Upgrading the protection of children from manipulative and addictive strategies in online games: Legal and technical solutions beyond privacy regulation

Tommaso Crepax
tommaso.crepax@santannapisa.it
LIDER-Lab, Istituto Dirpolis, Scuola Superiore Sant'Anna
Pisa, Italy

Jan Tobias Mühlberg
jantobias.muehlberg@cs.kuleuven.be
imec-DistriNet, KU Leuven
Leuven, Belgium

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.

KEYWORDS

online games, children, privacy, data protection, freedom of thought, confidential computing

1 INTRODUCTION

"The capture and re-sale of human attention became the defining industry of our time". With these words, Tim Wu [Wu17] summarizes the core mechanics of the *attention economy*. Coined by the psychologist, economist and Nobel laureate Herbert A. Simon [Sim94], 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 [oC19]. 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 [Har16], 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" [Zub19]. 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 [Har16].

The Weapons. The contenders use old and new marketing strategies to harvest attention [Wu17]. From Pavlov's experiments to condition dogs' behavior, to Fogg's persuasive technology [Fog02], behavioral and neuro-sciences have fed marketing research with deeper knowledge to understand and condition consumers' behavior.[2] Developers introduce addiction-by-design [Sch12] and compulsion-by-design [KEA+18] 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

---

[1]Recent revelations on Facebook's own internal research on effects of Instagram on teenage girls: "Congress grills Facebook exec on Instagram's harmful effect on children", The Guardian, 2021-09-30: https://www.theguardian.com/technology/2021/sep/30/facebook-hearing-testimony-instagram-impact

[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" [Mat15].

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

in legal terms [DBMML17] – 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 [KEA+18, Cou18]. 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" [KEA+18]. 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 [BDDC+19]. As "godlike technologies" take advantage of children's "paleolithic emotions" [Wil17], the legal, social and ethical systems nowadays in place are not succeeding at ensuring decent levels of protection [LTBG18] (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] through 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 [KEA+18, LTBG18, Har16].

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.

1.1 This Paper & Contributions

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:

(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?

1.2 Online Gaming: The Paradise of Child 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" [LW17][7] happens through the generation and collection of massive amounts of online gaming data [RRM18, NJ14, SA21]. In fact, game developers wallow in "dataveillance" [LW17],[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 receivers) while virtual world data are collected through a users' interactions with the game software [SA21, NJ14, KRCU21]. 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" [NJ14]. 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.,[HNSH12, SENDC13]). A recent survey of this field [SBE21] 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."

---

[4] E.g., 5Rights Foundations [KEA+18], Norwegian Consumer council [Cou18], Center for Humane Technology, NeuroRights Initiative, AlgoTransparency project.

[5] E.g., BetterInternet4Kids, [OEC21], Gam(e)(a)ble: 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 and [CMMMR22]

[7] Cf. also "Age appropriate design: a code of practice for online services", Information Commissioner's Office (U.K., 2020): https://ico.org.uk/for-organisations/age-appropriate-design-executive-summary-and-standards/

[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" [LW17].

[9] Cf. "The Platform Evolution of Game Analytics", Ben Weber, 2018: https://towardsdatascience.com/evolution-of-game-analytics-platforms-4b9efcb4a093

Following El-Nasr et al. [SENDC13] and Su et al [SBE21], 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, to infer information about the player's health, such as 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 [Mad15, IM21]. 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 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]

1.3 Profiling in Gaming

1.3.1 Telemetry-Driven Behavioral Profiling.

> "The old adage of big data having volume, velocity, variety and volatility holds very true for behavioral telemetry from games." [SDB18]

While players do volunteer some personal data, the vast majority is acquired by observation, derived through analysis, or inferred probabilistically off the *unaware subject* [SLG21, IM21, OR16]. The constant growth of training data volume generated by telemetry-driven behavioral profiling of thousands – sometimes many 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 [SDM97], 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.

The ability to predict which users will turn into long-term players, social network enablers and/or buyers of in-game content
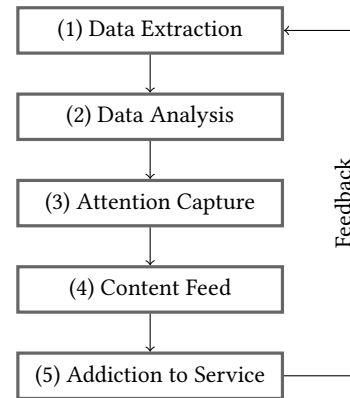

Figure 1: Addiction process: from personal data extraction to user addiction.

enables an optimization of Customer Relationship Management, and the tailoring of game content to the specific profiles of these users [SDB18]. Much like professionals at chicken sexing,[15] shallow profiling algorithms must individuate churners and buyers in as little time as possible (ca. 20 minutes [NJ14]). Deep profiling, instead, provides a toolbox for integrating varied player behaviors and experimenting on potential correlations with player psychology [SDB18] 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 Figure 1).

1.3.2 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 [Wri97, Can06, For19]. Therefore, to the problem of precise quantification of mental processes, neuroscience applied to marketing, although in its infancy [Ram19], provides promising answers [Swa12]: born to study mechanisms to understand the consumer's behavior [Smi02], neuromarketing exploits physiological-measuring techniques such as eyetracking, pupilometry, EEG, fMRI, facial coding, sensory marketing, as well as psychographics [KL11], to measure targeted people's emotions

---

[10]As seen in, e.g., the game Minecraft with assumptions made on different levels of completion [100%] [Rin19], 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.

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

[14]See e.g., the number of players of Fortnite in 2021 being between 6 and 12 million. https://www.ggrecon.com/guides/fortnite-player-count-how-many-people-play/

[15]See "The Lucrative Art of Chicken Sexing", Pacific Standard, 2018-08-08: 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]This understanding of the psychological state in the "human futures market", as said in [Zub19], is the sale of what we will do next [Ale21a].

and feelings [Lin10] 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 [WGH08], when the users finally desist from playing, they start receiving timed alerts or push notifications [KEA+18] that pull them back into the game.[19]

1.3.3 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 [LCB16]) 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 [PZ20].

There are "literally thousands" [Har16] 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 [KEA+18]: 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 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 [She11, KEA+18, SA21].

There is an emerging – yet underdeveloped [MRHJ21] – 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 [Alh20] and [Kar21], for instance through imposing the necessity of ever increasing predatory [KD18] "loot boxes" [Kar20], mostly due to challenging monetization mechanics [Kar21]. 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" [Kar21], 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 [FR19], which, combined with works on identification of technical controls designed specifically to protect children's privacy [CMMMR22], could help game developers in making ethical game design choices.

2 THE 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 [Zub19], 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." [oE19]

Persuasive design strategies, deployed to maximize the collection of personal data, disturb children's social, mental and physical development [KEA+18].

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 [SSAH17]. Personal harms include anxiety, social aggression, denuded relationships, sleep deprivation, impacts on education, health and wellbeing [KEA+18], psychosocial and financial harms, withdrawal from real life, heightened attention-deficit symptoms [Car20], impaired emotional and social intelligence, technology addiction, social isolation, impaired brain development, and disrupted sleep [SLK+20]. Because of young children's high brain plasticity, there may be consequences due to the normalization of gambling [DS18].[21] Scientific literature is increasingly coming to the conclusion that addiction is at least a disease of free will [KV16], and at worst a brain disease [Les97, FW17]. As not only is attention finite, but also the "bottleneck of human thought" [Sim94], 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 [SLK+20] has demonstrated that "internet addiction shares features with substance-use disorders or pathological gambling".

---

[19]See U.K. Research and Innovation (UKRI)'s written evidence for the "Immersive and Addictive Technologies" report, 2019-08-09: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/1846.pdf
[20]The idea is that of putting "slot machines in users' pockets," paraphrasing Tristan Harris' aticle "The Slot Machine in Your Pocket", Spiegel International, 2016-07-27: https://www.spiegel.de/international/zeitgeist/smartphone-addiction-is-part-of-the-design-a-1104237.html

[21]Henrietta Bowden-Jones notes: "Habits learnt in childhood require significant intervention, and that habits formed before the age of nine take considerable intervention 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", from "Video games are pushing children into gambling warns England's top mental health nurse", Health Tech Digital, 2020-02-19: https://www.healthtechdigital.com/video-games-are-pushing-children-into-gambling-warns-englands-top-mental-health-nurse/

As an answer to these dramatic risks, there have been some authoritative recognition of problematic gaming and calls for action. The U.K. 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".[22]

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. [Gri15]). However, studies reveal that these approaches may reduce risks – without eliminating them [SW08], vary substantially in effectiveness depending on the type of parental mediation and the age group of the children [LSM08], and suffer from increasing privacy and consent fatigue, which is promoted by the opaqueness of online systems [HM16]. 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. [SL18]). 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.

2.1 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 [Zub19]. "Stealthy neuromarketing" [MIR08], 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 [GC04, WGH08]. As behavioral science, neuro-science and deep learning techniques increasingly confirm the substantial impact of biology on decision making and action [Fuk03, DGH+11], 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 [WGH08], privacy [Bro12], freedom of thought [MJ19] and mental integrity [IA17].

Understanding the exact point where acceptable persuasion becomes unacceptable manipulation is one of the crucial issues for the regulation of digital manipulation [Ale21a]. Luckily, the literature

on marketing ethics on the topic of persuasion versus manipulation in advertising is lively and abundant [DJVdSHC19]. Among many others, some authoritative views are represented by Crisp [Cri87], 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 [Arr82]; and Aylsworth, who allows for manipulations, but only for ends that people accept and by means they endorse [Ayl20]. As the theoretical debate develops, some tried to create practical methodologies to distinguish ethical from unethical persuasions [BM01], but new research is needed to keep pace with the digital evolution [CS12].

As the debate follows on, unethical combination of tactics manipulate users toward the least privacy friendly options, jeopardizing the genuineness of consent [Cou18]. The public and academic skepticism [FM11] about uses of manipulating techniques [WOS+11] has called upon governments and market regulators to act, as well as upon industry to adopt ethical guidelines, etc [MIR08]. 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" [Ale21b].

3 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 and 2.1). It is unquestionable that the law, as one of the main means of regulation [Les09], 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 this gap.

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 [GPS11, LSN18, Ver20, LSN18]. A substantial portion of the legal scholarship is skeptical about the efficacy of privacy notices (for a comprehensive review on the topic cf. [VdBVdH12], but also [BN09, SW14, AAB+17, MK17, Har18, SBDC15, BSS14])[23]. Authoritative champion of this faction, Sartor claims that data subjects' opportunity to consent to risks they cannot foresee is not an *asset*

---

[22]"ICD-11: International Classification of Diseases 11th Revision – The global standard for diagnostic health information", WHO, 2019-05-25: https://icd.who.int/en

[23]Data protection became the law of everything which is "impossible to maintain" [Pur18] – and enforce, and as an essential "right to a rule" [DC20] 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 [LR07] 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".

for them, but a *liability* [SLG21].[24] 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 [AAB+17] on the side of the data subject mine the foundations of the "privacy calculus" [LW77], the theory of individual rational choice positing that data subjects are agents with stable preferences in regards to privacy.

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 [SA21]. 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, that is Instagram, is "toxic" to teenage girls.[25]

Another cause could be that the applicable legal framework is too complex and incoherent (cf. Table 1). It seems that the increasing addition of gaming features for attention capturing [OLAB13, BOBG14, VRJPVN10, WNT14] might have broadened the regulatory framework of online gaming so that it became too complex to be effective [SA21, LTBG18]. 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.[26] 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."[27]

In response to problems of children protection, academia, international organizations and civil society[28] 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" [MIR08, KEA+18, LSN19], through taking a public health approach,[29] or creating new privacy preserving technologies and standards.[30]

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."[31] 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 1: "Potentially applicable EU laws and provisions"), especially the finalized text of the proposal for an 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 this proposal is far from finished; 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."[32]

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

---

[24]Sartor et *al.* believe that "consent has been abused as a legal basis for targeted advertising" [SLG21], 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, […]". European Data Protection Board, 2020-05-04: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[25]Cf. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show", The Wall Street Journal, 2021-08-14: https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[26]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" (cf. 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) [DJVdSHC19].

[27]Cf. "Europe's enforcement paralysis: ICCL's 2021 report on the enforcement capacity of data protection authorities": https://www.iccl.ie/digital-data/2021-gdpr-report/

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

[29]Cf. "Video games are pushing children into gambling warns England's top mental health nurse", Health Tech Digital, 2020-02-19: https://www.healthtechdigital.com/video-games-are-pushing-children-into-gambling-warns-englands-top-mental-health-nurse/

[30]Cf. the work of IEEE Standards Association presented in their "Webinar Series: Children's Data Governance Applied Case Studies" at https://engagestandards.ieee.org/childrens-data-gov-webinar-register.html

[31]"Age appropriate design: a code of practice for online services", The U.K.'s 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/

[32]Cf. "The EU regulates AI but forgets to protect our mind", European Law Blog, 2021-07-07: https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/

manipulation will be automatically solved too. In fact, studies on policies versus gaming addiction by Király 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* [KGK⁺18]. 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.

4 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 [sig21], 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.

4.1 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 [MGC⁺17] are used to protect the service-side of the contact discovery mechanism from interference by compromised infrastructure or from the service provider [mox17]: 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*[33] 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.

4.2 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 [WSJ20] 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*,[34] 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.

4.3 A Concrete Example: Shufflepuck

To give a brief example of such a compartmentalization strategy for a mobile simulation of the game *table shuffleboard*.[35] 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

---

[33]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.

[34]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.

[35]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).

Table 1: 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
	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

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 used to distinguish individual players, to associate these players with natural persons, and keep scores.[36] 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.[37] The remote component of online games is currently not part of such audits, which our proposal strives to address.

4.4 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 [SPN+21] 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., [DRRT18, KRS+19], 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., [vSKGY20]) 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

---

[36]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.

[37]App audits mobile OS vendors are not always effective and there are many potentially harmful apps available at app stores, cf. [CDO+18, SSGA21].

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 attention (Alha 2020), are not affected by the complexity of the game (cf. [SENDC13]).[38] 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.

5   CHILDREN'S RIGHT TO FREEDOM OF THOUGHT

The call for a more integrative approach is getting traction in both academia [Ale21b, KEA+18, AAB+17] and international organizations.[39] Already in 2017, with the Recommendation 2102 (2017) [oEPA17], 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[40] 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."

5.1   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 [IM21].

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 [Ale21b], but something beyond it.

Some believe that to move beyond privacy means the need for new rights [SSS+21, Sie19, IA17]. 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" [IA17].[41]

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" [Ale21a], 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" [Ale21a], 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*

---

[38]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
[39]Cf. e.g., CoE [oEPA17] 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

[40]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)
[41]Although they individuate four 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*).

and belief in the digital environment, for example by emotional analytics or inference."[42]

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.

5.2 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 [Ale21a]

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" [IA17, Bub13, Sen04]. It should be understood as the "conceptual update" [Sen04] of the right to privacy in its self-determination connotation, mixed with interpretations of freedom of thought [Ale21a] already in the jurisprudence of the European Court of Human Rights (*see Nolan and K. v Russia*[43]), and as expressed in international human rights legislation.[44]

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 [Can18]. Emanation of moral value, the general prohibition of the use of manipulative tactics to take advantage of children's vulnerability [OCPo11] 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 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 [TBDO+17]. It is the children's right to be children,

to experience, to make mistakes, and to do so without malevolent interference from adults.

5.3 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 the right of others to conduct business –, freedom of thought is an *absolute* right and does not accept any interference.[45]

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 1), 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.

6 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

---

[42] 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."

[43] "Case of Nolan and K. v. Russia", European Court of Human Rights, 2512/04: https://hudoc.echr.coe.int/eng?i=001-91302

[44] 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 [Ale21a] "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."

[45] "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." [Ale21b]

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.

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

REFERENCES

[AAB⁺17] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, and others. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3):1–41, 2017. Publisher: ACM New York, NY, USA.

[Ale21a] Susie Alegre. Protecting freedom of thought in the digital age. 2021. Publisher: Centre for International Governance Innovation.

[Ale21b] Susie Alegre. Regulating around freedom in the "forum internum". In *ERA Forum*, volume 21, pages 591–604. Springer, 2021. Issue: 4.

[Alh20] Kati Alha. *The Rise of Free-to-Play: How the revenue model changed games and playing*. 2020. URL: https://researchportal.tuni.fi/en/publications/the-rise-of-free-to-play-how-the-revenue-model-changed-games-and-.

[Arr82] Robert L Arrington. Advertising and behavior control. *Journal of Business Ethics*, 1(1):3–12, 1982. Publisher: Springer.

[Ayl20] Timothy Aylsworth. Autonomy and manipulation: Refining the argument against persuasive advertising. *Journal of Business Ethics*, pages 1–11, 2020. Publisher: Springer.

[BDDC⁺19] Fran C. Blumberg, Kirby Deater-Deckard, Sandra L. Calvert, Rachel M. Flynn, C. Shawn Green, David Arnold, and Patricia J. Brooks. Digital Games as a Context for Children's Cognitive Development: Research Recommendations and Policy Considerations. *Social Policy Report*, 32(1):1–33, 2019. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/sop2.3. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/sop2.3, doi:10.1002/sop2.3.

[BM01] Sherry Baker and David L Martinson. The TARES test: Five principles for ethical persuasion. *Journal of Mass Media Ethics*, 16(2-3):148–175, 2001. Publisher: Taylor & Francis.

[BN09] Solon Barocas and Helen Nissenbaum. 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*, 2009.

[BOBG14] Mark Blades, Caroline Oates, Fran Blumberg, and Barrie Gunter. *Advertising to children: New directions, new media*. Springer, 2014.

[Bro12] Roger Brownsword. 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*, pages 223–244, 2012.

[BSS14] Omri Ben-Shahar and Carl E Schneider. *More than you wanted to know: The Failure of Mandated Disclosure*. Princeton University Press, 2014.

[Bub13] Jan-Christoph Bublitz. My mind is mine!? Cognitive liberty as a legal concept. In *Cognitive enhancement*, pages 233–264. Springer, 2013.

[Can06] Turhan Canli. When genes and brains unite: ethical implications of genomic neuroimaging. *Neuroethics: Defining the Issues in Theory, Practice and Policy*, pages 169–184, 2006.

[Can18] Peter Candy. lex (P) Laetoria. In *Oxford Research Encyclopedia of Classics*. 2018.

[Car20] Nicholas Carr. *The shallows: What the Internet is doing to our brains*. WW Norton & Company, 2020.

[CDO⁺18] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.

[CMMMR22] Tommaso Crepax, Victor Muntés-Mulero, Jabier Martinez, and Alejandra Ruiz. Information technologies exposing children to privacy risks: domains and children-specific technical controls. *Computer Standards & Interfaces*, 82:103624, 2022.

[Cou18] Norwegian Consumer Council. Deceived by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy. *Norwegian Consumer Council Report*, 2018. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[Cri87] Roger Crisp. Persuasive advertising, autonomy, and the creation of desire. *Journal of Business Ethics*, 6(5):413–418, 1987. Publisher: Springer.

[CS12] Barbie Clarke and Siv Svanaes. Digital marketing and advertising to children: a literature review. In *Advertising Education Forum*, volume 79, 2012.

[DBMML17] Nestor Duch-Brown, Bertin Martens, and Frank Mueller-Langer. The economics of ownership, access and trade in digital data. 2017. Publisher: JRC Digital Economy Working Paper 2017-01.

[DC20] Lorenzo Dalla Corte. A right to a rule: On the substance and essence of the fundamental right to personal data protection. *Data protection and privacy*, pages 27–58, 2020. Publisher: Hart Publishing.

[DGH⁺11] Kristina M Durante, Vladas Griskevicius, Sarah E Hill, Carin Perilloux, and Norman P Li. Ovulation, female competition, and product choice: Hormonal influences on consumer behavior. *Journal of Consumer Research*, 37(6):921–934, 2011. Publisher: University of Chicago Press Chicago, IL.

[DJVdSHC19] Steffi De Jans, Dieneke Van de Sompel, Liselot Hudders, and Veroline Cauberghe. Advertising targeting young children: an overview of 10 years of research (2006–2016). *International Journal of Advertising*, 38(2):173–206, 2019. Publisher: Taylor & Francis.

[DRRT18] Daniel Demmler, Peter Rindal, Mike Rosulek, and Ni Trieu. PIR-PSI: Scaling Private Contact Discovery. *Proc. Priv. Enhancing Technol.*, 2018(4):159–178, 2018.

[DS18] Aaron Drummond and James D. Sauer. Video game loot boxes are psychologically akin to gambling. *Nature Human Behaviour*, 2(8):530–532, August 2018. Number: 8 Publisher: Nature Publishing Group. URL: https://www.nature.com/articles/s41562-018-0360-1, doi:10.1038/s41562-018-0360-1.

[FM11] Ruth Fischbach and Janet Mindes. Why neuroethicists are needed. *Oxford handbook of neuroethics*, pages 343–76, 2011. Publisher: Oxford University Press New York.

[Fog02] Brian J Fogg. Persuasive technology: using computers to change what we think and do. *Ubiquity*, 2002(December):2, 2002. Publisher: ACM New York, NY, USA.

[For19] John B Ford. What do we know about neuromarketing? *Journal of Advertising Research*, 2019. Publisher: ARF, Advertising Research Foundation. doi:10.2501/JAR-2019-031.

[FR19] Dan Fitton and Janet C. Read. 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*, IDC '19, pages 407–418, New York, NY, USA, June 2019. Association for Computing Machinery. doi:10.1145/3311927.3323136.

[Fuk03] Francis Fukuyama. *Our posthuman future: Consequences of the biotechnology revolution*. Farrar, Straus and Giroux, 2003.

[FW17] Ted Fenton and Reinout W Wiers. Free will, black swans and addiction. *Neuroethics*, 10(1):157–165, 2017. Publisher: Springer.

[GC04] Joshua Greene and Jonathan Cohen. For the law, neuroscience changes nothing and everything. *Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences*, 359(1451):1775–1785, 2004. Publisher: The Royal Society.

[GPS11] Neil Gilbert, Nigel Parton, and Marit Skivenes. *Child protection systems: International trends and orientations*. OUP USA, 2011.

[Gri15] Mark D Griffiths. 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(2):31–37, 2015.

[Har16] Tristan Harris. How technology hijacks people's minds—from a magician and Google's design ethicist. *Medium Magazine*, 2016.

[Har18] Woodrow Hartzog. *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press, 2018.

[HM16] Eszter Hargittai and Alice Marwick. "what can i really do?" explaining the privacy paradox with online apathy. *International journal of communication*, 10:21, 2016.

[HNSH12] Kenneth Hullett, Nachiappan Nagappan, Eric Schuh, and John Hopson. Empirical analysis of user data in game software development. In *Proceedings of the 2012 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, pages 89–98. IEEE, 2012.

[IA17] Marcello Ienca and Roberto Andorno. Towards new human rights in the age of neuroscience and neurotechnology. *Life sciences, society and policy*, 13(1):1–27, 2017. Publisher: BioMed Central.

[IM21] Marcello Ienca and Gianclaudio Malgieri. Mental Data Protection and the GDPR. *Available at SSRN 3840403*, 2021.

[Kar20] Faltin Karlsen. Game Creation, Monetisation Models, and Ethical Concerns. October 2020.

[Kar21] Faltin Karlsen. Balancing Ethics, Art and Economics: A Qualitative Analysis of Game Designer Perspectives on Monetisation. *Games and Culture*, page 15554120211049579, December 2021. Publisher: SAGE Publications. doi:10.1177/15554120211049579.

[KD18] Daniel L. King and Paul H. Delfabbro. Predatory monetization schemes in video games (e.g. 'loot boxes') and internet gaming disorder. *Addiction (Abingdon, England)*, 113(11):1967–1969, November 2018. doi:10.1111/add.14286.

[KEA+18] Beeban Kidron, Alexandra Evans, Jenny Afia, Joanna R Adler, Henrietta Bowden-Jones, Liam Hackett, Anisha Juj, Andrew K Przybylski, Anghrarad Rudkin, and Young Scot. Disrupted childhood: the cost of persuasive design. 2018. Publisher: 5rights.

[KGK+18] Orsolya Király, Mark D Griffiths, Daniel L King, Hae-Kook Lee, Seung-Yup Lee, Fanni Bányai, Ágnes Zsila, Zsofia K Takacs, and Zsolt Demetrovics. Policy responses to problematic video game use: A systematic review of current measures and future possibilities. *Journal of Behavioral Addictions*, 7(3):503–517, 2018. Publisher: Akadémiai Kiadó Budapest.

[KL11] Peter Kenning and Marc Linzmajer. Consumer neuroscience: an overview of an emerging discipline with implications for consumer policy. *Journal für Verbraucherschutz und Lebensmittelsicherheit*, 6(1):111–125, 2011. Publisher: Springer.

[KRCU21] Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell, and Stefan Ullrich. Surveilling the gamers: Privacy impacts of the video game industry. *Available at SSRN 3881279*, 2021.

[KRS+19] Daniel Kales, Christian Rechberger, Thomas Schneider, Matthias Senker, and Christian Weinert. Mobile private contact discovery at scale. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1447–1464, 2019.

[KV16] George F Koob and Nora D Volkow. Neurobiology of addiction: a neurocircuitry analysis. *The Lancet Psychiatry*, 3(8):760–773, 2016. Publisher: Elsevier.

[LCB16] Sonia Livingstone, John Carr, and Jasmina Byrne. One in three: Internet governance and children's rights. 2016. Publisher: UNICEF. Office of Research-Innocenti.

[Les97] Alan I Leshner. Addiction is a brain disease, and it matters. *Science*, 278(5335):45–47, 1997. Publisher: American Association for the Advancement of Science.

[Les09] Lawrence Lessig. *Code: And other laws of cyberspace*. ReadHowYouWant.com, 2009.

[Lin10] Martin Lindstrom. *Buy ology: Truth and lies about why we buy*. Currency, 2010.

[LR07] Robert LaRose and Nora J Rifon. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, 41(1):127–149, 2007. Publisher: Wiley Online Library.

[LSM08] May O Lwin, Andrea JS Stanaland, and Anthony D Miyazaki. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of retailing*, 84(2):205–217, 2008.

[LSN18] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. Conceptualising privacy online: what do, and what should, children understand? *Parenting for a Digital Future*, 2018. Publisher: London School of Economics and Political Science.

[LSN19] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. Children's data and privacy online: growing up in a digital age: an evidence review. 2019. Publisher: London School of Economics and Political Science, Department of Media and ….

[LTBG18] Sonia Livingstone, Damian Tambini, Nikola Belakova, and Emma Goodman. Protection of children online: does current regulation deliver? *Media Policy Brief*, 2018.

[LW77] Robert S Laufer and Maxine Wolfe. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, 33(3):22–42, 1977. Publisher: Wiley Online Library.

[LW17] Deborah Lupton and Ben Williamson. The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5):780–794, 2017. Publisher: SAGE Publications Sage UK: London, England.

[Mad15] Jamie Madigan. *Getting gamers: The psychology of video games and their impact on the people who play them*. Rowman & Littlefield, 2015.

[Mat15] Steve Matthews. Neuromarketing: What is it and is it a threat to privacy? In *Handbook of Neuroethics*. 2015. doi:10.1007/978-94-007-4707-4_154.

[MGC+17] P. Maene, J. Götzfried, R. de Clercq, T. Müller, F. Freiling, and I. Verbauwhede. Hardware-Based Trusted Computing Architectures for Isolation and Attestation. *IEEE Transactions on Computers*, PP(99):1–1, 2017.

[MIR08] Emily R Murphy, Judy Illes, and Peter B Reiner. Neuroethics of neuromarketing. *Journal of Consumer Behaviour: An International Research Review*, 7(4-5):293–302, 2008. Publisher: Wiley Online Library.

[MJ19] Simon McCarthy-Jones. The autonomous mind: The right to freedom of thought in the twenty-first century. *Frontiers in Artificial Intelligence*, 2:19, 2019. Publisher: Frontiers.

[MK17] Milda Macenaite and Eleni Kosta. Consent for processing children's personal data in the EU: following in US footsteps? *Information & Communications Technology Law*, 26(2):146–197, 2017. Publisher: Taylor & Francis.

[mox17] moxie0. Technology preview: Private contact discovery for Signal. 2017. URL: https://signal.org/blog/private-contact-discovery/.

[MRHJ21] Andreas Kristiansen Melzer, Anna Kristine Roarsen, Marte Hoff Hagen, and Letizia Jaccheri. Towards Suitable Free-to-Play Games for Children. In Jannicke Baalsrud Hauge, Jorge C. S. Cardoso, Licínio Roque, and Pedro A. Gonzalez-Calero, editors, *Entertainment Computing – ICEC 2021*, Lecture Notes in Computer Science, pages 264–276, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-89394-1_20.

[NJ14] Joe Newman and Joseph Jerome. Press Start to Track Privacy and the New Questions Posed by Modern Video Game Technology. *AIPLA QJ*, 42:527, 2014. Publisher: HeinOnline.

[oC19] U.K. House of Commons. Immersive and addictive technologies, fifteenth report of session 2017–19. 2019. URL: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/1846.pdf.

[OCPo11] Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson, and others. The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4):800–804, 2011. Publisher: Am Acad Pediatrics.

[oE19] Council of Europe. Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. 2019. URL: https://www.coe.int/en/web/data-protection/-/declaration-by-the-committee-of-ministers-on-the-manipulative-capabilities-of-algorithmic-processes.

[OEC21] OECD. Children in the digital environment. (302), 2021. URL: https://www.oecd-ilibrary.org/content/paper/9b8f222e-en, doi:https://doi.org/https://doi.org/10.1787/9b8f222e-en.

[oEPA17] Council of Europe: Parliamentary Assembly. Technological convergence, artificial intelligence and human rights. 2017. URL: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726.

[OLAB13] Laura Owen, Charlie Lewis, Susan Auty, and Moniek Buijzen. Is children's understanding of nontraditional advertising comparable to their understanding of television advertising? Journal of Public Policy & Marketing, 32(2):195–206, 2013. Publisher: SAGE Publications Sage CA: Los Angeles, CA.

[OR16] Jukka-Pekka Onnela and Scott L Rauch. Harnessing smartphone-based digital phenotyping to enhance behavioral and mental health. Neuropsychopharmacology, 41(7):1691–1696, 2016. Publisher: Nature Publishing Group.

[Pur18] Nadezhda Purtova. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1):40–81, 2018. Publisher: Taylor & Francis.

[PZ20] Liliana Pasquale and Paola Zippo. A Review of Age Verification Mechanism for 10 Social Media Apps. 2020. Publisher: CyberSafe Ireland.

[Ram19] Thomas Zoëga Ramsøy. 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):281–294, 2019. Publisher: Journal of Advertising Research.

[Rin19] Kathryn E Ringland. 'Autsome': Fostering an Autistic Identity in an Online Minecraft Community for Youth with Autism. In International Conference on Information, pages 132–143. Springer, 2019.

[RRM18] N Cameron Russell, Joel R Reidenberg, and Sumyung Moon. Privacy in Gaming. Fordham Intell. Prop. Media %Ent. LJ, 29:61, 2018. Publisher: HeinOnline.

[SA21] Marijn Sax and Jef Ausloos. 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), 2021. Publisher: Elgar Online.

[SBDC15] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), pages 1–17, 2015.

[SBE21] Yanhui Su, Per Backlund, and Henrik Engström. Comprehensive review and classification of game analytics. Service Oriented Computing and Applications, 15(2):141–156, 2021.

[Sch12] Natasha Dow Schüll. Addiction by design. Princeton University Press, 2012.

[SDB18] Rafet Sifa, Anders Drachen, and Christian Bauckhage. Profiling in games: Understanding behavior from telemetry. Social interactions in virtual worlds: An interdisciplinary perspective, 2018. Publisher: Cambridge University Press.

[SDM97] Wolfram Schultz, Peter Dayan, and P Read Montague. A neural substrate of prediction and reward. Science, 275(5306):1593–1599, 1997. Publisher: American Association for the Advancement of Science.

[Sen04] Wrye Sententia. Neuroethical considerations: cognitive liberty and converging technologies for improving human cognition. Annals of the New York Academy of Sciences, 1013(1):221–228, 2004. Publisher: Blackwell Publishing Ltd Oxford, UK.

[SENDC13] Magy Seif El-Nasr, Anders Drachen, and Alessandro Canossa. Introduction. In Magy Seif El-Nasr, Anders Drachen, and Alessandro Canossa, editors, Game Analytics: Maximizing the Value of Player Data, pages 3–12. Springer, London, 2013. doi:10.1007/978-1-4471-4769-5_1.

[She11] Shlomo Sher. A framework for assessing immorally manipulative marketing tactics. Journal of Business Ethics, 102(1):97–118, 2011. Publisher: Springer.

[Sie19] Alexander Sieber. Souled out of rights? - Predicaments in protecting the human spirit in the age of neuromarketing. In Life Sciences, Society and Policy, volume 15, 2019. ISSN: 21957819 Issue: 1. doi:10.1186/s40504-019-0095-4.

[sig21] signal. Signal. 2021. URL: https://signal.org/.

[Sim94] Herbert A Simon. The bottleneck of attention: connecting thought with motivation. 1994. Publisher: University of Nebraska Press.

[SL18] van der Hof Simone 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(1), 2018.

[SLG21] Giovanni Sartor, Francesca Lagioia, and Federico Galli. Regulating targeted and behavioural advertising in digital services. 2021. Publisher: Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies.

[SLK+20] Gary W Small, Jooyeon Lee, Aaron Kaufman, Jason Jalil, Prabha Siddarth, Himaja Gaddipati, Teena D Moody, and Susan Y Bookheimer. Brain health consequences of digital technology use. Dialogues in Clinical Neuroscience, 22(2):179, 2020. Publisher: Les Laboratoires Servier.

[Smi02] Ale Smidts. Kijken in het brein: Over de mogelijkheden van neuromarketing. 2002. Publisher: EIA-2002-012-MKT.

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

[SSAH17] Steven J Stanton, Walter Sinnott-Armstrong, and Scott A Huettel. Neuromarketing: Ethical implications of its use and potential misuse. Journal of Business Ethics, 144(4):799–811, 2017. Publisher: Springer.

[SSGA21] Muhammad Suleman, Tariq Rahim Soomro, Taher M Ghazal, and Muhammad Alshurideh. Combating Against Potentially Harmful Mobile Apps. In The International Conference on Artificial Intelligence and Computer Vision, pages 154–173. Springer, 2021.

[SSS+21] Oleksii M Skriabin, Dmytro B Sanakoiev, Natalia D Sanakoieva, Vita V Berezenko, and Yuliia V Liubchenko. Neurotechnologies in the advertising industry: Legal and ethical aspects. Innovative Marketing, 17(2):2021, 2021. URL: http://dx.doi.org/10.21511/im.17, doi:10.21511/im.17(2).2021.17.

[SW08] Valerie Steeves and Cheryl Webster. Closing the barn door: The effect of parental supervision on canadian children's online privacy. Bulletin of Science, Technology & Society, 28(1):4–19, 2008.

[SW14] Robert H Sloan and Richard Warner. Beyond notice and choice: Privacy, norms, and consent. J. High Tech. L., 14:370, 2014. Publisher: HeinOnline.

[Swa12] Melanie Swan. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. Journal of Sensor and Actuator networks, 1(3):217–253, 2012. Publisher: Multidisciplinary Digital Publishing Institute.

[TBDO+17] Amanda Third, Delphine Bellerose, Juliano Diniz De Oliveira, Girish Lala, and Georgina Theakstone. Young and Online: Children's perspectives on life in the digital age. 2017. Publisher: Institute for Culture and Society (WS), UNICEF.

[VdBVdH12] Bibi Van den Berg and Simone Van der Hof. What happens to my data? A novel approach to informing users of data processing practices. First Monday, 17(7), 2012.

[Ver20] Valerie Verdoodt. Children's Rights and Commercial Communication in the Digital Era, volume 10. Intersentia, 2020.

[VRJPVN10] Eva A Van Reijmersdal, Jeroen Jansz, Oscar Peters, and Guda Van Noort. The effects of interactive brand placements in online games on children's cognitive, affective, and conative brand responses. Computers in Human Behavior, 26(6):1787–1794, 2010. Publisher: Elsevier.

[vSKGY20] Stephan van Schaik, Andrew Kwong, Daniel Genkin, and Yuval Yarom. SGAxe: How SGX Fails in Practice. 2020. URL: https://sgaxeattack.com/.

[WGH08] R Mark Wilson, Jeannie Gaines, and Ronald Paul Hill. Neuromarketing and consumer free will. Journal of consumer affairs, 42(3):389–410, 2008. Publisher: Wiley Online Library.

[Wil17] Edward O Wilson. The origins of creativity. Liveright Publishing, 2017.

[WNT14] Martin KJ Waiguny, Michelle R Nelson, and Ralf Terlutter. 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):257–277, 2014. Publisher: Springer.

[WOS+11] Joanna M Wardlaw, Garret O'connell, Kirsten Shuler, Janet DeWilde, Jane Haley, Oliver Escobar, Shaun Murray, Robert Rae, Donald Jarvie, Peter Sandercock, and others. "Can it read my mind?"–What do the public and experts think of the current (mis) uses of neuroimaging? PLoS one, 6(10):e25829, 2011. Publisher: Public Library of Science San Francisco, USA.

[Wri97] Benjamin D Wright. A history of social science measurement. Educational measurement: Issues and practice, 16(4):33–45, 1997. Publisher: Wiley Online Library.

[WSJ20] Kim Wuyts, Laurens Sion, and Wouter Joosen. LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pages 302–309. IEEE, 2020.

[Wu17] Tim Wu. The attention merchants: The epic scramble to get inside our heads. Vintage, 2017.

[Zub19] Shoshana Zuboff. Surveillance capitalism. Esprit, 5:63–77, 2019. Publisher: Editions Esprit.