’, *The Lancet*, 130(3344), p. 680. doi: 10.1016/S0140-6736(02)10308-4.

Genus, A. and Stirling, A. (2018) ‘Collingridge and the dilemma of control: Towards responsible and accountable innovation’, *Research Policy*. Elsevier, 47(1), pp. 61–69. doi: 10.1016/j.respol.2017.09.012.

Gheaus, A. (2018), Children's Vulnerability and Legitimate Authority Over Children. J Appl Philos, 35: 60-75. <https://doi.org/10.1111/japp.12262>

Giesinger, J. (2019) ‘Vulnerability and Autonomy–Children and Adults’, *Ethics and Social Welfare*. Taylor & Francis, 13(3), pp. 216–229. doi: 10.1080/17496535.2019.1647262.

Gorshkova, N., Robaina-Calderin, L. and Martin-Santana, J. D. (2020) ‘Paradigm Shifts in ICT Ethics Proceedings of the of the ETHICOMP 2020’, in Pelegrín-Borondo, J. et al. (eds) *Native Advertising: Ethical Aspects of Kid Influencers on Youtube*. Universidad de La Rioja, pp. 169–170.

Grafanaki, S. (2017) ‘Autonomy Challenges in the Age of Big Data’, *Fordham Intellectual Property, Media and Entertainment Law Journal*, 27(4), pp. 803–868.

Hilder, P., 2019. *‘They were planning on stealing the election’: Explosive new tapes reveal Cambridge Analytica CEO’s boasts of voter suppression, manipulation and bribery*. [online] openDemocracy. Available at: <https://www.opendemocracy.net/en/dark-money-investigations/they-were-planning-on-stealing-election-explosive-new-tapes-reveal-cambridg/> [Accessed 8 June 2021].

Holloway, D. and Green, L. (2016) ‘The Internet of toys’, *Communication Research and Practice*. Routledge, 2(4), pp. 506–519. doi: 10.1080/22041451.2016.1266124.

IDC. 2020. *IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data*. [online] Available at: <https://www.idc.com/getdoc.jsp?containerId=prUS46286020> [Accessed 8 June 2021].

Kahneman, D. (2011) *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux.

Kelly, H., 2021. *Instagram is making a kids’ app. Here’s what parents need to know about social media Jr.* [online] washingtonpost.com. Available at: <https://www.washingtonpost.com/technology/2021/03/24/instagram-kids-faq/> [Accessed 11 June 2021].

Keymolen, E. and Van der Hof, S. (2019) ‘Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust’, *Journal of Cyber Policy*. Taylor & Francis, 4(2), pp. 143–159. doi: 10.1080/23738871.2019.1586970.

Lanzing, M. (2019) ‘“Strongly Recommended” Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies’, *PhiloTechnol.*, 32, pp. 549–568. Available at: https://doi.org/10.1007/s13347-018-0316-4.

Lupton, D. (2017) ‘“It Just Gives Me a Bit of Peace of Mind”: Australian Women’s Use of Digital Media for Pregnancy and Early Motherhood’, *Societies*, 7(25), pp. 1–13. doi: 10.3390/soc7030025.

Macleod, C. (2019) Paradoxes of Children’s Vulnerability, *Ethics and Social Welfare*, 13:3, 261-271, DOI: [10.1080/17496535.2019.1630465](https://doi-org.ez.sun.ac.za/10.1080/17496535.2019.1630465).

Markham, A. N., Tiidenberg, K. and Herman, A. (2018) ‘Ethics as Methods: Doing Ethics in the Era of Big Data Research - Introduction’, *Social Media and Society*, 4(3), pp. 1–9. doi: 10.1177/2056305118784502.

Matz, S.C., Kosinski, M; Nave, G. and Stillwell, D.J. (2017) ‘Psychological targeting in digital mass persuasion’, *Proceedings of the National Academy*, 114(48) 12714-12719. doi: 10.1073/pnas.1710966114

McAfee, A. and Brynjolfsson, E. (2012) ‘Big Data: The Management Revolution’, *Harvard Business Review*, October, pp. 1–9. Available at: http://tarjomefa.com/wp-content/uploads/2017/04/6539-English-TarjomeFa-1.pdf.

McDonald, A. and Cranor, L. F. (2008) ‘The cost of reading privacy policies’, *I/S: A Journal of Law and Policy for the Information Society*, 4(3), pp. 543–568.

McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., Roesner, F. (2017) ‘Toys that listen: A study of parents, children, and internet-connected toys’, in *Conference on Human Factors in Computing Systems*. Denver. doi: 10.1145/3025453.3025735.

Mele, A.R. (1995). *Autonomous Agents: From Self-Control to Autonomy*. Oxford: Oxford University Press.

Mills, S (2019) ‘Into Hyperspace: An Analysis of Hypernudges and Personalised Behavioural

Science’ Available at SSRN: [https://ssrn.com/abstract=3420211](https://ssrn.com/abstract%3D3420211)

Mittelstadt, B. D. and Floridi, L. (2015) ‘The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts’, *Science and Engineering Ethics*. Dordrecht: Springer Netherlands, 22, pp. 303–341. doi: 10.1007/s11948-015-9652-2.

Montgomery, K. C., Chester, J. and Milosevic, T. (2017) ‘Children’s privacy in the big data era: Research opportunities’, *Pediatrics*, 140(2), pp. 117–121. doi: 10.1542/peds.2016-1758O.

Nissenbaum, H. (2011) ‘A contextual approach to privacy online’, *Dædalus*, 140(4), pp. 32–48. doi: 10.3233/978-1-61499-057-4-219.

Panger, G. (2016) ‘Reassessing the Facebook experiment: critical thinking about the validity of Big Data research’, *Information Communication and Society*. Taylor & Francis, 19(8), pp. 1108–1126. doi: 10.1080/1369118X.2015.1093525.

South Africa. Protection of Personal Information Act No. 4 of 2013.

Renda, A. (2020) ‘Europe: Toward a Policy Framework for Trustworthy AI’, in Dubber, M. D., Pasquale, F., and Das, S. (eds) *The Oxford Handbook of Ethics of AI*. Oxford. Available at: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190067397.001.0001/oxfordhb-9780190067397-e-41.

Richterich, A. 2018. *The Big Data Agenda: Data Ethics and Critical Data Studies*. Pp. 33–51. London: University of Westminster Press.

Schweiger, G. (2019) “Ethics, Poverty and Children’s Vulnerability”, *Ethics and Social Welfare*, 13(3), pp. 288-30. doi: [10.1080/17496535.2019.1593480](https://doi.org/10.1080/17496535.2019.1593480).

Sætra, H. S. (2019) ‘When nudge comes to shove: Liberty and nudging in the era of big data’, *Technology in Society*, 59, pp. 1–10. doi: 10.1016/j.techsoc.2019.04.006.

Shah, D. V., Cappella Ramesh, J. N. and Neuman, W. R. (2015) ‘Big Data, Digital Media, and Computational Social Science: Possibilities and Perils’, *Annals of the American Academy of Political and Social Science*, 659(1), pp. 6–13. doi: 10.1177/0002716215572084.

Shaw, D. (2016) ‘Facebook’s flawed emotion experiment: Antisocial research on social network users’, *Research Ethics*, 12(1), pp. 29–34. doi: 10.1177/1747016115579535.

Simons, J. and Ghosh, D. (2020) “[Utilities for democracy: Why and how the algorithmic infrastructure of Facebook and Google must be regulated](https://scholar.harvard.edu/dipayan/publications/utilities-democracy-why-and-how-algorithmic-infrastructure-facebook-and-google).” Brookings Institution. Available at: <https://scholar.harvard.edu/dipayan/publications/utilities-democracy-why-and-how-algorithmic-infrastructure-facebook-and-google>.

Solove, D. J. (2013) ‘Introduction: Privacy self-management and the consent dilemma’, *Harvard Law Review*, 126(7), pp. 1880–1903.

Susser, D., Roessler, B. and Nissenbaum, H. (2019) ‘Online Manipulation: Hidden Influences in a Digital World’, *Georgetown Law Technology Review,* 4(1), pp. 1–52.

Taylor, R. (2020) *Review of online targeting: Final report and recommendations*.

Thaler, R. and Sunstein, C. (2008) *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New York: Penguin Books.

Tollon, F. (2021) ‘Designed to Seduce: Epistemically Retrograde Ideation and YouTube’s Recommender System’, *International Journal of Technoethics*, 12(2), pp.60-71.

Van der Hof, S. (2017) ‘I Agree... Or Do I? A Rights-Based Analysis of the Law on Children’s Consent in the Digital World’, *Wisconsin International Law Jounral*, 34(2), pp. 409–445.

Véliz, C. (2020) *Privacy Is Power* . London, UK: Penguin (Bantam Press).

Walker, L. (2015) ‘Meet Hello Barbie: A Wi-Fi Doll That Talks to Children’, *Newsweek*, 17 February. Available at: https://www.newsweek.com/meet-hello-barbie-wi-fi-doll-talks-children-307482.

Yeung, K. (2017) ‘“Hypernudge”: Big Data as a mode of regulation by design’, *Information Communication and Society*. Taylor & Francis, 20(1), pp. 118–136. doi: 10.1080/1369118X.2016.1186713.

1. For the purposes of this paper, “Big Data” refers to the gathering, processing, and analysing of this massive amount of data (see Floridi and Mittelstadt 2016: 309). [↑](#footnote-ref-2)
2. The term “data cycle” can be understood as follows: *data providers* use online services, *data collectors* gather data produced on online services, *data analysts* process this data into information, *data users* make use of this information for different purposes (marketing, insurance, and so on). See Berman and Albright (2017: 23) for a detailed breakdown. [↑](#footnote-ref-3)
3. We will address the issue of what makes interference illegitimate in more detail below. [↑](#footnote-ref-4)
4. Also see Arneson (1991); Mele (1995), Cohen (2000) and Christman (2020). [↑](#footnote-ref-5)
5. Admittedly, this formulation is vague, but it is sufficient for our purposes, as we are setting the bar for “undue” influence relatively high—i.e., influence that constitutes manipulation and coercion. [↑](#footnote-ref-6)
6. Also note that responsibility here refers to “role responsibility”, where someone can be held to be counterfactually responsible for their actions, regardless of any moral responsibility that may or may not pertain (see Genus and Stirling, 2018: 62). [↑](#footnote-ref-7)
7. The distinction between one’s actions being authentically one’s own and one’s being responsible for such decisions and actions can be subtle and is much contested in the literature. For our purposes, it is sufficient to note that while I may authentically choose to raise my arm at time *t*, it is still possible for me to not be *responsible* for raising my arm at *t*, if it happens that someone else comes along and raises my arm for me at *t*. [↑](#footnote-ref-8)
8. It should be noted that various such models exist that differ in terms of detail and degrees of complexity. Here, we employ a maximally general conception of such a diachronic approach without committing ourselves to the finer-grained particulars. It is our contention that the practice of hypernudging children will fall foul on any such a model. [↑](#footnote-ref-9)
9. See Cave (2007) for an extensive discussion. [↑](#footnote-ref-10)
10. Various theorists have made the case that historical approaches to autonomy are better placed than structural accounts to deal with the ways in which one can be manipulated into making non-authentic (but seemingly autonomous) decisions. See Christman (1991; 2020), Mele (2001), and Cave (2007). [↑](#footnote-ref-11)
11. See Dworkin (1988) who provides an illuminating discussion on how one can be autonomous while still being influenced, to some extent, by others. [↑](#footnote-ref-12)
12. “Primary values” here refer to the values that no liberal democracy could be sustained without, including life, happiness, freedom, knowledge, ability, resources, and security Moor (1997: 29). [↑](#footnote-ref-13)
13. We use the status definition “children” developed by Brighouse and Swift (2014: 62), which argues that for an individual to be considered a child, they must possess four necessary features: *vulnerability*, *dependence*, no conception of *value* and the “*capacity* to develop into nonvulnerable and independent adults”. [↑](#footnote-ref-14)
14. With “paternalism” here we have in mind violations of a person’s autonomy for the good of that person (see Dworkin 1988, 123). [↑](#footnote-ref-15)
15. E.g., Dixon and Nussbaum (2012); Gheaus (2018); Geisinger (2019); Macleod (2019); Schweiger (2019). [↑](#footnote-ref-16)
16. Following (Yeung 2017: 119) we will refer to companies like these as the “Big Data barons”. [↑](#footnote-ref-17)
17. Lupton (2017) gives an account of how pregnancy apps bring *in utero* fetuses into the data cycle. [↑](#footnote-ref-18)
18. Attempts at this kind of digital manipulation are not uncommon. See Lanzing (2019); Susser, Roessler and Nissenbaum (2019); Shah, Cappella Ramesh and Neuman (2015); Chen and Quan-Haase (2020); Richterich (2018) and Taylor (2020). [↑](#footnote-ref-19)
19. See Giesinger (2019: 221). [↑](#footnote-ref-20)
20. For example, humans have a heuristic that makes them more likely to choose foods placed at the front of a selection. So, if the management of a school cafeteria want the pupils to eat healthier foods, they do not have to exclude unhealthy foods from the selection. By placing the healthy foods at the front of the table and unhealthy

foods at the back, the pupils will unconsciously choose more of the healthy foods (Thaler & Sunstein, 2008: 1). [↑](#footnote-ref-21)
21. Tahir *et al.*, (2019), analysed 5000 videos on YouTube Kids and found 20% to contain “fake, explicit, or violent content”. [↑](#footnote-ref-22)
22. While the effectiveness of this particular campaign may be difficult to determine, empirical studies suggest that targeted, “digital mass-persuasion” using harvested data is not only possible but effective in affecting the behaviour of its targets (e.g. Matz et al, 2017). [↑](#footnote-ref-23)
23. Among other campaigns, Cambridge Analytica used data captured from the Facebook pages of American voters to determine which voters were “persuadable” and used targeted advertising to attempt to sway these voters to vote for Donald Trump in the 2016 US Elections (see Markham, Tiidenberg and Herman, 2018; and Susser, Roessler and Nissenbaum, 2019). They claim to have done something similar in other countries. [↑](#footnote-ref-24)
24. The Facebook Emotional Experiment was an experiment conducted by Facebook employees in collaboration with researchers at top US universities. The experiment tested whether Facebook users could be made to experience negative emotions if their news feeds were filtered to only include negative content. The experiment was successful; however, this resulted in over 300 000 Facebook users being guided to experience negative emotions (see Panger, 2016; and Shaw, 2016). [↑](#footnote-ref-25)
25. Carolan (2018). [↑](#footnote-ref-26)
26. A case could be made that such a company could be required to pass such information on to an appropriate authority, but this issue lies beyond the scope of this paper. [↑](#footnote-ref-27)
27. According to the General Data Protection Regulation of the European Union, consent must be freely given, informed, specific, and unambiguous for it to be deemed legitimate (Van der Hof, 2017: 128). Such legitimate consent would require an autonomous individual to provide it without coercion, influence, or manipulation. [↑](#footnote-ref-28)