IRIE
International Review of Information Ethics Vol. 31 (08/2022)

Authors: Tommaso Crepax and Jan Tobias Mühlberg

Upgrading the protection of children from manipulative and addictive strategies in online games

Legal and technical solutions beyond privacy regulation

Abstract:

Despite the increasing awareness from academia, civil society and media to the issue of child manipulation online, the current EU regulatory system fails at providing sufficient levels of protection. Given the universality of the issue, there is a need to combine and further these scattered efforts into a unitary, multidisciplinary theory of digital manipulation that identifies causes and effects, systematizes the technical and legal knowledge on manipulative and addictive tactics, and to find effective regulatory mechanisms to fill the legislative gaps. In this paper we discuss manipulative and exploitative strategies in the context of online games for children, suggest a number of possible reasons for the failure of the applicable regulatory system, propose an "upgrade" for the regulatory approach to address these risks from the perspective of freedom of thought, and present and discuss technological approaches that allow for the development of games that verifiably protect the privacy and freedoms of players.

Agenda:

ISSN 1614-1687

Author(s):
Tommaso Crepax

- LIDER-Lab, Istituto Dirpolis, Scuola Superiore Sant'Anna, Santa Cecilia 3, 56127 Pisa
- 💻 tommaso.crepax@santannapisa.it

Jan Tobias Mühlberg

- imec-DistriNet, Computer Science, KU Leuven, Celestijnenlaan 200a, 3001 Leuven, Belgium
- ✉ jantobias.muehlberg@cs.kuleuven.be,
- 💻 https://distrinet.cs.kuleuven.be/people/JanTobiasMuhlberg

Introduction

Many online video games are designed to be manipulative, addictive personal data collection machines. Free-to-play ("F2P") mobile games (or "freemiums") exploit established and novel marketing techniques to take advantage of users' weaknesses, nudging them into in-app purchasing of items, and perpetually seek the user's attention.

A substantial portion of freemium consumers are represented by children. Most prominently during middle childhood, children are exceptionally vulnerable to such covert, manipulative marketing tactics and, unaware of the risks that seemingly harmless online games pose to their fundamental rights, they often fall prey to addictive behaviors that put their health and well-being in jeopardy. A current trend in marketing, which is informed by neuroscientific knowledge, boosted by data analytics and machine learning techniques, interferes with children's self-determination and development, health and social life in ways that should undergo renewed legal and ethical scrutiny.

To such imminent threats, the practical implementations in the EU of human rights, consumer protection and digital services regulation, have failed the test of digital reality – mostly, due to a general fixation on regulation based on notice and consent, overestimation of supervisory authorities capabilities and underestimation of effects on children. Meanwhile, the EU's latest regulatory efforts, although overall more aware of the manipulation issue, will only exercise their effects sometimes in the distant future.

Despite the increasing awareness from academia, civil society and media to the issue of child manipulation online, the current EU regulatory system fails at providing sufficient levels of protection. In this paper we discuss manipulative and exploitative strategies in the context of online games for children, suggest a number of possible reasons for the failure of the applicable regulatory system, propose an "upgrade" for the regulatory approach to address these risks from the perspective of freedom of thought, and present and discuss technological approaches that allow for the development of games that verifiably protect the privacy and freedoms of players.

"The capture and re-sale of human attention became the defining industry of our time". With these words, Tim Wu (Wu 2017) summarizes the core mechanics of the *attention economy*. Coined by the psychologist, economist and Nobel laureate Herbert A. Simon (1994), this term describes an economy where the almost infinite vendors can no longer sell products at a price, but must make revenue from capturing, extending, and maximizing user engagement (Commons 2019). Attention is the scarce, precious resource of this extraordinary economy. Product designers are trained on persuasive behavioral design to "play psychological vulnerabilities (consciously and unconsciously)" against users in the race to grab their attention (Harris 2016), necessitated by the prominent "freemium" model, a predatory business model that relies on the "harvesting and analysis of user data, in order to predict and/or manipulate users' preferences, perspectives, and behavior towards commercial or political outcomes" (Zuboff 2019). As the attention economy develops into an attention war, it has competing contenders, an ever-changing arsenal of weapons, it brings harm to the civilian population, and it faces a growing resistance.

The Contenders. Facebook, Twitter, Instagram,[1] Google, but also Epic Games, Blizzard, EA mobile, Roblox, Nintendo, Nyantic, these gigantic corporations and their advertising networks are caught in a zero-sum race for users' finite attention, constantly forced to outperform their competitors using increasingly persuasive techniques (Harris 2016).

The Weapons. The contenders use old and new marketing strategies to harvest attention (Wu 2017). From Pavlov's experiments to condition dogs' behavior, to Fogg's persuasive technology (Fogg 2002), behavioral and neuro-sciences have fed marketing research with deeper knowledge to understand and condition

[1] For the latest revelations on Facebook's own internal research on effects of Instagram on teenage girls, *see* https://www.theguardian.com/technology/2021/sep/30/facebook-hearing-testimony-instagram-impact

consumers' behavior.[2] Developers introduce addiction-by-design (Schüll 2012) and compulsion-by-design (Kidron et al. 2018) in their services, by applying nudges,[3] sludges, dark patterns, and algorithms that produce personalized content. A mixture of big data analytics, machine learning and neuromarketing boost old, and create new marketing strategies. Owning data – despite the debate of what data ownership means in legal terms (Duch-Brown, Martens, and Mueller-Langer 2017)– drives the entire digital ecosystem, as data is the means, the informational source to develop systems that capture and retain attention. If attention is the oil, then data is the drill to extract it.

The Civilians. Strategies designed to drive and extend user engagement are central to many of the online services that *children* use. This is as true for online games as it is for social media, online streaming services, or search engines (Kidron et al. 2018; Council 2018). Children are one third of internet users and, as a substantial portion of freemium games players, they are caught unguarded in the war for attention. As Baroness Beeban Kidron puts it, "the current asymmetry of power between the developing child and the most powerful companies in the world is hardly caring, and certainly not in the child's best interest" (Kidron et al. 2018). In this paper, we identify the "developing child" as players during their middle childhood (ages 7 through 12). This age is significant because it marks the time when, on one hand, children's highly plastic brain is biologically predisposed to absorb ever more complex information, while their critical thinking, on the other, is not sufficiently formed (Blumberg et al. 2019). As "godlike technologies" take advantage of children's "paleolithic emotions" (Wilson 2017), the legal, social and ethical systems nowadays in place are not succeeding at ensuring decent levels of protection (Livingstone et al. 2018) (cf. Section 3).

…and the Resistance! Meanwhile, international organizations, academia, civil society and many other initiatives worldwide are devoting efforts into showing the detrimental effects of gaming as well as to understanding the marketing tactics in the digital domain –most notably, in 2018 the World Health Organization added gaming disorders to the list of addictive behaviors. Responses to this problem are varied, ranging from individuating manipulative tactics and developing lists and categorizations of nudges, sludges and dark patterns,[4] to more general approaches to protect childrens' digital well-being,[5] trough developing technical controls and Privacy Enhancing Technologies specifically for children,[6] or asking the industry to adopt codes of ethics, and governments to take political and legal actions (Kidron et al. 2018; Livingstone et al. 2018; Harris 2016).

Although it is admirable that the problem of digital manipulation is getting attention from multiple stakeholders, its solution is *time consuming* and *complex*. Time-consuming, because an exhaustive solution would need a profound, critical social revision of policies concerning the endangerment of children for commercial purposes through data exploitation; complex, because alongside societal pressure and political changes, technological solutions are needed *now* to momentarily dab the bleeding with immediately actionable responses. That is, under the hypothesis that once the player's data finds its way into exploitative advertising networks, the (ab-)use of this data can no longer be controlled or supervised. Thus, we discuss technological approaches to verifiably minimize such data leakage.

This paper aims to pave the way for the regulatory solution and provide a technological option as a potential immediate fix but also to ease the enforcement of regulatory approaches. To reach these goals, this paper discusses the following *Research Questions*:

[2] Matthews clarifies: "Neuromarketing is simply an expected recruitment of an available technology that widens an already impressive suite of existing techniques for hidden persuasion" (Matthews 2015).

[3] Cf. "Nudge: The Final Edition" by Thaler and Sunstein; as well as ongoing works of the *5Rights Foundation*, algotransparency.org, and Tristan Harris

[4] (E.g., 5Rights Foundations (Kidron et al. 2018); Norwegian Consumer council (Council 2018); Center for Humane Technology; NeuroRights Initiative; AlgoTransparency project).

[5] E.g., BetterInternet4Kids; OECD (OECD 2021); EU funded project Gam(e)(a)ble), available at https://www.gameable.info/

[6] E.g., IEEE Standard Association report on Children's Data Governance Applied Case Studies at https://standards.ieee.org/initiatives/artificial-intelligence-systems/childrens-data-governance.html; EU funded PDP4E forthcoming paper "Information Technologies exposing Children to Privacy Risks: Domains and Children-Specific Technical Controls," by Crepax *et al.*

1 Is the current European focus on privacy and data protection adequate to protect children from manipulative and addictive neuromarketing techniques in online games, or is it necessary to *upgrade* the focus to the protection of children's right to freedom of thought?
2 What technical solutions can be implemented to support a privacy-by-design approach to develop game engines that verifiably guarantee that player data cannot be extracted by the game server operator?

Online gaming: the paradise of children profiling, manipulation and addiction

The likelihood that children experience harms, as well as their severity, are directly linked to the amount and sensitivity of data being accumulated. A substantial portion of children's "datafication" (Lupton and Williamson 2017)[7] happens through the generation and collection of massive amounts of online gaming data (Russell, Reidenberg, and Moon 2018; Newman and Jerome 2014; Sax and Ausloos 2021). In fact, game developers wallow in "dataveillance" (Lupton and Williamson 2017),[8] the process of continuously monitoring, tracking and evaluating activities happening in the children's real and virtual world. Profiting from In-App Purchases (IAPs) or third-party advertising, Free-to-Play (F2P) games depend on the skill of the developer to persuade users into buying items, clicking on ads or attract more players: this is done by feeding hyper-personalized content and manipulation through nudging techniques.

Manipulation's success depends on personalization, which is informed through heterogeneous data collection and processing. Physical world data are collected through sensors (cameras, microphones, accelerometers, GPS antennas) while virtual world data are collected through a users' interactions with the game software (Sax and Ausloos 2021; Newman and Jerome 2014; Kröger et al. 2021). The cycle of processing, called game telemetry,[9] starts with the collection of raw game input. Raw game data subsequently feeds game analytics – the process for discovering and communicating patterns in game data. Finally, game data is connected to single players, becoming "player metrics" (Newman and Jerome 2014). Game analytics and its use to infer player metrics are mature techniques that are employed in online games for more than a decade (e.g., Hullett et al. 2021; El-Nasr et al. (eds.) 2013). A recent survey of this field (Su et al. 2021) concludes that game analytics "can provide a service-oriented decision system through data analysis to guide the whole game industry, especially for the game publishing analytics, which can help acquire players, maintain players, and maximize game revenue effectively."

Following El-Nasr et al. (eds.) 2013 and Su et al. 2021, game analytics and player metrics are most commonly used during game development to improve the playing experience, to retain players and maximize revenue, and for marketing purposes. Player metrics analysis are used to *observe* and *infer* information off the player: *physical data* such as reflexes, handedness, dexterity are used to create a physical profile, or, through further evaluation and scoring, can infer information about the player's health: anomalies in sleeping patterns, state of general health (enough sleep, food, eye rest) or existence of specific diseases (epilepsy, abnormal dexterity or reflexes, neurological diseases, dementia, disability, OCDs, depression).[10] Adding levels of abstraction, psychological mechanisms may be used to extract in real time, or predict *"mental data"*, such as feelings, emotions, thoughts: behavioral preferences,[11] sexual preferences,[12] propensity for gaming addiction, and more (Madigan 2015; Ienca and Malgieri 2021). All such highly sensitive information, the essence of human weaknesses, become vulnerabilities to exploit by the competitors in the attention economy. Recently, journalists revealed that detailed profiling using similar approaches to game analytics is also applied in online gambling. The investigation highlights a company that maintains "detailed personal

[7] Information Commissioner's Office (U.K.) (2020), Age appropriate design code – Executive summary.

[8] Dataveillance is the "monitoring and evaluation of children by themselves or others that may include recording and assessing details of their appearance, growth, development, health, social relationships, moods, behaviour, educational achievements and other features.

[9] See https://towardsdatascience.com/evolution-of-game-analytics-platforms-4b9efcb4a093

[10] As seen in, e.g., the game Minecraft with assumptions made on different levels of completion [100%] (Ringland 2019), or in choices of colors as potential signs of depression.

[11] Player categorization according to Bartle's taxonomy: killer, achiever, socializer, explorer, see e.g. https://www.essex.ac.uk/people/bartl01006/richard-bartle

[12] From gender of character, or customization of characters, through clothes, hairstyle, etc.

profiles revealing intimate gambling behaviour. The files contained 186 separate attributes for a single individual, which painted a detailed and personal portrait of their gambling behaviour, including their propensity to gamble, favourite games, and susceptibility to marketing."[13]

Profiling in gaming

"*The old adage of big data having volume, velocity, variety and volatility holds very true for behavioral telemetry from games*" (Sifa, Drachen, and Bauckhage 2018)

Telemetry-driven behavioral profiling.

While players do volunteer some personal data, the vast majority is acquired by observation, derived through analysis, or inferred probabilistically off the *unaware subject* (Sartor, Lagioia, and Galli 2021; Ienca and Malgieri 2021; Onnela and Rauch 2016). The constant growth of training data volume generated by telemetry-driven behavioral profiling of thousands – sometimes hundreds of millions–[14] of players worldwide feeds supervised machine learning algorithms with accurate, labeled data classes to create nearly-perfect user profiles; reinforcement learning algorithms, mimicking humans "rewards seeking" actions (Schultz, Dayan, and Montague 1997), improve at predicting behaviors by exploiting rewards signals embedded by design in the software code; unsupervised learning algorithms fed by raw data find unanticipated users' clusters, affiliations and anomalies. Thanks to data analytics, AI and machine learning techniques, the game gets to know the users and exploit what triggers them.

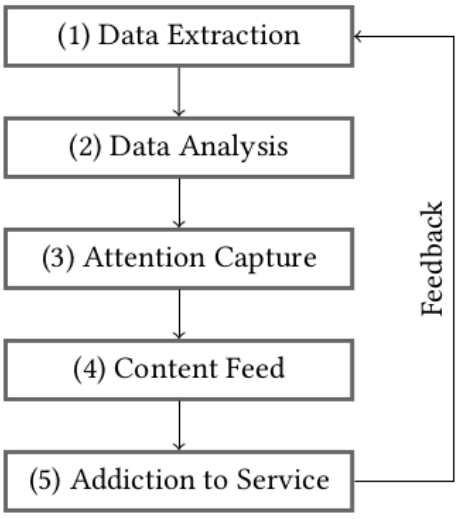

Fig. 1. Addiction process: from personal data extraction to user addiction.

The ability to predict which users will turn into long-term players, social network enablers and/or buyers of in-game content enables an optimization of Customer Relationship Management, and the tailoring of game

[13] "Investigation reveals scale of behavioural surveillance by online gambling firms", https://cleanupgambling.com/news/cracked-labs, 2022-01-26

[14] *See*, e.g., the number of players of Fortnite in 2021 https://bit.ly/3mgl07u

content to the specific profiles of these users (Sifa, Drachen, and Bauckhage 2018). Much like professionals at chicken sexing,[15] shallow profiling algorithms must individuate churners and buyers in as little time as possible (*circa* 20 minutes (Newman and Jerome 2014)). Deep profiling, instead, provides a toolbox for integrating varied player behaviors and experimenting on potential correlations with player psychology (Sifa, Drachen, and Bauckhage 2018) through unsupervised machine learning. The process can be simplified in the following tasks: *extraction and analysis* of data on user to understand weaknesses, *capture* of attention through manipulative tactics, *feeding* ever personalized content until *addiction* to service is achieved (*See Fig.* [fig:addictionprocess]).

Psychological profiling and neuromarketing.

In such hyper-competitive market for attention, where games' designs are based on customers' data, telemetry-driven behavioral profiling[16] is only the *quantitative* side of the medal. The *qualitative* side is *psychological profiling*. Marketers exploit psychographics, user-testing, surveys, focus-groups for customer modeling based on *self-reported* consumer's emotions, values, personality traits,[17] lifestyle, opinions, interests, and try to build an understanding of the psychological state of the player at points in the future.[18]

Psychological profiling based on market research techniques may still suffer from inaccurate measurements due to qualitative self-reporting biases in the samples (Wright 1997; Ford 2019; Canli 2006). Therefore, to the problem of precise quantification of mental processes, neuroscience applied to marketing, although in its infancy (Ramsøy 2019), provides promising answers (Swan 2012): born to study mechanisms to understand the consumer's behavior (Smidts 2002), neuromarketing exploits physiological-measuring techniques such as eyetracking, pupilometry, EEG, fMRI, facial coding, sensory marketing, as well as psychographics (Kenning and Linzmajer 2011), to measure targeted people's emotions and feelings (Lindstrom 2010) in reaction to stimuli (graphic lines, content or ads) at *subconscious* level.

Input from neuromarketing findings are coded by developers into video games design, translated into more attractive graphic lines, landing pages and microsites. Stimulated by using an uninterrupted series of targeted persuasion attempts (Wilson, Gaines, and Hill 2008), when the users finally desist from playing, they start receiving timed alerts or push notifications (Kidron et al. 2018) that pull them back into the game.[19]

Manipulative and addictive tactics.

The manipulative and addictive tactics, designed over neuroscientific evidence into most digital services available on the Internet, are irrespective of that there is a high chance (one in three (Livingstone, Carr, and Byrne 2016)) that the user is a child. Although some manipulative tactics may come from the unintentional, naive use of well-established persuasive design tactics, other come from the conscious, malevolent choice of the developers of a service for a child, or because the service, albeit not for children, is accessed by children nonetheless –in fact, most age verification systems fail at determining age (Pasquale and Zippo 2020).

There are "literally thousands" (Harris 2016) of "sticky features" to hijack users' minds, divided into *nudge* features, that push users into behaviors that are in the commercial interest of services, and *sludge* features, that are barriers to users making decisions in their own interests (Kidron et al. 2018): tactics range from controlling menu choices, to exploiting reward loops,[20] or fears of missing something important; items can be "like" buttons to stimulate social reciprocity, infinite feeds, video autoplay, instant interruptions, daily login

[15] See https://psmag.com/magazine/the-lucrative-art-of-chicken-sexing

[16] It is a mix of snapshot, dynamic, contextual and spatio-temporal profiling

[17] E.g., D.W. Fisk's OCEAN model, acronym for Openness, Consciousness, Extraversion, Agreeableness and Neuroticism

[18] Which in the "human futures market", as said in (Zuboff 2019), is the sale of what we will do next (Alegre 2021a)

[19] See U.K. Research and Innovation (UKRI)'s written evidence for the Immersive and Addictive Technologies Report

[20] The idea is one of putting "slot machines in users' pockets"

and streaks rewards, no save-no pause defaults, limited time offers, coins-for-ad watching, burning graphics, pull to refresh and swipe mechanisms, timed alerts, push notifications, "summons" such as buzzes, pings, vibrations, or even the color red (Kidron et al. 2018; Sax and Ausloos 2021, 2021; Sher 2011).

There is an emerging –yet underdeveloped (Melzer et al., 2021)– body of literature specifically on addictive game design that addresses the interplays among freemium content, ethics and youth. Such literature shows overall consensus that the freemium model has negatively impacted on game design [(Alha, 2020),(Karlsen, 2021)], for instance through imposing the necessity of ever increasing predatory (King and Delfabbro 2018) "loot boxes" (Karlsen, 2020), mostly due to challenging monetization mechanics (Karlsen, 2021). Interviews with informants from game design companies with different business models showed that freemium companies, as opposed to premium and indie developers, tend to downplay ethical responsibilities. This is because, as one freemium developer said, it is "literally impossible to launch an ethical game on the App Store" (Karlsen, 2021), stressing that freemium developers *need* to manipulate players into micro purchases. In response to such industry's need, some solution seekers suggested the use of framework like the App Dark Design (ADD) to critically evaluate the design of freemium apps (Fitton & Read, 2019), which, combined with works on identification of technical controls designed specifically to protect children's privacy (Crepax et al., 2022)**,** could help game developers in making ethical game design choices.

Effects of manipulative and addictive content on children

In this attention economy driven by AI and big personal data analytics, the impact on users is unprecedented and unforeseeable (Zuboff 2019), but surely significant and severe. In fact, in 2019, the Committee of Ministers of the Council of Europe produced a Declaration "on the manipulative capabilities of algorithmic processes" (hereinafter, the "Declaration"), where they remark:

"Fine grained, sub-conscious and personalized levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions. These effects remain underexplored but cannot be underestimated. Not only may they weaken the exercise and enjoyment of individual human rights, but they may lead to the corrosion of the very foundation of the Council of Europe. Its central pillars of human rights, democracy and the rule of law are grounded on the fundamental belief in the equality and dignity of all humans as independent moral agents."

Persuasive design strategies, deployed to maximize the collection of personal data, disturb children's social, mental and physical development (Kidron et al. 2018).

Harms include immediate effects on individual consumers as well as long-term effects on society, and span over a wide range of categories, from harms to human rights, to physical and psychological harms, through social harms. The involved rights include positive rights to privacy, autonomy, and dignity as well as negative rights not to be deceived, subjected to experiments without consent, or used as a means (Stanton, Sinnott-Armstrong, and Huettel 2017). Personal harms include anxiety, social aggression, denuded relationships, sleep deprivation, impacts on education, health and wellbeing (Kidron et al. 2018), psychosocial and financial harms, withdrawal from real life, heightened attention-deficit symptoms (Carr 2020), impaired emotional and social intelligence, technology addiction, social isolation, impaired brain development, and disrupted sleep (Small et al. 2020). Because of young children's high brain plasticity, there may be consequences due to the normalization of gambling (Drummond and Sauer, 2018) .[21] Scientific literature is increasingly coming to the conclusion that addiction is at least a disease of free will (Koob and Volkow 2016), and at worst a brain disease (Fenton and Wiers 2017; Leshner 1997). As not only is attention finite, but also the "bottleneck of human thought" (Simon 1994), providing only content that pleases the child's interests takes their attention away from diverging content and is a hindrance to develop robust critical thinking. Finally, Small (Small et al.

[21] Henrietta Bowden-Jones notes: "Habits learnt in childhood require significant intervention, and that habits formed before the age of nine take considerable interventions to change in adulthood. Given that many of the techniques used in gambling are deployed both in online games and other kinds of services used by children, this should be a source of real concern", https://www.healthtechdigital.com/video-games-are-pushing-children-into-gambling-warns-englands-top-mental-health-nurse/

2020) has demonstrated that "Internet addiction shares features with substance-use disorders or pathological gambling".

As an answer to these dramatic risks, there have been some authoritative recognition of problematic gaming and calls for action. The United Kingdom Chief Medical Officers' commentary on "Screen-based activities and children and young people's mental health and psychosocial wellbeing" has called on the technology industry to "develop structures and remove addictive capabilities' from their services". Meanwhile, the World Health Organization has included gaming disorder in the 11th Revision of the International Classification of Diseases (ICD-11), defining it as a pattern of gaming behavior ("digital-gaming" or "video-gaming") characterized by "impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences".

A number of authors note the importance of media literacy for children and parents, together with parental supervision, to mitigate risks stemming from online interactions (e.g. Griffiths 2015; Smith and Shade 2018). However, studies reveal that these approaches may reduce risks –without eliminating them (Steeves and Webster 2007), vary substantially in effectiveness depending on the type of parental mediation and the age group of the children (Lwin et al. 2008), and suffer from increasing privacy and consent fatigue, which is promoted by the opaqueness of online systems (Hargittai and Marwick 2016). It is argued that specifically this opaqueness, leading to "consent overload, information overload, complexity of data processing, and lack of actual choice," also renders parental consent a highly questionable basis for the lawful processing of children's data and an inadequate choice for the protection of children's fundamental rights (cf. van der Hof and Lievens 2018). In the following we discuss the ethics and harmful impact of digital manipulation; we then revisit legal challenges, such as using consent as a basis for data processing.

Neuromarketing and ethics

"The mind, unconquered by violent passions, is a citadel, for a man has no fortress more impregnable in which to find refuge and remain safe forever"

Marco Aurelio, *A sé stesso*

The harms of digital manipulation impact on ethical aspects too. Increasingly, companies are developing the ability to unobtrusively observe and predict neurological states and functions, as well as to manipulate emotions (Zuboff 2019). "Stealthy neuromarketing" (Murphy, Illes, and Reiner 2008), the manipulation of oblivious consumers with the intent to addict and profit, limits their *free will* using them as means to an end, violating at once Rawlsian as well as Kantian ethics (Wilson, Gaines, and Hill 2008; Greene and Cohen 2004). As behavioral science, neuro-science and deep learning techniques increasingly confirm the substantial impact of biology on decision making and action (Fukuyama 2003; Durante et al. 2011), they are also sabotaging the Renaissance concept of human autonomy; the use of stealthy neuromarketing applied to children in gaming puts into question the respect of fundamental ethical notions of agency (Wilson, Gaines, and Hill 2008), privacy (Brownsword 2012), freedom of thought (McCarthy-Jones 2019) and mental integrity (Ienca and Andorno 2017).

Understanding the exact point where acceptable persuasion becomes unacceptable manipulation is one of the crucial issues for the regulation of digital manipulation (Alegre 2021a). Luckily, the literature on marketing ethics on the topic of persuasion *v.* manipulation in advertising is lively and abundant (De Jans et al. 2019). Among many others, some authoritative views are represented by Crisp, (Crisp 1987) who blames amorality on all forms of advertising that override the autonomy of consumers; Arrington, who makes it a question about what level of persuasion is the standard person assumed to withstand (Arrington 1982); and Aylsworth, who allows for manipulations, but only for ends that people accept and by means they endorse (Aylsworth 2020). As the theoretical debate develops, some tried to create practical methodologies to distinguish ethical

from unethical persuasions (Baker and Martinson 2001), but new research is needed to keep pace with the digital evolution (Clarke and Svanaes 2012).

As the debate follows on, unethical combination of tactics manipulate users toward the least privacy friendly options, jeopardizing the genuineness of consent (Council 2018). The public and academic skepticism (Fischbach and Mindes 2011) about uses of manipulating techniques (Wardlaw et al. 2011) has called upon governments and market regulators to act, as well as upon industry to adopt ethical guidelines, etc (Murphy, Illes, and Reiner 2008). Manipulating children for commercial purposes and enslaving them to addictive content is not the type of digital future that society should wish for, but one that discredits human dignity, creativity and diversity of thought. The inviolable freedom of thought and opinion is described as "the foundation of democratic society", "the basis and origin of all other rights", without which freedom to think for ourselves "we lose our freedom to be human" (Alegre 2021b).

Legal challenges

Considering the severity of effects (*see Section* 2), it is surprising that there still are freemium games with manipulative and addictive features available to children on easily accessible stores.

In such a complex context, the causes to the problem are various in nature (technical, commercial, social, etc.) and intertwined (*see Sections* 1.1, 2.1). It is unquestionable that the law, as one of the main means of regulation (Lessig 2009), did have an impact on the current situation, so what is important to understand is *what* caused the legal system to fail at children protection, and *how* to fix it. As there is no specific, unitary study on the matter, this paper is an attempt to fill such gaps.

Some causes of the failure might be rooted in the *vexata quaestio* of the efficacy of regulation based on risk together with notice and consent mechanisms, especially in regards to parental consent (Gilbert, Parton, and Skivenes 2011; Lievens et al. 2018; Livingstone et al. 2018; Verdoodt 2020; Livingstone, Stoilova, and Nandagiri 2018). A substantial portion of the legal scholarship is skeptical about the efficacy of privacy notices (for a comprehensive review on the topic *see* (Van den Berg and Van der Hof 2012), but also (Barocas and Nissenbaum 2009; Sloan and Warner 2014; Acquisti et al. 2017; Macenaite and Kosta 2017; Hartzog 2018; Schaub et al. 2015; Ben-Shahar and Schneider 2014))[22]. Authoritative champion of this faction, Sartor claims that data subjects' opportunity to consent to risks they cannot foresee is not an *asset* for them, but a *liability* (Sartor, Lagioia, and Galli 2021).[23] Moreover, abundant research in the fields of behavioral decisions, behavioral economics and experimental psychology applied to privacy by Acquisti *et al.* individuated privacy decision making hurdles that affect – if not altogether invalidate – regulative efforts based on the "privacy calculus" (*e.g.*, rules on consent as a legal basis for data processing). They claim that incomplete and asymmetric information, heuristics and bounded rationality, and cognitive and behavioral biases (Acquisti et al. 2017) on the side of the data subject mine the foundations of the "privacy calculus" (Laufer and Wolfe 1977), the theory of individual rational choice positing that data subjects are agents with stable preferences in regards to privacy.

[22] Data protection became the law of everything which is "impossible to maintain" (Purtova 2018) – and enforce, and as an essential "right to a rule" (Dalla Corte 2020) its enforcement depends on the interest to uphold the rule – so long as the subject to it understands why the rule is there in the first place. Larose and Rifon (LaRose and Rifon 2007) bring about the idea of data protection as protection against risks to data subjects' *safety*. To them, the problem is one of "personal safety protection" as they critic the inadequacies of privacy policies models that do not motivate "consumers to take protective actions". Data subjects are like consumers who need means to "consider the potential consequences (…) associated with personal information disclosures", so that "they can make informed choices and enact appropriate behaviors that will shield them from online privacy threats".

[23] Sartor et *al.* believe that "consent has been abused as a legal basis for targeted advertising" (Sartor, Lagioia, and Galli 2021 p 20). "The data subjects' power to consent or object to the processing of their personal data cannot be described as an asset – a power to determine how they want their data to be processed – but rather becomes a liability, something that makes them liable to surrender to any request made by businesses and platforms they interact with". Similarly, the Article 29 working Party, in their "Guidelines on consent under Regulation 2016/679" state that: "If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes *illusory* and consent will be an invalid basis for processing, (…)".

As for newer, less debated causes of the failure, the following are worth developing.

One cause could be that existing regulatory frameworks, although based on risks, are not receptive of the scientific evidence of risks and consequences of manipulative and addictive content (Sax and Ausloos 2021). It seems that there is a lack of subsumption of health, social and psychological knowledge about gaming disorders into law, and the problem might relate to multiple causes. On one hand, effects on children will only be visible in many years; on the other, only the most visible ones will be measurable – think of incidence on rising gambling practices, or gaming disorders that need medical attention –, whereas "softer" effects, such as lack of compassion due to scarce critical thinking, radicalization, devaluation of relationships, normalization of gambling, and so on, will be harder to prove. Moreover, companies, such as Facebook, who are best suited to study the effects of their services on children, might cover their research showing that one of their most famous services, tht is Instagram, is "toxic" to teenage girls.[24]

Another cause could be that the applicable legal framework is too complex and incoherent (*see Table [tab:LegalAquis]*). It seems that the increasing addition of gaming features for attention capturing (Owen et al. 2013; Blades et al. 2014; Van Reijmersdal et al. 2010; Waiguny, Nelson, and Terlutter 2014) might have broadened the regulatory framework of online gaming so that it became too complex to be effective (Sax and Ausloos 2021; Livingstone et al. 2018). If games might trigger regulation by consumer rights, data protection, audiovisual media, marketing, digital content, products safety, national gambling, health and criminal law, there is a chance that over-regulation is jeopardizing rights enforcement.[25] The latter is likely the case in the EU, where a report from the Irish Council for Civil Liberties shows that Europe has an *enforcement paralysis*, and is "unable to police how big tech firms use people's data."[26]

In response to problems of children protection, academia, international organizations and civil society[27] have asked the industry, regulatory authorities and policy makers to resort to actions. The request to action vary from identifying and grading impacts of persuasive design features, to creating a "fair game" charter with "ethically child-centric standards" (Kidron et al. 2018; Livingstone, Stoilova, and Nandagiri 2019; Murphy, Illes, and Reiner 2008), through taking a public health approach,[28] or creating new privacy preserving technologies and standards.[29]

In the EU, only the U.K. government has reacted to these requests by approving the Age Appropriate Design Code, a set of 15 flexible standards to which all organizations shall conform to as of September 2, 2021. Conforming to the code is necessary to comply with data protection laws and should "ensure that an organization providing online services likely to be accessed by children in the UK takes into account the best interests of the child".[30] The standards are enforced on a proportionate and risk-based approach, thus they do not prescribe or ban specific manipulative tactics; however, concepts such as the "detrimental use of data" standard are definitely worth exploring in upcoming policy making efforts.

Some of the recent proposals for future EU Regulations might also bear some positive effects (*see Table* "Potentially applicable EU laws and provisions"), especially the draft AI Act which, in art. 5 sec. b) specifically prohibits "the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behavior of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm". Unfortunately, the legislative *iter* for

[24] *See* https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=hp_lead_pos7&mod=article_inline

[25] Regulation should have adapted to the rapid changes in the *medium* without letting the responsibilities and protections of "this inter-disciplinary concern that often falls in between established mandates of relevant authorities" (*See* CoE Declaration) to be scattered. Moreover, "despite the growing importance of embedded advertising, many of the new ad formats remain neglected (e.g. native and mobile advertising) (De Jans et al. 2019).

[26] *See* https://www.iccl.ie/digital-data/2021-gdpr-report/

[27] E.g., UNICEF, 5rights Foundation, Center for Humane Technology, EUkidsonline.net, and more.

[28] *See* https://www.healthtechdigital.com/video-games-are-pushing-children-into-gambling-warns-englands-top-mental-health-nurse/

[29] *See* the work of IEEE Standards Association at https://engagestandards.ieee.org/childrens-data-gov-webinar-register.html

[30] The Information Commissioner's Office, available at https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/executive-summary/

this proposal is far from finished (the proposal is being discussed by the Parliament and Council separately); moreover, there is already authoritative criticism about the AI Act by the European Data Protection Board and the European Data Protection Supervisor jointly, as well as by Malgieri and Ienca, the latter noting that the AI Act fails at protecting the "mind" of data subjects by forgetting to "explicitly include in the high-risk list the AI systems that rely on mental information such as emotion recognition systems (in any form) and digital nudgers".[31]

As a conclusive remark, and notwithstanding the inaction of most European countries, it is not guaranteed that once the mentioned legal causes are fixed, the bigger problem of children's digital manipulation would be automatically solved too. In fact, studies on policies *versus* gaming addiction by Kiraly *et al.* show that countries that are trying to address gaming problems through different classes of policy attempts are failing at it. Measures limiting availability of video games (e.g., shutdown policy, fatigue system, and parental controls), reduce risk and harm (e.g., warning messages), or help services for addicted players have proven to be *ineffective* (Király et al. 2018). The reason, the authors say, may be that such measures and policies "only addressed or influenced specific aspects of the problem instead of using a more integrative approach." Therefore, the question: what could this "more integrative approach" be? In the following sections we make two complementary proposals to address this question, one technical and one legal.

Potentially applicable EU laws and provisions

Topic	**Legislative Act**
Information Society and Media	Audio Visual Media Service Directive (amended, 2018)
Judiciary and Fundamental Rights	Charter of Fundamental Rights of the European Union ("Charter")
	European Convention on Human Rights (CoE)
	UN Convention on the Rights of the Child ("UNCRC")
	Universal Declaration of Human Rights (UN)
	International Covenant of Civil and Political Rights (UN)
Information Society and Media / Justice, Freedom and Security	Directive combating the sexual abuse and sexual exploitation of children and child pornography
	Convention 108 (+) (CoE)
	General Data Protection Regulation

[31] *See* https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/

	ePrivacy directive
	Unfair Commercial Practices Directive
	Digital Content Directive
	Consumer Rights Directive
	Proposal for Regulation of: Artificial Intelligence, ePrivacy, Digital Services, Digital Markets, Data Governance

Tech support for auditably privacy-preserving gaming platforms

In the simplest terms, the ability to create personalized addictive content from the side of the game provider is based on their ability to collect and process fine-granular player data. In this section we focus on a development approach that allows for games to be designed so as to allow users to interact with the software, without the game provider being able to tap into the interaction. Then, the provider would not be able to tailor more targeted content.

Across the space of privacy-preserving technologies, researchers and industry made a range of proposals, and built scalable infrastructures for storage and processing of data with strong confidentiality guarantees. For example, end-to-end encrypted cloud storage allows users to store data on centralized infrastructure without the infrastructure operator being able to access this data. Similarly, end-to-end encrypted messaging services allow users to interact without the provider to listen in on the exchanged information. On top of that, messaging services with a focus on privacy, such as Signal (signal 2021), take this a step further and hide the social graph of communicating user from the infrastructure and service provider, in addition to also protecting message confidentiality.

Confidential computing

Technically this notion of privacy-preserving confidential messaging is achieved by leveraging concepts of *confidential computing*. In the case of Signal, for example, TEEs (Maene et al. 2017) are used to protect the service-side of the contact discovery mechanism from interference by compromised infrastructure or from the service provider (moxie0 2017): the service has published a contact discovery protocol that is designed to not reveal a user's social graph to the service by relying on irreversibly hashed user identifiers only. The privacy-preserving properties of this protocol also rely on the correct implementation of its service-side. To establish trust into this implementation, Signal open-sourced the implementation and reproducibly links the source code to the compiled service, and is executing the resulting code in an *enclave*[32] in a server-side TEE. A client can then securely connect to the enclave and obtain cryptographic proof that they are indeed interacting with the intended remote software through a process called *attestation*. All this happens before the user transmits their hashed contacts to the service, to establish a prior notion of trust. The verifiable guarantee for the user, which results from the protocol briefly outlined above, is that the Signal service persists no knowledge of a user's social graph. Therefore the service cannot abuse or impart such knowledge for personal gain, or if it is compromised by an attacker or subpoenaed.

[32] The term "enclave" was coined by Intel to denote isolated software execution in untrusted environments (e.g., on other people's computers), where hardware-based isolation mechanisms guarantee that potentially compromised system software cannot interfere with the integrity and confidentiality with code execution inside the enclave.

Zero-knowledge gaming

In this paper we outline and discuss a proposal to use technologies similar to the "enclaved contact discovery" in the gaming sector. In our vision, online games should be designed to minimize the possibilities to collect or extract personal data, including non personal data that might become personal through extensive processing and aggregation. This can be achieved by compartmentalizing a game into several components, which are then individually protected by means of enclaved execution. Such a compartmentalization should depend on the extent to which a component interacts with the user, processes personal data, but may also reflect whether these components contain critical intellectual property of the game producer. Privacy threat modeling techniques such as LINDDUN (Wuyts, Sion, and Joosen 2020) can help with making privacy-conscious choices in this compartmentalization process. The resulting components can then be individually audited and assessed, and depending on their sensitivity, be enclaved as necessary. This would lead to a notion of *zero-knowledge gaming*,[33] where a gaming service may gain very little knowledge about how users are using the service. The strategy for a user to acquire trust in a game can then proceed, like in the case of the Signal messenger, from a game component on the user's device which attests the trustworthiness and integrity of remote components before passing on data that could be used for extended user profiling. Ideally, all such sensitive components should be open-source, be independently assessed not to store or leak sensitive data, and be reproducibly built from the assessed source code. Sensitive game components may, however, pass pseudonymized, anonymized, or otherwise aggregated user data to less sensitive game components. We believe that such a strategy does not hinder the development of interesting game content, but makes information flows explicit and reproducible for interested communities or designated authorities, and verifiable by the users –under the assumption that they want to trust their devices and the locally executing game components.

A concrete example: Shufflepuck

To give a brief example of such a compartmentalization strategy for a mobile simulation of the game *table shuffleboard*.[34] Two players push simulated weights down a long table, aiming to hit a scoring area at the opposite end of that table, which is defended by the opposing player. For this game, we would consider two software components: *(1)* a mobile app, which communicates with *(2)* a server component. The server would receive user inputs (shooting angles, force, defensive actions) from the players' apps, it would then compute the respective outcomes of the players actions, and communicate these back to the apps, which visualize the game and process inputs from the mobile devices' sensors. All software components – the app as well as the server – could technically profile users and use profiling data for purposes not intended by the users. This could be basic information about players' contact details and who likes to play with whom (a social graph!) but also delicate information such as someone's playing skills, reaction times, and their behavior when they win or lose. In our model, a core component of the game app would be assessed and reproducibly built to only communicate user inputs (encrypted and integrity-protected) to an attested server component. That server component would be independently audited to not persist or leak the information received. It might very well propagate a high-score table or similar aggregated information. Also other game components, e.g. for visualization, can receive aggregated, pseudonymized or anonymized information from the core components, allowing for intellectual property to be protected in these components.

The essential property of our proposal is that personal information flows are being made explicit, auditable, and verifiable from the user's device. In games where players interact or compete, personal data needs to be

[33] Zero-knowledge gaming is a reference to "zero-knowledge proofs", a group of cryptographic protocols that allow a party to prove knowledge of a secret to another party without revealing that secret.

[34] Computer simulations of this game have a long history. More experienced readers might remember the famous Shufflepuck Cafè (cf. https://en.wikipedia.org/wiki/Shufflepuck_Cafe).

used to distinguish individual players, to associate these players with natural persons, and keep scores.[35] We argue that such data accumulation can be rendered independent of in-game data, without losing reproducibility. As such, our proposal dramatically reduces the possibilities for a mobile game to record, store, and proliferate in-game data without this being flagged during an audit or being reported as an integrity breach in a game component. On the side of mobile apps, users already enjoy a certain level of protection from malicious apps and spyware, as these are (automatically) audited by mobile OS vendors.[36] The remote component of online games is currently not part of such audits, which our proposal strives to address.

Limitations & Challenges

Of course, our design has a few drawbacks. For example, game developers may be scared by the additional complexity introduced by compartmentalization and TEE features. Ongoing work (Scopelliti et al. 2021) aims to address this by providing cross-platform abstractions to build distributed TEE applications. We are critically aware of the dangers of working with (often proprietary) hardware-based TEE platforms. Proposals to provide similar security and privacy guarantees in the context of discovering social graphs but without trusted hardware do exist (e.g., Demmler et al. 2018; Kales et al. 2019), yet, these have not been implemented in mainstream messaging services. A range of attacks against hardware security frameworks that may compromise the security of a contact discovery approach such as Signal's have been published (e.g., Schaik et al. 2020) and we deem research on securing processors and cryptographic algorithms as orthogonal to our proposal. Ongoing work in the space of homomorphic encryption, zero-knowledge protocols, and secure multi-party computations may be capable of providing the confidentiality and authenticity guarantees of TEEs without relying on specific hardware support.

Remaining issues may, however, be with performance and scalability for certain highly interactive and computationally intensive games. In the case of games for smaller children, where additional transparency and enforcement of data protection may be most needed, we do not see such constraints. We further allow for a notion of end-to-end encryption in multi-player online games, which makes it impossible for the gaming service or third parties to trace fraud (e.g., in-game cheating or fraudulent player item trading between players) or abuse (e.g., verbal abuse or grooming through an in-game chat). Thus, games must be designed not to have features that can lead to fraud or abuse. Ultimately, we believe that user's trust is a key element of a privacy-preserving gaming platform but, regrettably, it is no easy task to gain trust in such a platform. In our case, certain properties of a software product are verified at run-time by means of cryptographic methods – this happens, however, between machines (e.g., complex computations on the user's smartphone and cloud infrastructure) and is not immediately reproducible by the user. Therefore, the trust-establishing element of such a privacy-preserving gaming system can only be the independent and repeated audit of a game (or a gaming platform, if such a generalization is feasible) by a dedicated community or authority, who follows a strong regulatory framework that requires data minimization and that clearly defines "labels" to tag games that deviate from the data minimization requirement in whatever way. Most importantly, however, introducing such a regulatory framework and the technological backing to enforce the regulations, will require a shift in business models for many free-to-download games that are based on targeted advertising.

We have been explaining the idea behind our approach based on a simple simulation game, which may not be considered representative for games typically played by today's teenagers. Importantly, and depending on implementation specifics, our example may very well feature the full scale of game analytics and player metrics of a *jump 'n' run* game or a complex multiplayer role-playing game because player inputs interactions may be of similar complexity, and the goals of the gaming company, that is maximizing revenue through

[35] We assume basic features that require personal data to be essential in some games: One wants to play with or against one's friends, competitive players may want to be associated with their achievements, and a gaming economy may require player-specific financial transactions.

[36] App audits mobile OS vendors are not always effective and there are many potentially harmful apps available at app stores, cf. (Chatterjee et al. 2018; Suleman et al. 2021).

attention (Alha 2020), are not affected by the complexity of the game (cf. El-Nasr et al. (eds.) 2013).[37] Most importantly, our idea does not actually restrict player interactions and game dynamics. Instead, we propose data flows between game components to be made explicit and distinguishable, ensuring that an auditor can assess these data flows and that a game company cannot change critical parts of a game without this being detectable by users. As such, our proposal may ask for new privacy-centered game architectures that have not been explored to date. We aim to follow up on these questions in experimental work in the future, where we explore different software architectures, aiming to refactor a representative open-source game to implement our idea.

After having discussed the technological side of the integrative approach, we now move to the legal aspect.

Children's right to freedom of thought

The call for a more integrative approach is getting traction in both academia (Alegre 2021b; Kidron et al. 2018; Acquisti et al. 2017) and international organizations.[38] Already in 2017, with the Recommendation 2102 (2017) (Council of Europe 2017), the CoE asked for guidelines on "the recognition of new rights in terms of respect for private and family life, the ability to refuse to be subjected to profiling, (…) and *to be manipulated or influenced*." In the 2019 "Declaration", the CoE pointed out that European policy has focused and relied intensively on people's protection through personal data regulation, while instead it should have moved "beyond data protection". As a result, the search for *actual* impacts of digital manipulation through digital technologies and AI[39] is currently a key issue for the CoE Ad hoc Committee on Artificial Intelligence (CAHAI).

Meanwhile, from the perspective of law in practice, early forms of recognition of addictive technologies are starting to appear. For example, the case *Beau Zanca, et al. v. Epic Games, Inc.* is the first American class action against the gaming company Epic Games. In this case, the maker of the blockbuster freemium Fortnite reached a settlement to avoid the chance of being found guilty of wrongdoing over the use of loot boxes in children's games. As a second example, another class action *F.N. et J.Z. v. Epic Games Inc. et al.* has been filed by Calex legal in Quebec, Canada, on behalf of two parents of minors lamenting "the highly addictive nature of the game". The development of this case will be particularly relevant for European consumers in view of the entering into force of the Directive EU 2020/1828 on "representative actions for the protection of the collective interests of consumers".

Beyond Privacy

The current legal literature on digital harms argues whether existing right to privacy and its interpretations are enough to face the new challenges posed by AI, big data analytics and neuromarketing. To some, secondary law implementations in the EU (mostly GDPR) and latest interpretations of risks by the European Data Protection Board can withstand such challenge today (Ienca and Malgieri 2021).

However, it is increasingly getting traction the idea that EU regulation failed to recognize that people's protection from digital harms cannot always be granted by only respecting rules on data processing; this is because, as is the case of children's protection from manipulation, sometimes the context changes so much that the ultimate human right at risk is no longer digital privacy (Alegre 2021b), but something beyond it.

[37] In fact, several of the highest-grossing games a puzzle games with remarkably simple game mechanics: https://en.wikipedia.org/wiki/List_of_highest-grossing_mobile_games

[38] See, e.g., CoE (Council of Europe 2017) and the Declaration; and the United Nations' Secretary-General's High-level Panel on Digital Cooperation and the subsequent Secretary-General's Roadmap for Digital Cooperation and reports by David Kaye, former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

[39] There is a "need for additional protective frameworks related to data that go beyond current notions of personal data protection and privacy and address the significant impacts of the targeted use of data on societies and on the exercise of human rights more broadly" (Europe 2019)

Some believe that to move beyond privacy means the need for new rights (Skriabin et al. 2021; Sieber 2019; Ienca and Andorno 2017). Above all, Ienca and Adorno claim that the implications raised by neuroscience and neurotechnology "urge a prompt and adaptive response from human rights law with new neuro-specific rights" (Ienca and Andorno 2017).[40]

As a different approach, that is moving beyond privacy without creating new rights, Alegre calls upon a focus shift from privacy to "freedom of thought" (Alegre 2021a), which seems to be also the approach that the CoE and the UN are interested in developing. In fact, the Committee on the Rights of the Child, in General Comment 25 to the UNCRC is the "first clear articulation of the right to freedom of thought in the digital age from a UN body" (Alegre 2021a), as it:

"encourages States parties to introduce or update data protection regulation and design standards that identify, define and prohibit practices that manipulate or interfere with *children's right to freedom of thought* and belief in the digital environment, for example by emotional analytics or inference."[41]

We believe that the approach of Alegre, the CoE and the UN to shift from privacy to freedom of thought is the right one to adopt. We discuss the reasons for the "upgrade" of the right to privacy to that of freedom of thought in the following sections.

Regulating from the perspective of freedom of thought: ancient rules in future-proof regulation

"Regulating from the perspective of the right to freedom of thought is new and complex, but it is crucial to our future as autonomous humans living in democratic societies founded on human rights"
Susie Alegre (Alegre 2021a)

Old and dusted, the right to freedom of thought has been shadowed by the right to privacy for the past 15 years and now needs new interpretations in the light of the digital evolution. In its digital clothes, freedom of thought is best described in the literature by the concept of "cognitive liberty" (Ienca and Andorno 2017; Bublitz 2013; Sententia 2004). It should be understood as the "conceptual update" (Sententia 2004) of the right to privacy in its self-determination connotation, mixed with interpretations of freedom of thought (Alegre 2021a) already in the jurisprudence of the European Court of Human Rights (*see Nolan and K. v Russia*), and as expressed in international human rights legislation.[42]

Applying the right to freedom of thought to children's rights would not be a new concept. Multiple laws in most western legal systems have long since provided for that, dating back to the 2nd century BC, when the *Lex laetoria de circumscriptione adolescentibus* gave action against who fraudulently induced a minor to enter into a transaction and condemning them with *infamia*, the loss of reputation (Candy 2018). Emanation of moral value, the general prohibition of the use of manipulative tactics to take advantage of children's vulnerability (O'Keeffe, Clarke-Pearson, and others 2011) has been early embedded into roman contract and criminal law, and nowadays into EU human rights, commercial, advertising, market, audiovisual, and digital services laws. We are of the opinion that, today, it must be recognised and defined specifically in human rights law, to make sure it does not get lost in the unreliable protections of data privacy (*see Section* 3) or in the complex application of the best interest of the child. This rule's *rationale* is the protection of the freedom

[40] Although they individuate 4 rights to cognitive liberty, mental privacy, mental integrity and psychological continuity, only that to cognitive liberty seems relevant to develop a theory of mental self-determination and freedom from manipulation (*see infra*).

[41] The quote so continues: "Automated systems may be used to make inferences about a child's inner state. They should ensure that automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development."

[42] article 19 of the International Covenant on Civil and Political Rights,, The right to "hold opinions without interference" art. 18 of Universal Declaration of Human Right and art. 10 of the EU Charter (Alegre 2021a) "Cognitive liberty is the neuro-cognitive substrate of all other human and civil liberties", clarifies the UN Human Rights Committee, and it is of utmost importance that it is constantly protected even in a precautionary fashion., On this point, the UK Chief Medical Officers recommends that, while new research is being carried out, technology companies "recognise a precautionary approach in developing structures and remove addictive capabilities."

of a child to develop their self without interference from third parties that do not have their best interest in mind, such as forms of commercial exploitation (Third et al. 2017). It is children's right to be children, to experience, to make mistakes, and to do so without malevolent interference from adults.

Challenges ahead

Notwithstanding the maturity of this ancient principle of law, regulating today's technologies from the perspective of freedom of thought implies radical substantial and procedural changes: whereas privacy and data protection are non-absolute rights that have been limited by balancing with other fundamental rights – such as of others to conduct business –, freedom of thought is an *absolute* right and does not accept any interference.[43]

To this day, the regulators have been addressing personalized addictive content under the assumption that a well designed system of procedural rules on personal data collection and processing could be the adequate shield with which to protect all of data subjects' fundamental rights. We instead claim otherwise: some of the cornerstones of EU data protection, most notably its risk-based approach and its tolerance to lawful interferences – as in, "procedurally sound" interferences – have allowed organizations to keep poking holes and finding cracks in such shield, exploiting state-of-the-art technical and organizational measures for the market-necessary aim of demonstrating compliance. We instead believe that what's important is not so much whether procedural data protection rules on processing are respected, but whether the fundamental rights of children, which those rules aim to protect, are respected in their essence. In practice, this means that when a processing activity interferes with the right to children's freedom of thought, notwithstanding how well it respects data protection rules, it is a violation of such right.

A shift from data privacy to protection of freedom of thought means changing the status of the fundamental right being protected, from relative to absolute, which in turn will have systemic legal repercussions, and calls for a rethinking of the entire regulatory ecosystem: from its ethics, to human rights interpretations, to adaptations of secondary law (*see EU Legal Acquis Table [tab:LegalAquis]*), and so on. All this considered, it seems that the biggest challenge ahead, at least from a legal perspective, is to understand how regulating digital manipulations through the right to freedom of thought is going to affect the EU legal system, and what will be its repercussions.

Conclusions & Future Directions

The predatory tactics and tools of the attention economy have shown their worst side in the context of gaming. Freemium business models are harming children's health, social, and personal well-being, in a fast-changing technological context where regulators have failed at being receptive to the new risks, and to adequately respond with effective regulatory means. We believe that if regulators keep addressing the issue of children digital manipulation through new regulation along the lines of established concepts involving data protection and privacy, it will only incentivize novel analytics and a diversification of addictive strategies rather than prioritize the best interest, and uphold the fundamental rights of children.

We discuss reasons whether and why decision makers' reliance on European privacy laws for the protection of children from digital manipulation has proven unsuccessful. The failure, we claim, is not only due to reasons of inefficient law enforcement systems (*see* Section 3 on the "enforcement paralysis"), but also to a fundamental error in the detection of the asset to protect. This asset, in fact, we do not identify as the relative human right to privacy, rather the absolute right to freedom of thought.

[43] "Little has been done to develop fully operational legislative and regulatory frameworks to ensure that enjoyment of the right to freedom of thought is real and effective in a modern context (…) there are also positive obligations to protect all those in their jurisdiction from interference with the right. So, laws must be in place, not only to prevent state actions that could interfere with our rights to freedom in the 'forum internum,' but also prohibiting others from doing so."(Alegre 2021b)

Pending new regulations, we propose one technical and one regulatory approach to address this issue: a zero-knowledge model for a gaming information system, to "dab the bleeding" with a technical fix, and a regulatory "upgrade", which is a shift from privacy to freedom of thought. The interplay of the two should provide for an "integrative approach" with immediate as well as long term effects, hopefully fit to shape a more humane future that forbids children's manipulation and exploitation for commercial purposes.

The idea of such an "integrative approach" needs to be picked up and considered across regulatory bodies, authorities that oversee the development of content for minors, technology companies, and researchers alike. Specifically, we see a need for action by competent national regulatory authorities for streamlining the analysis of manipulative neuromarketing techniques (in view of the upcoming AI Act and its classification of prohibited AI due to manipulative practices) and homogenizing the assessment of online games. As for policy makers, we believe they should invest resources into understanding the risks of addictive technologies and finding regulatory solutions. Game developers, on their side, should become aware of risks of addictive technologies and make conscious choices about ethical software design, as well as foster digital alphabetization and raise users' risk awareness.

Acknowledgments

This research is funded by the Research Fund KU Leuven, and by the Flemish Research Programme Cybersecurity.

References

Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, et al. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." ACM Computing Surveys (CSUR) 50 (3): 1–41.

Alha, Kati. "The rise of free-to-play: How the revenue model changed games and playing." (2020).

Alegre, Susie. 2021a. "Protecting Freedom of Thought in the Digital Age."

———. 2021b. "Regulating Around Freedom in the 'Forum Internum'." In ERA Forum, 21:591–604. 4. Springer.

Arrington, Robert L. 1982. "Advertising and Behavior Control." Journal of Business Ethics 1 (1): 3–12.

Aylsworth, Timothy. 2020. "Autonomy and Manipulation: Refining the Argument Against Persuasive Advertising." Journal of Business Ethics, 1–11.

Baker, Sherry, and David L Martinson. 2001. "The Tares Test: Five Principles for Ethical Persuasion." Journal of Mass Media Ethics 16 (2-3): 148–75.

Barocas, Solon, and Helen Nissenbaum. 2009. "On Notice: The Trouble with Notice and Consent." In Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information.

Ben-Shahar, Omri, and Carl E Schneider. 2014. More Than You Wanted to Know: The Failure of Mandated Disclosure. Princeton University Press.

Blades, Mark, Caroline Oates, Fran Blumberg, and Barrie Gunter. 2014. Advertising to Children: New Directions, New Media. Springer.

Blumberg, F. C., Deater-Deckard, K., Calvert, S. L., Flynn, R. M., Green, C. S., Arnold, D., & Brooks, P. J. (2019). Digital Games as a Context for Children's Cognitive Development: Research Recommendations and Policy Considerations. Social Policy Report, 32(1), 1–33.

Brownsword, Roger. 2012. "Regulating Brain Imaging: Questions of Privacy, Informed Consent, and Human Dignity." I Know What You're Thinking. Brain Imaging and Mental Privacy. Oxford University Press, Oxford, 223–44.

Bublitz, Jan-Christoph. 2013. "My Mind Is Mine!? Cognitive Liberty as a Legal Concept." In Cognitive Enhancement, 233–64. Springer.

Candy, Peter. 2018. "Lex (P) Laetoria." In Oxford Research Encyclopedia of Classics.

Canli, Turhan. 2006. "When Genes and Brains Unite: Ethical Implications of Genomic Neuroimaging." Neuroethics: Defining the Issues in Theory, Practice and Policy, 169–84.

Carr, Nicholas. 2020. The Shallows: What the Internet Is Doing to Our Brains. WW Norton & Company.

Chatterjee, Rahul, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. "The Spyware Used in Intimate Partner Violence." In 2018 Ieee Symposium on Security and Privacy (Sp), 441–58. IEEE.

Clarke, Barbie, and Siv Svanaes. 2012. "Digital Marketing and Advertising to Children: A Literature Review." In Advertising Education Forum. Vol. 79.

Commons, House of. 2019. "Immersive and Addictive Technologies."

Council, Norwegian Consumer. 2018. "Deceived by Design, How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy." Norwegian Consumer Council Report.

Council of Europe, Parliamentary Assembly. 2017. "Technological Convergence, Artificial Intelligence and Human Rights."

Crepax, T., Muntés-Mulero, V., Martinez, J., & Ruiz, A. (2022). Information technologies exposing children to privacy risks: Domains and children-specific technical controls. Computer Standards & Interfaces, 82, 103624

Crisp, Roger. 1987. "Persuasive Advertising, Autonomy, and the Creation of Desire." Journal of Business Ethics 6 (5): 413–18.

Dalla Corte, Lorenzo. 2020. "A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection." Data Protection and Privacy, 27–58.

De Jans, Steffi, Dieneke Van de Sompel, Liselot Hudders, and Veroline Cauberghe. 2019. "Advertising Targeting Young Children: An Overview of 10 Years of Research (2006–2016)." International Journal of Advertising 38 (2): 173–206.

Demmler, Daniel, Peter Rindal, Mike Rosulek, and Ni Trieu. 2018. "PIR-Psi: Scaling Private Contact Discovery." Proc. Priv. Enhancing Technol. 2018 (4): 159–78.

Drummond, A., & Sauer, J. D. (2018). Video game loot boxes are psychologically akin to gambling. Nature Human Behaviour, 2(8), 530–532.Duch-Brown, Nestor, Bertin Martens, and Frank Mueller-Langer. 2017. "The Economics of Ownership, Access and Trade in Digital Data."

Durante, Kristina M, Vladas Griskevicius, Sarah E Hill, Carin Perilloux, and Norman P Li. 2011. "Ovulation, Female Competition, and Product Choice: Hormonal Influences on Consumer Behavior." Journal of Consumer Research 37 (6): 921–34.

El-Nasr, Magy Seif, Anders Drachen, and Alessandro Canossa. Game analytics. Springer London Limited, 2016.

Europe, Council of. 2019. "Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes."

Fenton, Ted, and Reinout W Wiers. 2017. "Free Will, Black Swans and Addiction." Neuroethics 10 (1): 157–65.

Fitton, D., & Read, J. C. (2019, June). Creating a framework to support the critical consideration of dark design aspects in free-to-play apps. In Proceedings of the 18th ACM International Conference on Interaction Design and Children (pp. 407-418).

Fischbach, Ruth, and Janet Mindes. 2011. "Why Neuroethicists Are Needed." Oxford Handbook of Neuroethics, 343–76.

Fogg, Brian J. 2002. "Persuasive Technology: Using Computers to Change What We Think and Do." Ubiquity 2002 (December): 2.

Ford, John B. 2019. "What Do We Know About Neuromarketing?" Journal of Advertising Research. https://doi.org/10.2501/JAR-2019-031.

Fukuyama, Francis. 2003. Our Posthuman Future: Consequences of the Biotechnology Revolution. Farrar, Straus; Giroux.

Gilbert, Neil, Nigel Parton, and Marit Skivenes. 2011. Child Protection Systems: International Trends and Orientations. OUP USA.

Greene, Joshua, and Jonathan Cohen. 2004. "For the Law, Neuroscience Changes Nothing and Everything." Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences 359 (1451): 1775–85.

Griffiths, Mark D. "Adolescent gambling and gambling-type games on social networking sites: Issues, concerns, and recommendations." Aloma: revista de psicologia, ciències de l'educació i de l'esport Blanquerna 33, no. 2 (2015): 31-37.

Hargittai, Eszter, and Alice Marwick. ""What can I really do?" Explaining the privacy paradox with online apathy." International journal of communication 10 (2016): 21.

Harris, Tristan. 2016. "How Technology Hijacks People's Minds—from a Magician and Google's Design Ethicist." Medium Magazine.

Hartzog, Woodrow. 2018. Privacy's Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press.

Hullett, Kenneth, Nagappan, Nachiappan, Schuh, Eric, and Hopson, John. "Empirical analysis of user data in game software development," Proceedings of the 2012 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, 2012, pp. 89-98, doi: 10.1145/2372251.2372265.

Ienca, Marcello, and Roberto Andorno. 2017. "Towards New Human Rights in the Age of Neuroscience and Neurotechnology." Life Sciences, Society and Policy 13 (1): 1–27.

Ienca, Marcello, and Gianclaudio Malgieri. 2021. "Mental Data Protection and the Gdpr." Available at SSRN 3840403.

Kales, Daniel, Christian Rechberger, Thomas Schneider, Matthias Senker, and Christian Weinert. 2019. "Mobile Private Contact Discovery at Scale." In 28th USENIX Security Symposium (USENIX Security 19), 1447–64.

Karlsen, F. (2020). Game Creation, Monetisation Models, and Ethical Concerns.

Karlsen, F. (2021). Balancing Ethics, Art and Economics: A Qualitative Analysis of Game Designer Perspectives on Monetisation. Games and Culture, 15554120211049579.Kenning, Peter, and Marc Linzmajer. 2011. "Consumer Neuroscience: An Overview of an Emerging Discipline with Implications for Consumer Policy." Journal Für Verbraucherschutz Und Lebensmittelsicherheit 6 (1): 111–25.

King, D. L., & Delfabbro, P. H. (2018). Predatory monetization schemes in video games (eg 'loot boxes') and internet gaming disorder.

Kidron, Beeban, Alexandra Evans, Jenny Afia, Joanna R Adler, Henrietta Bowden-Jones, Liam Hackett, Anisha Juj, Andrew K Przybylski, Anghrarad Rudkin, and Young Scot. 2018. "Disrupted Childhood: The Cost of Persuasive Design."

Király, Orsolya, Mark D Griffiths, Daniel L King, Hae-Kook Lee, Seung-Yup Lee, Fanni Bányai, Ágnes Zsila, Zsofia K Takacs, and Zsolt Demetrovics. 2018. "Policy Responses to Problematic Video Game Use: A Systematic Review of Current Measures and Future Possibilities." Journal of Behavioral Addictions 7 (3): 503–17.

Koob, George F, and Nora D Volkow. 2016. "Neurobiology of Addiction: A Neurocircuitry Analysis." The Lancet Psychiatry 3 (8): 760–73.

Kröger, Jacob Leon, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. 2021. "Surveilling the Gamers: Privacy Impacts of the Video Game Industry." Available at SSRN 3881279.

LaRose, Robert, and Nora J Rifon. 2007. "Promoting I-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior." Journal of Consumer Affairs 41 (1): 127–49.

Laufer, Robert S, and Maxine Wolfe. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory." Journal of Social Issues 33 (3): 22–42.

Leshner, Alan I. 1997. "Addiction Is a Brain Disease, and It Matters." Science 278 (5335): 45–47.

Lessig, Lawrence. 2009. Code: And Other Laws of Cyberspace. ReadHowYouWant. com.

Lievens, Eva, Sonia Livingstone, Sharon McLaughlin, Brian O'Neill, and Valerie Verdoodt. 2018. "Children's Rights and Digital Technologies." International Children's Rights Law, 487–513.

Lindstrom, Martin. 2010. Buy Ology: Truth and Lies About Why We Buy. Currency.

Livingstone, Sonia, John Carr, and Jasmina Byrne. 2016. "One in Three: Internet Governance and Children's Rights."

Livingstone, Sonia, Mariya Stoilova, and Rishita Nandagiri. 2018. "Conceptualising Privacy Online: What Do, and What Should, Children Understand?" Parenting for a Digital Future.

———. 2019. "Children's Data and Privacy Online: Growing up in a Digital Age: An Evidence Review."

Livingstone, Sonia, Damian Tambini, Nikola Belakova, and Emma Goodman. 2018. "Protection of Children Online: Does Current Regulation Deliver?"

Lupton, Deborah, and Ben Williamson. 2017. "The Datafied Child: The Dataveillance of Children and Implications for Their Rights." New Media & Society 19 (5): 780–94.

Lwin, May O., Andrea JS Stanaland, and Anthony D. Miyazaki. "Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness." Journal of retailing 84, no. 2 (2008): 205-217.

Macenaite, Milda, and Eleni Kosta. 2017. "Consent for Processing Children's Personal Data in the Eu: Following in Us Footsteps?" Information & Communications Technology Law 26 (2): 146–97.

Madigan, Jamie. 2015. Getting Gamers: The Psychology of Video Games and Their Impact on the People Who Play Them. Rowman & Littlefield.

Maene, P., J. Götzfried, R. de Clercq, T. Müller, F. Freiling, and I. Verbauwhede. 2017. "Hardware-Based Trusted Computing Architectures for Isolation and Attestation." IEEE Transactions on Computers PP (99): 1–1.

Matthews, Steve. 2015. "Neuromarketing: What is it and is it a threat to privacy?" In Handbook of Neuroethics. https://doi.org/10.1007/978-94-007-4707-4_154.

McCarthy-Jones, Simon. 2019. "The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century." Frontiers in Artificial Intelligence 2: 19.

Melzer, A. K., Roarsen, A. K., Hagen, M. H., & Jaccheri, L. (2021, November). Towards Suitable Free-to-Play Games for Children. In International Conference on Entertainment Computing (pp. 264-276). Springer, Cham.

moxie0. 2017. "Technology Preview: Private Contact Discovery for Signal."

Murphy, Emily R, Judy Illes, and Peter B Reiner. 2008. "Neuroethics of Neuromarketing." Journal of Consumer Behaviour: An International Research Review 7 (4-5): 293–302.

Newman, Joe, and Joseph Jerome. 2014. "Press Start to Track Privacy and the New Questions Posed by Modern Video Game Technology." AIPLA QJ 42: 527.

OECD. 2021. "Children in the Digital Environment," no. 302. https://doi.org/https://doi.org/https://doi.org/10.1787/9b8f222e-en.

O'Keeffe, Gwenn Schurgin, Kathleen Clarke-Pearson, and others. 2011. "The Impact of Social Media on Children, Adolescents, and Families." Pediatrics 127 (4): 800–804.

Onnela, Jukka-Pekka, and Scott L Rauch. 2016. "Harnessing Smartphone-Based Digital Phenotyping to Enhance Behavioral and Mental Health." Neuropsychopharmacology 41 (7): 1691–6.

Owen, Laura, Charlie Lewis, Susan Auty, and Moniek Buijzen. 2013. "Is Children's Understanding of Nontraditional Advertising Comparable to Their Understanding of Television Advertising?" Journal of Public Policy & Marketing 32 (2): 195–206.

Pasquale, Liliana, and Paola Zippo. 2020. "A Review of Age Verification Mechanism for 10 Social Media Apps."

Purtova, Nadezhda. 2018. "The Law of Everything. Broad Concept of Personal Data and Future of Eu Data Protection Law." Law, Innovation and Technology 10 (1): 40–81.

Ramsøy, Thomas Zoëga. 2019. "Building a Foundation for Neuromarketing and Consumer Neuroscience Research: How Researchers Can Apply Academic Rigor to the Neuroscientific Study of Advertising Effects." Journal of Advertising Research 59 (3): 281–94.

Ringland, Kathryn E. 2019. "'Autsome': Fostering an Autistic Identity in an Online Minecraft Community for Youth with Autism." In International Conference on Information, 132–43. Springer.

Russell, N Cameron, Joel R Reidenberg, and Sumyung Moon. 2018. "Privacy in Gaming." Fordham Intell. Prop. Media %Ent. LJ 29: 61.

Sartor, Giovanni, Francesca Lagioia, and Federico Galli. 2021. "Regulating Targeted and Behavioural Advertising in Digital Services."

Sax, Marijn, and Jef Ausloos. 2021. "Getting Under Your Skin(s): A Legal-Ethical Exploration of Fortnite's Transformation into a Content Delivery Platform and Its Manipulative Potential." Interactive Entertainment Law Review 4 (1).

Schaik, Stephan van, Andrew Kwong, Daniel Genkin, and Yuval Yarom. 2020. "SGAxe: How SGX Fails in Practice."

Schaub, Florian, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. "A Design Space for Effective Privacy Notices." In Eleventh Symposium on Usable Privacy and Security (Soups 2015), 1–17.

Schüll, Natasha Dow. 2012. Addiction by Design. Princeton University Press.

Schultz, Wolfram, Peter Dayan, and P Read Montague. 1997. "A Neural Substrate of Prediction and Reward." Science 275 (5306): 1593–9.

Scopelliti, Gianluca, Sepideh Pouyanrad, Job Noorman, Fritz Alder, Frank Piessens, and Jan Tobias Mühlberg. 2021. "POSTER: An Open-Source Framework for Developing Heterogeneous Distributed Enclave Applications." In CCS '21. New York, NY, USA: ACM. https://doi.org/10.1145/3460120.3485341.

Sententia, Wrye. 2004. "Neuroethical Considerations: Cognitive Liberty and Converging Technologies for Improving Human Cognition." Annals of the New York Academy of Sciences 1013 (1): 221–28.

Sher, Shlomo. 2011. "A Framework for Assessing Immorally Manipulative Marketing Tactics." Journal of Business Ethics 102 (1): 97–118.

Sieber, Alexander. 2019. "Souled out of rights? - Predicaments in protecting the human spirit in the age of neuromarketing." In Life Sciences, Society and Policy. Vol. 15. 1. https://doi.org/10.1186/s40504-019-0095-4.

Sifa, Rafet, Anders Drachen, and Christian Bauckhage. 2018. "Profiling in Games: Understanding Behavior from Telemetry." Social Interactions in Virtual Worlds: An Interdisciplinary Perspective.

signal. 2021. "Signal."

Simon, Herbert A. 1994. "The Bottleneck of Attention: Connecting Thought with Motivation."

Skriabin, Oleksii M, Dmytro B Sanakoiev, Natalia D Sanakoieva, Vita V Berezenko, and Yuliia V Liubchenko. 2021. "Neurotechnologies in the advertising industry: Legal and ethical aspects." Innovative Marketing 17 (2): 2021. https://doi.org/10.21511/im.17(2).2021.17.

Sloan, Robert H, and Richard Warner. 2014. "Beyond Notice and Choice: Privacy, Norms, and Consent." J. High Tech. L. 14: 370.

Small, Gary W, Jooyeon Lee, Aaron Kaufman, Jason Jalil, Prabha Siddarth, Himaja Gaddipati, Teena D Moody, and Susan Y Bookheimer. 2020. "Brain Health Consequences of Digital Technology Use." Dialogues in Clinical Neuroscience 22 (2): 179.

Smidts, Ale. 2002. "Kijken in Het Brein: Over de Mogelijkheden van Neuromarketing."

Smith, Karen Louise, and Leslie Regan Shade. "Children's digital playgrounds as data assemblages: Problematics of privacy, personalization, and promotional culture." Big Data & Society 5, no. 2 (2018): 2053951718805214.

Stanton, Steven J, Walter Sinnott-Armstrong, and Scott A Huettel. 2017. "Neuromarketing: Ethical Implications of Its Use and Potential Misuse." Journal of Business Ethics 144 (4): 799–811.

Steeves, Valerie, and Cheryl Webster. "Closing the barn door: The effect of parental supervision on Canadian children's online privacy." Bulletin of Science, Technology & Society 28, no. 1 (2008): 4-19.

Su, Yanhui, Per Backlund, and Henrik Engström. "Comprehensive review and classification of game analytics." Service Oriented Computing and Applications 15, no. 2 (2021): 141-156.

Suleman, Muhammad, Tariq Rahim Soomro, Taher M Ghazal, and Muhammad Alshurideh. 2021. "Combating Against Potentially Harmful Mobile Apps." In The International Conference on Artificial Intelligence and Computer Vision, 154–73. Springer.

Swan, Melanie. 2012. "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0." Journal of Sensor and Actuator Networks 1 (3): 217–53.

Third, Amanda, Delphine Bellerose, Juliano Diniz De Oliveira, Girish Lala, and Georgina Theakstone. 2017. "Young and Online: Children's Perspectives on Life in the Digital Age."

Van den Berg, Bibi, and Simone Van der Hof. 2012. "What Happens to My Data? A Novel Approach to Informing Users of Data Processing Practices." First Monday 17 (7).

Simone, van der Hof, and Eva Lievens. "The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR." Communications law 23, no. 1 (2018).

Van Reijmersdal, Eva A, Jeroen Jansz, Oscar Peters, and Guda Van Noort. 2010. "The Effects of Interactive Brand Placements in Online Games on Children's Cognitive, Affective, and Conative Brand Responses." Computers in Human Behavior 26 (6): 1787–94.

Verdoodt, Valerie. 2020. Children's Rights and Commercial Communication in the Digital Era. Vol. 10. Intersentia.

Waiguny, Martin KJ, Michelle R Nelson, and Ralf Terlutter. 2014. "The Relationship of Persuasion Knowledge, Identification of Commercial Intent and Persuasion Outcomes in Advergames—the Role of Media Context and Presence." Journal of Consumer Policy 37 (2): 257–77.

Wardlaw, Joanna M, Garret O'connell, Kirsten Shuler, Janet DeWilde, Jane Haley, Oliver Escobar, Shaun Murray, et al. 2011. "'Can It Read My Mind?'–What Do the Public and Experts Think of the Current (Mis) Uses of Neuroimaging?" PloS One 6 (10): e25829.

Wilson, Edward O. 2017. The Origins of Creativity. Liveright Publishing.

Wilson, R Mark, Jeannie Gaines, and Ronald Paul Hill. 2008. "Neuromarketing and Consumer Free Will." Journal of Consumer Affairs 42 (3): 389–410.

Wright, Benjamin D. 1997. "A History of Social Science Measurement." Educational Measurement: Issues and Practice 16 (4): 33–45.

Wu, Tim. 2017. The Attention Merchants: The Epic Scramble to Get Inside Our Heads. Vintage.

Wuyts, Kim, Laurens Sion, and Wouter Joosen. 2020. "LINDDUN Go: A Lightweight Approach to Privacy Threat Modeling." In 2020 Ieee European Symposium on Security and Privacy Workshops (Euros&PW), 302–9. IEEE.

Zuboff, Shoshana. 2019. "Surveillance Capitalism." Esprit 5: 63–77.