

Being played in everyday life

Massive data collection on mobile games as part of ludocapitalist surveillance dispositif

MAUDE BONENFANT, ALEXANDRA DUMONT,
& LAURA ISEUT LAFRANCE ST-MARTIN

DEPARTMENT OF SOCIAL AND PUBLIC COMMUNICATION, UNIVERSITÉ DU QUÉBEC À MONTRÉAL,
CANADA

ABSTRACT

Surveillance in videogames is a well-known phenomenon. Designated as the fastest-growing sector of the videogame industry, mobile games – particularly free-to-play games – capitalise substantially on the collection of user data. Based on the promise of offering personalised gaming and advertising experiences, a vast quantity of data, including personal identifier and geolocation data, is acquired through players' mobile devices. While the information obtained may appear fragmented or invisible to players, they are consolidated in the hands of data brokers, resulting in a very lucrative economic sector. From this perspective, the practice of the mobile game, although innocuous at first consideration, raises essential ethical questions regarding the ludocapitalist surveillance dispositif established by this industry. In this chapter, we seek to problematise everyday surveillance in mobile gaming, explain how the videogame and marketing industries operate it, and examine gamers' ("ordinary" citizens) involvement in the banalisation of this massive data gathering.

KEYWORDS: ludocapitalism, mobile games, free-to-play, surveillance capitalism, Foucauldian dispositif

Bonenfant, M., Dumont, A., & Lafrance St-Martin, L. I. (2023). Being played in everyday life: Massive data collection on mobile games as part of ludocapitalist surveillance dispositif. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 21–44). Nordicom, University of Gothenburg. <https://doi.org/10.48335/9789188855732-1>

Introduction

Journalist Julian Dibbell (2007) highlighted, in his article “The Life of the Chinese Gold Farmer”, the growing connection between playing videogames and capitalism. This *New York Times* article describes the harsh living conditions of Chinese workers forced to play “massive multiplayer online games” for extended periods to acquire and then sell commodities over the Internet for profit. Dibbell argued that these modern-day sweatshops are symptoms of the capitalist ideology that aims to transform all human activities into instruments of wealth creation.

This economic framework blurs the distinction between labour and leisure by combining the principles of play (*ludus*) with contemporary capitalism. Known as ludocapitalism, this paradigm refers to,

a hybrid or transitional moment of capitalism that describes its processes of commodity production and capital accumulation through reference to playing as a central concept of human activity and social organization, superseding the concept of work as the locus of rationality in traditional capitalist labour formations. (Jordan, 2014: 1)

Therefore, ludocapitalism considers the act of playing and generating wealth to be equivalent.

However, the capitalisation of players’ activities is no longer the industry’s primary monetisation method (Dibbell, 2007). Numerous game developers’ revenue streams instead depend on collecting and selling consumer data, giving rise to new surveillance-based business models (Whitson, 2013). As such, surveillance capitalism centres primarily on commodifying personal data, with various industries – including marketing, insurance, and healthcare – using personal information to create profiles and infer customer behaviour (Zuboff, 2018). Zuboff described this economic and political shift as “a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales” (Zuboff, 2018: v). Accordingly, collecting personal data allows the prediction of behavioural patterns through increasingly sophisticated automated computer techniques, such as machine learning and artificial intelligence. Data exploitation aims to induce consumer behaviour by relying on the self-fulfilling prophecy (Merton, 1948) and manipulating desires through ever-increasingly precise individual profiling. Zuboff referred to this transition as a “dispossession by surveillance”, an “exploitation of human nature”, and a mechanism of social control that undermines freedom, democracy, and privacy. Furthermore, Zuboff (2015) argued that the well-known figure of Big Brother now takes the form of Big Other, a distributed power network for massive data collection.

In this chapter, we propose to articulate the principles of ludocapitalism and those of surveillance capitalism to introduce the new concept of surveillance ludocapitalism. While observable in the videogame industry,

this concept rationale is most pervasive in the mobile game sector; rather than relying on retail profits, free-to-play mobile games depend substantially on the extensive collection of user data, including in-game behaviours and exchanges, which is algorithmically processed to develop targeted sales profiles (Bonenfant, 2021). The more individuals play, the more lucrative they become. Accordingly, a player's every action is subject to capitalisation, as autonomous algorithms log and extract each choice made in the game, the app store, and the smartphone itself. Despite its numerous negative implications for gamers and citizens, this business model based on surveillance capitalism grows year after year.

From this perspective, we explore everyday surveillance in mobile gaming, define how the videogame and marketing sectors use it, and examine gamers' participation as "ordinary" citizens in the trivialisation of this massive data gathering. The question guiding our research is: What are the conditions of possibility for widespread acceptance of large-scale surveillance through mobile gaming? We aim to provide a better understanding of the mobile games' economic, technical, psychological, semiotic, legal, and social context by focusing on participants' voluntary involvement and engagement within this everyday ludocapitalist surveillance dispositif, including, but not limited to, their "disciplinarisation" (Foucault, 1975). Our study contributes to the existing literature by schematising an industry traditionally challenging to investigate due to a lack of information and its structure's opacity.

First, we briefly explain the mobile game industry's general business model, emphasising the free-to-play model. This demonstration illustrates the interrelations between this business model and the surveillance economic ecosystem. We then focus on the persuasive design strategies implemented by mobile games to ensure recurring and prolonged player connection, thus highlighting the various deceptions that some companies use to exploit individuals' gaming activity and prevent them from fully understanding consent issues raised by gaming apps. We then examine these issues in the context of the North American and European regulatory frameworks, underlining the shortcomings of the legal protection that citizens – particularly children – are given. Subsequently, we examine these legal flaws in relation to the current social context, which promotes individuals' transparency and considers data collection as standard, to the point of being unproblematic, invisible, and indisputable. Finally, the Foucauldian notion of dispositif is used to analyse how mobile gaming is perceived as an assemblage of several elements, thus allowing us to explain the disciplinarisation of players to participate directly and voluntarily in this ludocapitalist surveillance dispositif.

Mobile game business models – from free-to-play to pay-to-win

Beginning in the early 2000s, data collection on player behaviour by videogame companies slowly gained popularity as technological developments advanced: network gaming, digital distribution, mobile games, and online console gaming. This widespread data collection practice resulted in a shift toward a data-driven industry (Whitson, 2013). Among its various iterations, three major business models are now prevalent: premium games, downloadable content, and games as a service (Nieborg, 2016b).

The premium games model refers to the conventional concept in which players must purchase a videogame to enjoy it (Nieborg, 2016b). In contrast, the downloadable content model focuses on additional content, either in the form of a game expansion or cosmetics goods that players can purchase for a lesser fee (Lee et al., 2015). Lastly, the games-as-a-service model provides access to videogame titles through a monthly or annual subscription, much like the paradigm shift operated by several large software developers. Along these various models, developers use player data to modulate the in-game experience and assist in their design choices, such as incorporating features that promote extended connection times. However, the business model that relies most heavily on monetising players' data is the free-to-play model (Nieborg, 2016a).

In addition to encouraging the videogame industry to reconsider its economic strategies, technological advancements such as smartphones and tablets have contributed to the rising popularity of gaming. Supported by their high global adoption rates, mobile devices have swiftly imposed themselves as the platform of choice for many gamers and developers (Newzoo, 2021). In the Nordics, mobile phones are the preferred gaming platform (26%), outpacing consoles (11%) and personal computers (21%) (Deloitte, 2019). The revenues generated by this segment attest to its new popularity; in 2020, the mobile gaming market accounted for 52 per cent of the industry's overall revenue, totalling USD 79 billion (Newzoo, 2021). However, unlike console or computer games, mobile games are frequently available for free, thus leading the industry to explore alternative forms of income compatible with this medium and consumers' expectations.

Based on preexisting models, the videogame industry established various monetisation sources over the years. While sporting different names, the mobile games business models rely primarily on two sources of income: microtransactions and ad revenues (Whitson, 2019). Microtransactions, ubiquitous in free-to-play (also called freemium) mobile games, usually take the form of consumable (one-time-use) or non-consumable (permanent-access) items, granting players game advantages, whether functional or aesthetic (Alha, 2020). These virtual items, which range in price from a couple to over a hundred US dollars, provide studios with a simple income stream. This

business model uses the collection of personal data to predict player behaviour by creating consumer profiles to present offers on items at times when the probability of purchase is highest (Nieborg, 2016a). The exploitation of these possible purchase behaviours even gives rise to what the industry has called whales (Balakrishnan & Griffiths, 2018). Central to the mobile game economic ecosystem, whales are the dedicated high-spending gamers who account for 2–5 per cent of the player population and whose purchases account for a significant portion of the mobile gaming industry's income (Whitson, 2019).

On the other hand, advertising sales are a substantial and consistent source of revenue for mobile games (Alha, 2020). More than selling spaces in the form of interstitial advertising, interactive commercials, native ads, or rewarded video ads, developers give advertisement companies access to their players' personal information. Under the guise of offering personalised advertising, these various commercial entities have access to data related to the mobile device used, including persistent information, such as device ID, serial number, SIM ID, but also personal and sensitive information like name, gender, address, postal code, e-mail address, location data, search terms, and medical information (Christl & Spiekermann, 2016; Reyes et al., 2018; Wijesekera et al., 2017).

Given the primarily opaque nature of the industry's data processing ecosystem, it proves challenging to piece together an accurate image (Nieborg, 2016a). Nonetheless, we can partially reconstruct this circuit by relying on players' acquisition process of mobile games combined with investigative work with field actors. The data collection process begins whenever a user accepts the terms of service of a mobile game, thus granting developers access to their personal information (Wijesekera et al., 2017). Specific data, such as device information, network connection information, or player activity, are initially collected and used to ensure the game's proper functioning (Reyes et al., 2018). Furthermore, mobile games encourage users to disclose additional personal information by sometimes requiring excessive permissions or allowing players to connect with their social network accounts (Alha, 2020; Kröger et al., 2021). Presented as a means of interacting with friends or preserving one's progress, the use of Facebook or Google accounts allows developers to connect the player's profile to their offline identity (Brückner et al., 2017; Christl, 2017).

Beyond the developers' use, the players' information is subsequently shared with advertising companies responsible for monetising the application. Through programmatic advertising techniques, ad providers then use this information to associate each player with offers relevant to them (Christl & Spiekermann, 2016). This complex procedure, also known as real-time bidding, refers to an automatic auction process involving multiple ad publishers bidding for advertising space related to specific consumer segments (Christl &

Spiekermann, 2016). Accordingly, this monetisation strategy includes many intermediaries with whom personal information might be shared. If developers declare in their privacy policies that the information collected is solely utilised for game stability and general operation, third parties with whom they conduct business, such as Google AdMob, AppsFlyer, or Mopub, are exempt from these conditions (Appfigures, 2022; Valentino-DeVries et al., 2018).

Accordingly, a vast quantity of data is acquired throughout players' mobile devices, including geolocation data and MAC address (Unity, 2020):

By design, any third-party service bundled in an Android app inherits access to all permission-protected resources that the user grants to the app. In other words, if an app can access the user's location, then all third-party services embedded in that app can as well. (Reardon et al., 2019: 1)

These third parties, usually constituted of software development kits, provide developers with services assisting them in the various stages of their product's deployment, such as game engines, coding, analytical tools for crash reports, advertising, or financial services (Myrstad & Tjøstheim, 2021; Reardon et al., 2019). These development tools are commonplace, as a 2016 study calculated that free-to-play mobile game apps had an average of 18.6 third parties (Jonathan, 2016). While reducing the cost associated with development and game maintenance, these third parties lack transparency regarding their use of consumers' data. The ambiguity surrounding these critical security and ethical issues is even more concerning, given that third-party vendors are free to share the data obtained with their own third parties (Myrstad & Tjøstheim, 2021).

The various entities partaking in this ecosystem can sell the data they have gathered to data brokers. The United States Federal Trade Commission (FTC, 2012: para. 2) defines these entities as "companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies". Data brokers specialise in profiling and predicting consumers' behaviours using large databases fed by public and private data on individuals' consumption patterns (Rieke et al., 2016). These profiles are later sold to other entities working in the marketing or risk assessments sectors (Myrstad & Tjøstheim, 2021)

While the general public is familiar with some of the major companies in this industry, primarily because of the development of credit scores, companies such as Acxiom and Equifax also created various consumer scores ranging from Job Security Score, Charitable Donor Scores, and even Medication Adherence Score (Christl & Spiekermann, 2016). Acquiring data, including personal identifiers from mobile devices, social network profile information, credit card usage, and public records, these companies generate profiles capable of inferring our desires before they occur (Myrstad & Tjøstheim, 2021).

The influence of these companies becomes even more significant when we

consider that these various actors buy and sell each other's data (Christl & Spiekermann, 2016). Accordingly, the current state of mobile gaming and its commercial ramification makes it nearly impossible for users to track the companies with whom their data is shared. In their report, *Out of Control: How Consumers are Exploited by the Online Advertising Industry*, Myrstad and Tjøstheim (2021: 11) argued: "The extent of tracking and complexity of the adtech industry is incomprehensible to consumers, meaning that individuals cannot make informed choices about how their personal data is collected, shared and used". Consequently, the massive commercial surveillance throughout the adtech industry is at odds with our fundamental rights and freedoms. From this perspective, the practice of the mobile game, although innocuous at first sight, raises essential ethical questions regarding the surveillance ludocapitalism established by this industry.

Persuasive design – playing or being played?

Surveillance ludocapitalism partially shares the same economic logic as platform capitalism, often labelled the "fourth economic revolution" (Srnicek, 2017). The European Commission projected in 2017 that the personal data processing industry would generate EUR 1 trillion in revenue by 2020, accounting for roughly 8 per cent of the European Union's GDP (gross domestic product) (Thirani & Gupta, 2017). The longer users interact with and remain on a digital platform, the more wealth they create for the platform's owners. Users are developers' resources, but they are also the client of the transformed product: They are the audience of increasingly targeted advertising. Therefore, user attention is one of the foundations of platform capitalism (Citton, 2014).

In a world of information overload, data collectors and marketing agencies compete for users' attention. In these "Great Platform Wars", big digital platforms such as Facebook and Google use various techniques to keep users connected and engaged for as long as possible. Srnicek (2017: 58) argued that "the more activities a firm has access to, the more data it can extract and the more value it can generate from those data, and therefore the more activities it can gain access to". Thus, platforms constantly create new ways to access parts of users' lives, such as unified logins and monopolistic game stores.

Within the context of platform capitalism, mobile games also use various design techniques to capture and maintain the attention of as many users as possible. Games have an advantage: They are fun and can conceal the data collection behind quick and straightforward game mechanics, such as time-limited rewards, interval resource collection, or daily quests. From this perspective, developers implement many features based on persuasive design with the fundamental intent of directly influencing behaviour. Thus, the principles of this design approach rely on classical and operant conditioning and behavioural psychology.

Reinforcement techniques are the basis of the persuasive designs imple-

mented by mobile game studios to “train” behaviour. As part of our research project, we compiled a comprehensive list of persuasive design tactics that benefit surveillance ludocapitalism. Some of the more prevalent strategies used in free-to-play games are as follows: 1) setting number or time limits on actions (e.g., energy regeneration), forcing the player to wait between gaming sessions in order to continue their progression, which causes them to think about the game often and make time during the day to play; and 2) giving players rewards each time they connect to the game (with, e.g., a daily or time limit on the gift they can receive), which, based on positive reinforcement, ensures that most players join at least once a day, thus creating a habit through conditioning.

Conversely, some games use negative reinforcement techniques, for example, possession removal, which involves threatening to take away a player’s asset if they do not perform a given action at the designated time. This way of conditioning behaviour is considered more efficient, as the fear of losing something is stronger than the promise of winning a gift (loss aversion).

Furthermore, mobile games often implement irregular rewards and gambling mechanics (e.g., loot box), making it difficult to predict when the game will reward the player. According to operant conditioning and contemporary cognitive science, irregular rewards are more addictive: “Random rewards motivate players to engage in an activity with persistent effort to obtain a desired item” (Legner et al., 2019). Some games create a compulsion loop by gradually increasing the difficulty of obtaining rewards, the worth of which is always random. The desire to earn rewards, combined with serotonin responses, promotes obsessive behaviour, especially when the collection of rare rewards is encouraged.

The integration of online multiplayer mode also extends players’ connection times by adding cooperative or competitive features:

The fact that people respond socially to computer products has significant implications for persuasion. It opens the door for computers to apply a host of persuasion dynamics that are collectively described as social influence – the type of influence that arises from social situations. (Fogg, 2002: 90)

Following this idea, persuasive design uses known social dynamics such as peer pressure, social comparison, and fear of missing out to influence users’ behaviours. Regarding the production and collection of personal data, persuasive design increases the return rate of players and time spent in a game to ensure a consistent output of data and advertising time.

Considering the capital invested and the market’s competitiveness, some developers even employ design dark patterns explicitly aimed to deceive people into performing actions they do not necessarily intend to do (Hodent, 2020). For example, “platforms use [design tactics] to manipulate users into

disclosing information” (Waldman, 2020: 105). While they are widespread in online platforms, these tactics are also present in videogames: “A gaming dark pattern is something that is deliberately added to a game to cause an unwanted negative experience for the player with a positive outcome for the game developer” (Dark Pattern Games, n.d). The website *Dark Pattern Games* (www.darkpattern.games) identifies many temporal, monetary, social, and psychological dark patterns.

These various design choices highlight the pervasiveness and apparent invisibility from which free-to-play mobile games can manipulate and mislead players’ practices. Through design based on behavioural psychology, users are encouraged to extend their gaming sessions, link their social media accounts, and, in the process, share additional information about their whereabouts, habits, risk aversions, or their ability to delay gratification. This data obtained continuously over time could then be used to fine-tune companies’ consumer profiles, resulting in more accurate predictions. Given the increasing sophistication of these techniques, it seems difficult, if not impossible, for individuals to avoid or protect themselves against these manipulations.

Deception and dishonesty – agreeing to terms of service

Concerns over consumer data usage have received considerable attention in recent years. The publications of various stories in mainstream media on the safety issues surrounding our online habits, added to the rising popularity of password managers and virtual private networks, may indicate that individuals have acquired greater digital literacy regarding cybersecurity (Ghosh, 2020; Ringel, 2021; Stahl, 2021; Wamsley, 2020; Winder, 2019). Despite increased awareness, individuals still find it challenging to discern how companies use their information. Terms of service agreements rarely provide information about which third parties have access to a player’s data, and when they do, it is the consumer’s responsibility to review those third parties’ privacy policies (Myrstad & Tjøstheim, 2021).

These documents’ lack of transparency extends beyond their substance and into their structure and verbiage. In their conference proceedings, “On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies”, Okoyomon and colleagues (2019) argued that mobile-app privacy policies employ ambiguous wording, an inadequate reading level of expression, and long-winded formats, which contributes to their vagueness. Furthermore, the design used by companies to communicate their privacy policies, while adhering to legal standards, is not suited for consumer comprehension. Ari Ezra Waldman (2018: 133) claimed in his article, “Privacy, Notice, and Design”, that the current format of privacy policies represents “‘unpleasant design,’ or design that deters certain behaviours by exercising a form of social control against actors”. Accordingly, these decisions, whether voluntary or not, made

by service providers discourage individuals from informing themselves about the use of their personal information, thus preventing them from granting free and informed consent (Okoyomon et al., 2019).

Companies' deceptive practices are not limited to "manipulative and unfair" policies but also to their implementation (Waldman, 2018: 81–82). For instance, numerous applications for children include contradicting information about safety measures implemented to safeguard minors. Analysing 8,030 apps published under the Google Play Store's "Designed For Families" section, Okoyomon and colleagues (2019: 5) discovered that 9.1 per cent of them (728 apps) expressed in their privacy policies that their products are not aimed at children under 13 years old, thus indicating inconsistency between the nature of their products and their legal records. Furthermore, 30.6 per cent (2,457 apps) of the apps studied maintained that they are "not knowingly" collecting personally identifiable information from minors under the age of 13 (Okoyomon et al., 2019: 5). As Okoyomon and colleagues pointed out, this is even more problematic, as it implies that developers are oblivious about the data they collect and share with third parties.

If companies cannot protect the personal data of the most vulnerable population, adult data privacy violations are also prevalent, enabling surveillance capitalism via mobile gaming. Accordingly, privacy policies' lack of transparency, confusing terminology, and developers' non-compliance underline the need to protect individuals and regulate the industries benefiting from data collection.

Legal and regulatory framework – playing between the lines

There is currently little legislation governing the collection and use of players' data by videogame developers. Examining the current laws in North America, Europe, and the Nordic countries reveals that individuals are sometimes poorly or insufficiently protected and that these regulations do not reflect the current technological context.

Information collection is regulated in Canada by the Personal Information Protection and Electronic Documents Act (PIPEDA). This Act, intended to safeguard Canadians whose personal information is collected by commercial entities, does not include any provisions relating to minors (PIPEDA, 2019). Accordingly, from a legal standpoint, no distinction is made between adults, adolescents, and children, leaving Canadians unprotected. Furthermore, this federal legislation has been criticised for being ill-suited to the current digital environment, its limited actions in assigning sanctions, and its difficulty in holding companies accountable for personal data breaches (Terrien, 2021).

The US has no federal regulations dedicated explicitly to protecting its citizens' data against commercial use (Rieke et al., 2016). In their report, *Data Brokers in an Open Society*, Rieke, Yu, Robinson, and von Hoboken

(2016: 16) described the American legal landscape as “a patchwork of sector-specific laws [that] govern the collection and use of personal information in certain situations, in certain sectors, or by certain types of entities”. Thus, the laws implemented provide limited and circumstantial safeguards. These legislations aim to ensure the confidentiality of medical data by healthcare providers and insurers (Health Insurance Portability and Accountability Act), the protection of data used by credit companies (Fair Credit Reporting Act), and the protection of communications exchanged by verbal or electronic means (Electronic Communications Privacy Act) (Rieke et al., 2014).

Although no federal law specifically addresses the data collected in the context such as mobile gaming, minors are covered by the Children’s Online Privacy Protection Act (COPPA). COPPA, which was approved in 1998, adopted in 2000, and updated in 2013, requires service providers who collect personal information from children under the age of 13 to make their privacy policies, which outline how personal data is gathered and handled, widely available to the public (FTC, 2020). Parents must also be directly informed about data collection and privacy policies, and their consent must be obtained before children access their products. Finally, users must have the opportunity to withdraw their consent and delete the data collected. While COPPA defines civil penalties for non-compliant operators, the Federal Trade Commission has sanctioned only eight service providers in the last three years (PRIVO, n.d.). However, Reyes and colleagues (2018) described these cases as “isolated incidents” in their article, “Won’t Somebody think of the Children? Examining COPPA Compliance at Scale”.

In Europe, the General Data Protection Regulation (GDPR) is undoubtedly the law that best protects individuals, although it could be stricter (GDPR, 2018). Adopted in April 2016 and implemented in May 2018, the GDPR aims to protect the privacy of European Union residents while also harmonising the numerous regulatory measures of its nations (Rieke et al., 2016). This legislation focuses on personal data processing, safeguarding one’s fundamental rights and freedoms relating to information privacy, and holding the entities involved in the data processing accountable for their actions.

The GDPR acknowledges the importance of protecting children’s data, and according to article 8, it is legal to collect and handle data from minors above 16 (GDPR.EU, 2018). However, service providers can lawfully use the data of minors aged 16 and under with the consent of the child’s parent or guardian. This article also stipulates that companies must exercise reasonable effort to obtain and verify parental consent. It is worth mentioning that GDPR’s members can lower the age of consent to 13 years old, which Denmark, Finland, Norway, and Sweden implemented (Macenaite & Kosta, 2017). The exclusion of this demographic group from digital platforms was a significant point of contention during the law’s passage, with many support-

ers believing that it would be detrimental to children's freedom of expression and right to information (Macenaite & Kosta, 2017).

In addition to being protected by the European Union legislation, the Nordic countries have adopted additional regulations to address some of the GDPR's shortcomings. These laws, which complement the GDPR and thereby better safeguard Nordic citizens, do not provide further protection for minors. As a result, children aged 13 and up are legally regarded as adults in Denmark, Finland, Norway, and Sweden regarding data processing (Macenaite & Kosta, 2017).

In the event of non-compliance with these regulations, the GDPR can enforce administrative fines based on the severity of the offence (GDPR, 2018). Accordingly, the penalties attributed are based on a series of criteria, such as the nature, severity, duration, harm done to consumers, and the company's intentional or negligent conduct. Since its implementation in May 2018, the GDPR imposed 940 fines for a total sum of EUR 1,556,179,408 (CMS, 2022). Although the GDPR constitutes one of the most robust legislations to date, several challenges related to its enforcement remain. Among these are the countries' disparities in interpretation, application, and fines assessment procedure regarding the offenders' financial operations (Rieke et al., 2016; McKean et al., 2022).

Aside from these numerous laws, the videogame industry has tried to self-regulate its activities and assist consumers in making more informed decisions. Examples include videogame rating systems such as the Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI). Although this grading system is entirely voluntary, some businesses insist on its inclusion in the items they sell. In this sense, access to specific sales platforms represents one of the only incentives for developers to use these tools. However, these self-regulation programmes solely evaluate the game's content (ESRB, n.d.; PEGI, n.d.). While shown alongside the game classification, interactive or content elements such as in-game purchases or user interactions do not affect a product's rating (ESRB, n.d.). Digital games, like mobile games, can also obtain a rating under the International Age Rating Coalition (IARC), enabling digital sales platforms to display the appropriate rating according to the organisation's guidelines in place in the user's country (IARC, n.d.). None of the above are reliable indicators of player privacy protection or compliance with legislation such as COPPA or the GDPR (Falzon, 2019; PEGI, n.d.).

On the other hand, some self-regulatory programmes explicitly target data collection from kids under the age of 13. This voluntary initiative, known as the Safe Harbor Program, is implemented by COPPA, and the US Federal Trade Commission allows developers to obtain certification from an approved association indicating that their products are COPPA-compliant. However, this programme implemented to encourage the development of

best practices is rarely used. As the research by Reyes and colleagues (2018) reveals, it is difficult to identify companies that have obtained the Safe Harbor certification, even on the accrediting bodies' websites. Furthermore, the authors point out in their research that the practices of Safe Harbor accredited apps are neither more secure nor COPPA-compliant. Indeed, Reyes and colleagues discovered that some of these programmes communicate players' permanent IDs through insecure networks and employ third parties whose usage is specifically prohibited in goods aimed at minors (Reyes et al., 2018). Therefore, it is apparent that the self-regulatory instruments and their enforcement by the legislative body are merely accessories and contribute very little to protecting children's data.

Although the United Nations Human Rights Office recognises digital privacy as a human right, and numerous nations have enacted legislation to that effect, individuals are still inadequately protected (Human Rights Watch, 2018; OHCHR, 2019). Accordingly, the present regulations are unsuited to the economic ecosystem that has evolved around the data processing sector. While the American legislation focuses more on the permitted commercial uses of personal data, the European GDPR provides thorough guidelines and sanctions to protect its citizens' digital privacy. The legislation shortcomings become even more apparent when considering the globalised nature of mobile games. Accordingly, regulatory agencies may find it challenging to implement sanctions on non-compliant entities due to the blurring of boundaries between developers' countries of origin, the geographical location of their data servers, and the user's location. Whether in North America or Europe, the current legislative landscape is far from sufficient to ensure citizens' digital privacy, especially for minors. This is particularly alarming as the data and predictive analytics industry has experienced significant growth in recent years.

Social discourses, surveillance, and mobile games – “I have nothing to hide”

Despite the privacy concerns about the mobile gaming industry, few voices have been raised against this surveillance ludocapitalism system. The omnipresence of digital technologies in the contemporary Western world makes these economic models acceptable due to the invisibility of these technical devices. For example, mobile phone penetration rates in Europe are 70 per cent, but in the Nordic countries, the rate rises to 92 per cent on average (Statistica, 2021), demonstrating the technology's pervasiveness in this region. The concept of habituation is helpful in understanding how technological devices slowly become invisible as they spread and become entangled with everyday life. Fickers and van der Oever (2020: 71) defined habituation as the “dissipation of a target-psychological response, e.g. psychophysiological activation at the presentation of a novel stimulus due to repeated exposure

only”. Over time, what shocks or seems strange at first sight gradually ceases to have this effect and becomes a regular part of life without needing much attention. The habituation of users makes these digital technologies invisible, familiar, and standardised.

Habituation coupled with the acceleration of technological innovations, societal changes, and the ever-accelerating rhythm of life (Rosa, 2010) facilitates rapid ways of thinking. Rosa (2010) demonstrated, through his “social critique of time”, that the frantic pace of our lives encourages us to crave smaller but more short-term and guaranteed gratifications: We believe that the growing practice of mobile gaming could be understood in this accelerated context of rewards and conditioned behaviour. Mobility enables this fluid and practically omnipresent activity, monetising every bit of “spare time” with regular tiny gratifications.

The collection of personal data is similar in many platforms and mobile games. As the relative importance of social media platforms such as Facebook, TikTok, and YouTube grow, surveillance becomes part of everyday life (Trottier, 2016). Therefore, when mobile games start to collect personal data and sell them to third parties, individuals will not necessarily pay attention to it (and the game’s condition of use) – it already happens on every other platform, every day, and everywhere. This habituation, initially considered at the psychological level, thus becomes social when it becomes part of the discourse that trivialises and normalises the use of these technologies and traceability. The ubiquitous use of the Internet in our everyday lives has made data collection a seemingly unavoidable norm.

As we have shown elsewhere (Bonenfant et al., 2018, 2019; Crémier et al., 2019), current discourses regarding the production and circulation of data present it as a natural fact about computers and digital technologies rather than rational decisions. Geological metaphors such as “raw data”, “data mining”, “new gold”, and so on, contribute to the social depiction of data as a natural resource waiting to be used (Gitelman, 2013; Puschmann & Burgess, 2014; van Dijck, 2014). As a socially depicted natural “resource” or “force”, the economical use of personal data is easy to justify in a neoliberal society. Those with financial interests ensure minimal opposition, and citizens do not appear to have much authority to confront this operating method. These metaphors hide that data production is always intentional: Mobile game developers and third parties write specific lines of code to create data each time a condition is met (e.g., each click, each ad view, etc.). Therefore, discourses concerning personal data surveillance plays a crucial role in their social acceptability.

Moreover, some tech executives, such as Google’s former CEO, Eric Schmidt, value citizens’ transparency by equating honesty with disclosing the totality of one’s private life (Jennings, 2009). In their book *Transparent Lives*, Bennett and colleagues (2014) pointed out, among other trends, a

“security culture”, a “growing ambiguity of personal information”, and a “global surveillance market”. The well-known phrase “nothing to hide” becomes a social injunction that benefits a minority of personal data operators who profit from the general public’s incomprehension of genuine privacy issues posed by these technologies (Andrejevic, 2007).

While the common perception of data as a natural resource and its injunction on transparency are critical to social acceptance, free-to-play mobile games, for their part, allow for the development of surveillance structures. Indeed, the ludic nature of mobile apps is often used to justify dubious ethical practices, such as collecting data not directly related to the game (e.g., GPS localisation without a specific game mechanic). Data collection looks innocuous when it is “just for fun” or “to maximise in-game pleasure”, but game developers – and more importantly, their third parties – regularly neglect to disclose that the data’s primary purpose is to be sold. Thus, mobile games’ social discourse legitimises data collection and promotes the widespread acceptance of surveillance capitalism. The Foucauldian approach to power, discourse, and dispositif can help us better understand this socioeconomic system’s conditions and possibilities.

A Foucauldian approach – “Here is my data, help yourself”

Michel Foucault’s work centres on a critical examination of contemporary forms of power. Moving away from the substantialist approach, Foucault (1978) argued that power is understood as inequality within the various relationships we engage in throughout our daily life, creating a dominant and a dominated group. Accordingly, power is exercised on the individual level and not just by society’s various institutions; thus, power has no defined subject, is dispersed, and can be challenging to identify. According to Foucault (1976), these inequities are enabled through the various discourses formulated by individuals belonging to the dominant status: Discourse acts as a device and a space within which power relations can be confronted.

Accordingly, the dominant group’s discourse aims to reproduce and perpetuate the power structure in place using a variety of elements such as “gestures, attitudes, ways of being, behavioural patterns or spatial configurations” (Foucault, 1976: 123). Thus, discourses allow dominant groups to assert their position through multiple ways of being and doing that are not limited to language. However, one should not confuse discourse as the source of power relations; it rather constitutes a mechanism that allows them to be actualised. For example, personal data operators trivialise ludocapitalist surveillance by using specific expressions or overemphasising its transparency, consequently ensuring their position of power over the ordinary citizens who play free-to-play mobile games that they consider “inoffensive”.

If discourse and power are inextricably linked, Foucault will then argue

that these elements are actualised within what he calls a *dispositif*. He defines this concept as,

a resolutely heterogeneous whole including speeches, institutions, architectural arrangements, regulatory decisions, laws, administrative measures, scientific statements, philosophical and moral philanthropic proposals; in short, what is said as well as what is not said. [...] Therefore, the *dispositif* is always inscribed in a game of power, but always linked to one or several limits of knowledge that emerge from it, but, just as much, condition it [translated]. (Foucault, 1977: 299)

Accordingly, Foucault understands the *dispositif* as the meeting of multiple components whose objective is to monitor and control individuals inscribed in specific power relations. As a result, the *dispositif* corresponds to the intersection of living and non-living, and said and unsaid, elements, having an incidence on the orientation of the forces at work (Lafleur, 2015). This concept can be understood as a network of elements allowing the power relationship to be exercised.

Surveillance occurring under ludocapitalism is made possible by a *dispositif* comprising the following elements: the current economic system, mobile and trackable technologies, mobile games' persuasive designs, a legislative and self-regulatory framework, our habit of using and carrying mobile phones, social discourse trivialising data collection, our ever-increasing pace of life, and so on. This ludocapitalist surveillance *dispositif* asserts and reiterates the dominant group's position over the dominated, thus impeding their privacy and freedom of thought and action.

Insofar as the dominant groups control the dominated's possible field of action, they benefit from leaving little room for potential resistance against the power structure in place. Hence, the numerous *dispositifs* of our daily lives can be transformed into disciplinary devices. Raffnsøe (2008) subsequently characterised discipline as a dressing tool preventing behaviours before they occur, thus interfering with individuals' everyday activities. It is crucial to emphasise that discipline does not create "ideal-type" subjects; instead, it encourages behaviours driven by the need to accomplish specific actions, dictated by the power relationships governing our everyday lives (Foucault, 1980).

In this sense, the *dispositif* plays a crucial role in disciplining bodies by indicating the encouraged and proscribed behaviours without coercion or physical force. Free-to-play mobile gaming is an excellent illustration of individuals' willingness to frequently engage with and carry tracking devices at all times, even if it means returning home if they forget them. Raffnsøe and colleagues (2014) further described this disciplinarisation in their article, "What is a dispositive? Foucault's historical mappings of the networks of social reality", as follows:

It is an arrangement that makes certain social tendencies or inclinations more likely to occur than others. A given dispositif is itself brought about through several social actions and incidents and is constantly evolving and being displaced. A dispositif articulates a new level of normativity that has evolved through our way of interacting, while simultaneously effecting this interaction. (Raffnsøe et al., 2014: 4)

Ultimately, a dispositif is about disciplining behaviour and social relationships to the point of social control (Deleuze, 1990).

From this perspective, discipline defines the rules of conduct that ensure order and the maintenance of the power relationship by preventing dissenting behaviours. In this ludocapitalist surveillance dispositif, the subjects of the surveillance are not even aware of being watched anymore. More precisely, they have internalised the surveillance system to the point of participating in this contemporary panopticism: Those observed abide by the rules without knowing whether or not the supervisor is there (Foucault, 1975). Citizens discipline themselves by performing certain acts that reproduce and bring about the surveillance dispositif: They participate and are themselves part of the surveillance system that benefits an economic and political minority (Lyon, 2001, 2006).

We believe that the surveillance dispositif is even more pernicious in mobile gaming since individuals are “typically entertained”, paralysing any opposition to this ludocapitalistic mode of exploitation. By employing persuasive design techniques and deceiving players about their terms of service, free-to-play mobile games increase the effectiveness of their data collection process. Encouraged by incentives and other behavioural conditioning techniques, players discipline themselves and reproduce large-scale surveillance until it becomes socially accepted.

Conclusion

This chapter aimed to provide a comprehensive overview of the interdependence between the mobile game ecosystem and everyday surveillance – and its widespread acceptance by citizens. To define this phenomenon, we have proposed the concept of ludocapitalist surveillance dispositif, based on the notions of ludocapitalism, surveillance capitalism, and dispositif. While some have raised security and ethical concerns associated with surveillance and videogames, our concept represents an effort to distinguish the surveillance occurring within free-to-play mobile games (Kröger et al., 2021; Myrstad & Tjøstheim, 2021; Reyes et al., 2018). We have demonstrated how players’ everyday behaviours reproduce the surveillance ludocapitalist dispositif through the economic, technical, psychological, semiotic, legal, and social dimensions of mobile gaming. Accordingly, what appears to be a commonplace practice is embedded in an economic model based on the commodification

of personal data and the distribution of targeted advertising. We have emphasised how persuasive design strategies further reinforce this economic model through mobile games developed to condition players to stay connected as much as possible, even if it makes them addicted. Despite its legitimacy, the industry-regulated framework is frequently misleading and difficult for citizens to understand. Laws are piecemeal, even those for protecting children, and inadequate concerning technological and economic transformations.

We have argued that collective habituation leads to a normalisation of mobile technologies and traceability, to the point of trivialising surveillance. Commercial data collection discourse that values citizen transparency neutralises any contestation or adoption of alternative technologies. Finally, we have postulated that the present context of social acceleration, frequent gratification, and the promotion of playfulness associated with connotations of innocuity also contribute to its normalisation.

The contributions of this research rest on the comprehensive portrait we have presented of the various actors involved in free-to-play mobile game surveillance. This particularity is even more critical considering the complexity and opacity surrounding the forces involved in this ecosystem. Furthermore, we contend that combining concepts unique to game studies and surveillance studies allowed us to go beyond the technical aspects of surveillance and analyse the predominant persuasive design strategies of free-to-play games.

From this perspective, we have defended the idea that mobile games contribute to this ludocapitalist surveillance dispositif by disciplining citizens as data producers and consumers of advertising – they enable this form of capitalism by diverting people’s attention. From a semantic point of view, to divert is to turn away, deter, and distract, which is the act of distracting someone from their concerns. Similar to how many academics considered mass entertainment as ideological indoctrination (Horkheimer & Adorno, 1947; Marcuse, 1964), free-to-play mobile games has become a way to conceal large-scale data collection that benefits a minority at the expense of individuals’ privacy. Used in this manner, playing seemingly harmless mobile games facilitates surveillance capitalism.

However, play as a practice has always had a socially beneficial role, as it is associated with freedom (Huizinga, 1938), creation (Fink, 1966), and the building of social relationships (Caillois, 1958). But in this ludocapitalist surveillance dispositif, mobile games become a means to discipline and control individuals. As we saw in the 2016 American elections (Jamieson, 2018), the risks of political manipulation are real: If targeted and personalised marketing can successfully sell products, it can equally sell ideas. The more precise advertising profiling becomes through massive data collection, the more influential political marketing campaigns will be, leaving individuals at risk of being directly manipulated by political groups. While the Nordic countries are among the world leaders in mobile game development, with companies

such as King (Sweden), Supercell (Finland), and Rovio (Finland), it seems imperative that the actors of this industry question their practices and their implications in the erosion of our digital privacy. Consequently, all citizens are affected by these issues, whether they are gamers or not.

Acknowledgements

This research was conducted within the “Canada Research Chair on Big Data and Gaming Communities” and was funded by the Canadian Social Sciences and Humanities Research Council (SSHRC).

References

- Alha, K. (2020). *The rise of free-to-play: How the revenue model changed games and playing* [Doctoral thesis, Tampere University]. <http://urn.fi/URN:ISBN:978-952-03-1774-4>
- Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. University Press of Kansas.
- Appfigures. (2022). *Most popular SDKs in apps and games*. <https://appfigures.com/top-sdks/all/all>
- Balakrishnan, J., & Griffiths, M. D. (2018). Loyalty towards online games, gaming addiction, and purchase intention towards online mobile in-game features. *Computers in Human Behavior*, 87, 238–246. <https://doi.org/10.1016/j.chb.2018.06.002>
- Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (Eds.). (2014). *Transparent lives: Surveillance in Canada*. Athabasca University Press. <https://www.doi.org/10.15215/aupress/9781927356777.01>
- Bonenfant, M. (2021). Hypermodern video games as emblems of empire or how the gaming multitude adapts to hypermodernity. *Games and Culture*, 16(3), 357–370. <https://doi.org/10.1177/1555412020961849>
- Bonenfant, M., Crémier, L., & Lafrance St-Martin, L. I. (2018). Réflexions sémiotiques sur le circuit des données massives [Semiotic reflections on the big data circuit]. In A. Mondoux, & M. Ménard (Eds.), *Big data et société: Industrialisation des médiations symboliques* [Big data and society: Industrialisation of symbolic mediations]. Presses de l'Université du Québec.
- Bonenfant, M., Lafrance St-Martin, L. I., & Crémier, L. (2019). Affected data: Understanding knowledge production in algorithmic events. *Global Media Journal*, 11(2), 66–78. <https://www.proquest.com/scholarly-journals/affected-data-understanding-knowledge-production/docview/2434436008/se-2>
- Brückner, S., Sato, Y., Kurabayashi, S., & Waragai, I. (2017). The handling of personal information in mobile games. *International Conference on Advances in Computer Entertainment*, 415–429. https://doi.org/10.1007/978-3-319-76270-8_29
- Cailliois, R. (1958). *Les jeux et les hommes* [Games and people]. Gallimard.
- Christl, W. (2017). *Corporate surveillance in everyday life: How companies collect, combine, analyze, trade, and use personal data on Billions*. Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
- Christl, W., & Spiekermann, S. (2016). *Networks of control: A report on corporate surveillance, digital tracking, big data & privacy*. Facultas. https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf
- Citton, Y. (2014). *L'économie de l'attention: Nouvel horizon du capitalisme?* [The attention economy: New horizon of capitalism?]. La Découverte. <https://doi.org/10.3917/dec.citto.2014.01>
- CMS. (2022). *GDPR Enforcement Tracker*. <https://www.enforcementtracker.com>
- Crémier, L., Bonenfant, M., & L. I. Lafrance Saint-Martin (2019). Raw data or hypersymbols? Modelizing sign function in big data meaning-making processes, *Semiotica*, (230), 189–212. <https://doi.org/10.1515/sem-2018-0110>
- Dark Pattern Games. (n.d.). *Helping you find healthy mobile games*. Retrieved January 28, 2022, from <https://www.darkpattern.games/>
- Deleuze, G. (1990). Post-scriptum sur les sociétés de contrôle [Postscript on societies of control]. *L'autre Journal*, 1.
- Deloitte. (2019). *Smartphone: The center of life: A study on Nordic mobile consumer behaviour*. Deloitte Global Mobile Consumer. <https://www2.deloitte.com/content/dam/Deloitte/se/Documents/technology-media-telecommunications/Global-Mobile-Consumer-Survey-2019-Nordic-Cut.pdf>
- Dibbell, J. (2007, June 17). The life of the Chinese gold farmer. *The New York Times*. <https://www.nytimes.com/2007/06/17/magazine/17lootfarmers-t.html>
- ESRB. (n.d.). *Ratings guides, categories, content descriptors*. ESRB Ratings. Retrieved February 14, 2022, from <https://www.esrb.org/ratings-guide/>

- Falzon, J. (2019, December 18). *Does an E or E10+ rating mean a game or app is “directed to children” for purposes of COPPA?* ESRB Ratings. <https://www.esrb.org/privacy-certified-blog/does-an-e-or-e10-rating-mean-a-game-or-app-is-directed-to-children-for-purposes-of-coppa/>
- Fickers, A., & van der Oever, A. (2020). (De)habitation histories: How to re-sensitize media historians. In N. Hall, & J. Ellis (Eds.), *Hands on media history: A new methodology in the humanities and social sciences* (pp. 58–75). Routledge. <https://doi.org/10.4324/9781351247412>
- Fink, E. (1966). *Le jeu comme symbole du monde* [*The game as a symbol of the world*] (H. Hildenbrand & A. Lindenberg, Trans.). Éditions de Minuit.
- Fogg, B. J. (2002). Persuasive technology: Using computers to change what we think and do. *Ubiquity* (December), Article 5. <https://doi.org/10.1145/764008.763957>
- Foucault, M. (1975). *Surveiller et punir* [Surveil and punish]. Gallimard.
- Foucault, M. (1976). Le discours ne doit pas être pris comme... [Speech should not be taken as...]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et écrits: 1976–1979* [*Said and written: 1976–1979*] (pp. 123–124). Gallimard.
- Foucault, M. (1977). Le jeu de Michel Foucault [The game of Michel Foucault]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et écrits III 1976-1979* [*Said and written: 1976–1979*] (pp. 298–329). Gallimard.
- Foucault, M. (1978). Dialogue sur le pouvoir [Dialogue about power]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et écrits: 1976-1979* [*Said and written: 1976–1979*] (pp. 464–476). Gallimard.
- Foucault, M. (1980). Table ronde du 20 mai 1978 [Round table of 20 May 1978]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et Écrits IV* [*Said and written: 1976–1979*]. Gallimard.
- FTC. (2012, December 18). *FTC to study data broker industry’s collection and use of consumer data*. Federal Trade Commission. <https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data>
- FTC. (2020). *Complying with COPPA: Frequently asked questions*. Federal Trade Commission. <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>
- GDPR. (2018, November 14). *Art. 83 GDPR – General conditions for imposing administrative fines*. GDPR.Eu. <https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/>
- GDPR.EU. (2018). *Art. 8: GDPR conditions applicable to child’s consent in relation to information society services*. <https://gdpr.eu/article-8-childs-consent/>
- Ghosh, D. (2020, July 17). Don’t give up on your digital privacy yet. *Slate*. <https://slate.com/technology/2020/07/data-privacy-surveillance-law-marketers.html>
- Gitelman, L. (2013). *Raw data is an oxymoron*. MIT Press. <https://doi.org/10.7551/mitpress/9302.001.0001>
- Hodent, C. (2020). *The psychology of video games*. Routledge. <https://doi.org/10.4324/9781003045670>
- Horkheimer, M., & Adorno, T. W. (1947). *Dialektik der Aufklärung* [*Dialectic of enlightenment*]. Querido Verlag.
- Huizinga, J. (1938). *Homo Ludens: Essai sur la fonction sociale du jeu* [*Homo Ludens: An Essay on the Social Function of Play*]. Gallimard.
- Human Rights Watch. (2018, April 19). Data privacy is a human right. *Human Rights Watch*. <https://www.hrw.org/news/2018/04/19/data-privacy-human-right>
- IARC. (n.d.). *How the international age rating coalition works* | IARC. Retrieved February 14, 2022, from <https://www.globalratings.com/how-iarc-works.aspx>
- Jamieson, K. H. (2018). *Cyberwar: How Russian hackers and trolls helped elect a president: What we don’t, can’t, and do know*. Oxford University Press.
- Jennings, J. (2009, December 11). Google CEO: *If you want privacy, do you have something to hide?* Computerworld. <https://www.computerworld.com/article/2468308/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html>
- Jonathan. (2016, June 2). *Slimming down: Fighting SDK fatigue and bloat*. AdColony. <https://www.adcolony.com/blog/2016/06/02/fighting-sdk-fatigue/>

- Jordan, W. G. (2014). *Ludocapital: The political economy of digital play* [UC Irvine]. <https://escholarship.org/uc/item/0985k4rw>
- Kröger, J. L., Raschke, P., Campbell, J. P., & Ullrich, S. (2021, July 6). Surveilling the gamers: Privacy impacts of the video game industry. SSRN. <https://doi.org/10.2139/ssrn.3881279>
- Laflleur, S. (2015). Foucault, la communication et les dispositifs [Foucault, communication and devices]. *Communication. Information Médias Théories Pratiques*, 33(2). <https://doi.org/10.4000/communication.5727>
- Lee, J. H., Jett, J., & Perti, A. (2015). The problem of “additional content” in video games. *Proceedings of the 15th ACM/IEEE-CS Joint Conference on Digital Libraries*, 237–240. <https://doi.org/10.1145/2756406.2756949>
- Legner, L., Eghtebas, C., & Klinker, G. (2019). Persuasive mobile game mechanics for user retention. *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 493–500. <https://doi.org/10.1145/3341215.3356261>
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education.
- Lyon, D. (2006). *Theorizing surveillance: The panopticon and beyond*. William Publishing.
- Macenaite, M., & Kosta, E. (2017). Consent for processing children’s personal data in the EU: Following in US footsteps? *Information & Communications Technology Law*, 26(2), 146–197. <https://doi.org/10.1080/13600834.2017.1321096>
- Marcuse, H. (1964). *One-dimensional man*. Beacon Press.
- McKean, R., Kuroska-Tober, E., & Waem, H. (2022). *GDPR fines and data breach survey: January 2022*. DLA Piper. <https://www.dlapiper.com/en/austria/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/>
- Merton, R. K. (1948). The self-fulfilling prophecy. *The Antioch Review*, 8(2), 193–210. <https://doi.org/10.2307/4609267>
- Myrstad, E., & Tjøstheim, I. (2021). *Out of control: How consumers are exploited by the on-line advertising industry*. <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>
- Newzoo. (2021). *Newzoo global games market report*. <https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2021-free-version/>
- Nieborg, D. B. (2016a). Free-to-play games and app advertising: The rise of the player commodity. In J. F. Hamilton, R. Bodle, & E. Korin (Eds.), *Explorations in critical studies of advertising* (pp. 38–51). Routledge. <https://doi.org/10.4324/9781315625768>
- Nieborg, D. B. (2016b). From premium to freemium: The political economy of the app. In T. Leaver, & M. Willson (Eds.), *Social, casual and mobile games: The changing gaming landscape* (pp. 225–240). <https://doi.org/10.5040/9781501310591.ch-016>
- OHCHR. (2019). *OHCHR and privacy in the digital age*. UN High Commissioner for Human Rights. <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>
- Okoyomon, E., Samarin, N., Wijesekera, P., Elazari Bar On, A., Vallina-Rodriguez, N., Reyes, I., Feal, Á., & Egelman, S. (2019). On the ridiculousness of notice and consent: Contradictions in app privacy policies. *Workshop on Technology and Consumer Protection (ConPro 2019), in Conjunction with the 39th IEEE Symposium on Security and Privacy*. <https://www.ieee-security.org/TC/SPW2019/ConPro/papers/okoyomon-conpro19.pdf>
- PEGI. (n.d.). *PEGI age ratings*. Retrieved February 14, 2022, from <https://pegi.info/page/pegi-age-ratings>
- PIPEDA. (2019). *Testimony of PIPEDA*. <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/>
- PRIVO. (n.d.). *History of COPPA violations*. Retrieved February 14, 2022, from <http://www.privo.com/history-of-coppa-violations>
- Puschmann, C., & Burgess, J. (2014). Metaphors of big data. *International Journal of Communication*, 8, 1690–1709. <https://ijoc.org/index.php/ijoc/article/view/2169/1162>
- Raffnsøe, S. (2008). Qu’est-ce qu’un dispositif? L’analytique sociale de Michel Foucault [What is a dispositive? The social analytics of Michel Foucault]. *Symposium*, 12(1), 44–66. <https://doi.org/10.5840/symposium20081214>

- Raffnsøe, S., Gudmand-Høyer, M. T., & Thaning, M. S. (2014). *What is a dispositive? Foucault's historical mappings of the networks of social reality* [Working paper, Copenhagen Business School, Denmark]. <https://hdl.handle.net/10398/9077>
- Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., & Egelman, S. (2019). 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. *28th USENIX Security Symposium (USENIX Security 19)*, 603–620. <https://www.usenix.org/system/files/sec19-reardon.pdf>
- Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018). "Won't somebody think of the children?" Examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies*, 2018(3), 63–83. <https://doi.org/10.1515/popets-2018-0021>
- Rieke, A., Yu, H., Robinson, D., & von Hoboken, J. (2014). *Data brokers: A look at the Canadian and American landscape*. https://www.priv.gc.ca/media/1778/db_201409_e.pdf
- Rieke, A., Yu, H., Robinson, D., & von Hoboken, J. (2016). *Data brokers in an open society*. Open Society Foundations. <https://www.opensocietyfoundations.org/publications/data-brokers-open-society>
- Ringel, G. (2021). *Council post: Rethinking privacy: The road to data ownership*. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2021/08/02/rethinking-privacy-the-road-to-data-ownership/>
- Rosa, H. (Ed.). (2010). *High-speed society: Social acceleration, power, and modernity*. Penn State Press.
- Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.
- Stahl, A. (2021). *What you need to know to protect your data online*. Forbes. <https://www.forbes.com/sites/ashleystahl/2021/06/04/what-you-need-to-know-to-protect-your-data-online/>
- Statista. (2021). *Mobile devices in the Nordics*. <https://www.statista.com/study/38811/mobile-device-usage-in-the-nordics-statista-dossier/>
- Terrien, D. (2021, June 15). *L'avenir de la réforme des lois sur la protection des renseignements personnels au Canada* [The future of privacy law reform in Canada]. https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2021/sp-d_20210526/
- Thirani, V., & Gupta, A. (2017). *The value of data*. World Economic Forum. <https://www.weforum.org/agenda/2017/09/the-value-of-data/>
- Trottier, D. (2016). *Social media as surveillance: Rethinking visibility in a converging world*. Routledge. <https://doi.org/10.4324/9781315609508>
- Unity. (2020). *Privacy policy hub*. <https://unity3d.com/legal/privacy-policy>
- Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. *The New York Times*. <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>
- van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- Waldman, A. E. (2018). Privacy, notice, and design. *Stanford Technology Law Review*, 21(1), 74–127.
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, 31, 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- Wamsley, L. (2020, October 13). *Your technology is tracking you: Take these steps for better online privacy*. NPR. <https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy>
- Whitson, J. R. (2013). Gaming the quantified self. *Surveillance & Society*, 11(1/2), 163–176. <https://doi.org/10.24908/ss.v11i1/2.4454>
- Whitson, J. R. (2019). The new spirit of capitalism in the game industry. *Television & New Media*, 20(8), 789–801. <https://doi.org/10.1177/1527476419851086>

- Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., & Beznosov, K. (2017). The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. *2017 IEEE Symposium on Security and Privacy (SP)*, 1077–1093. <https://doi.org/10.1109/SP.2017.51>
- Winder, D. (2019, December 31). Get yourself cybersecure for 2020. *The Guardian*. <https://www.theguardian.com/technology/2019/dec/31/get-cybersecure-for-2020-cybersecurity-passwords-smartphone>
- Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>
- Zuboff, S. (2018). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.