DANGEROUS GAME

Protecting the Privacy of Children Under 13 in Mobile Games

Results from Research Funded by the Office of the Privacy Commissioner of Canada (2024-2025)

UQÀM | Université du Québec à Montréal

McGill UNIVERSITY

uOttawa

CRC JEU TECHNOLOGIES SOCIÉTÉ

RESEARCH FACULTY TEAM

Maude Bonenfant, PhD. Full Professor, Université du Québec à Montréal
Thomas Burelli, PhD. Associate Professor, Université d'Ottawa
Sara Grimes, PhD. Full Professor, McGill University
Hafedh Mili, PhD. Full Professor, Université du Québec à Montréal
Jean Privat, PhD. Full Professor, Université du Québec à Montréal

STUDENT RESEARCH TEAM

Coordinator: Alexandra Dumont, PhD Candidate, Université du Québec à Montréal

Hazem Allouche, Master Student in Informatics, Faculté des sciences, UQAM

Nabil Bennani, Master Student in Informatics, Faculté des sciences, UQAM

Amanda Buttice, PhD Candidate in Legal Studies, Faculté de droit, uOttawa

Gabriel Cadieux, PhD Candidate in Legal Studies, Faculté de droit, uOttawa

Cédric Duchaineau, Master Student in Communication, Faculté de communication, UQAM

Pierre Gabriel Dumoulin, PhD candidate in Semiotic Studies, Faculté des arts, UQAM

Simon Fraser, Master Student in Communication, Faculté de communication, UQAM

Tom Humeau, PhD Candidate in Communication, Faculté de communication, UQAM

Irina Joseph, PhD Candidate in Sociology, Faculté des sciences humaines, UQAM

Iulian Madalin Lupu, Master Student in Informatics, Faculté des sciences, UQAM

Emmanuel Merlot, Master Student in Informatics, Faculté des sciences, UQAM

Hugo Veillé, PhD Candidate in Studies and Practices of the Arts, Faculté des arts, UQAM

GRAPHICS

Elisa Vial, PhD candidate, Université du Québec à Montréal
Hugo Engel, PhD candidate, Université du Québec à Montréal

ILLUSTRATION

Marcia Diaz
Portofolio : https://marciadiaz.myportfolio.com

Julien Toulze
Website : http://julien.tools

This project received financial support through the Office of the Privacy Commissioner of Canada's Contributions Program. The opinions expressed in this summary and report are those of the authors and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada.

Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

This project was carried out as part of the work of the Canada Research Chair (CRC) in Games, Technologies and Society. crc-jeu.uqam.ca

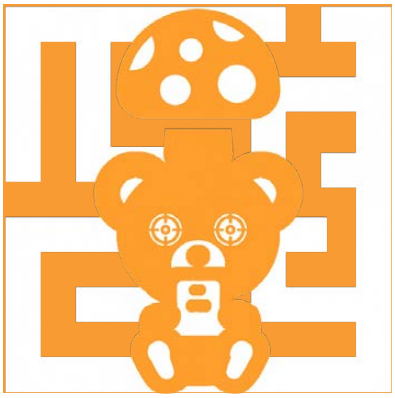
TABLE OF CONTENTS

SUMMARY

The business models that support the mobile games industry, including those for children, are primarily based on the collection and sale of personal data, display advertising, and microtransactions. An entire techno-economic infrastructure makes this system possible, and it is often highly opaque. There are many game development studios and third-party companies profiting from this lucrative market, and the means available to parents to provide informed consent are inadequate.

For this research project, the team, consisting of five professors in game studies, communication, law, and computer science, combined their multidisciplinary expertise around the following question: is the privacy protection of children under the age of 13 years guaranteed in the terms of use and privacy policies of the mobile games that are targeted to them?

The results presented here highlight the fact that no policy fully complies with Quebec, Canadian, and United States children's privacy laws. Various issues were identified, some of which demonstrate a malicious intent to override children's rights in order to collect personal data through the game application. Additionally, parents lack the tools and knowledge necessary to make an informed choice to protect their children. Furthermore, the information provided can confuse or even deceive parents by giving them false assurances that their children's privacy is protected. A gap thus exists between the need to protect children from the commercial exploitation of their personal data and the regulation of the mobile gaming industry. This report aims to alert political authorities, the general public, and the industry itself.



CHILDREN'S VIDEO GAMES

In 2022, 53% of Canadians claimed they played video games, and 71% of parents played video games with their children at least once a week. According to the industry lobby Entertainment Software Association of Canada (ESAC), young people aged 6 to 17 spend an average of 7.9 hours per week playing video games (ESAC, 2022).

It is also estimated that 39% of children aged 6 to 17 play video games via mobile platforms (Ibid.).

Concurrently, 39% of Canadian children aged 2 to 6 use a smartphone, and 50% of 7 to 11-year-olds own a mobile device. This figure rises to 87% among 12 to 17-year-olds who have their own smartphone (Statista, 2022). Mobile gaming is therefore common among young people, many of whom own their own device.

Alongside this normalization of mobile phone or tablet usage and video games among children, the mobile gaming industry has been experiencing exponential growth for several years. In 2024, mobile games constituted 55% of the entire video game market, a market notably dominated by Chinese giant Tencent (Buijsman, 2025). Having become the most lucrative sector of the video game industry with 87.89 billion downloads worldwide (Data.ai., 2024), more and more development studios are investing in mobile gaming compared to computer or console games. Major companies associated with the development of Triple A games (requiring significant financial investment) are now turning to mobile gaming (i.e. EA, Ubisoft).

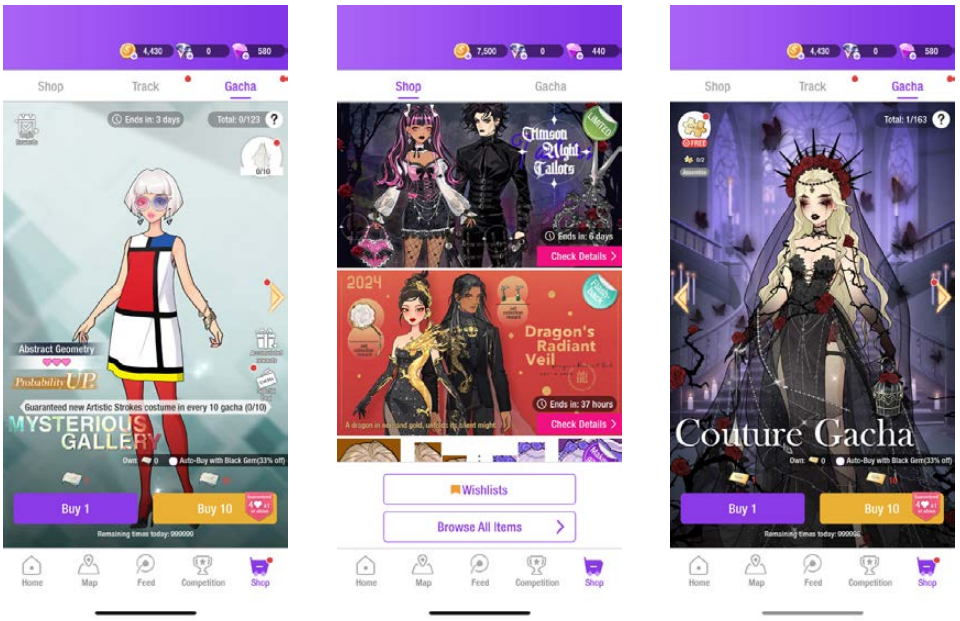
In the mobile games industry, the industry's standardized business model relies on microtransactions, display advertising, and the collection of personal data (Nieborg, 2016; Oehlenschlager, 2021), necessitating extended connection times. To ensure better performance, studios use various persuasive design techniques to keep the individual connected for as long as possible — including young children — and to increase the number of playing sessions as much as possible (Fogg, 2002; Zagal et al., 2013; Legner et al., 2019; Alha, 2020; Mathur et al., 2021).

Example of a persuasive design strategy to keep children playing daily

In the Pokémon Café ReMix game *(Everyone/4+), the child is encouraged to develop a daily gaming habit by receiving a "free" gift every day; on the third day of login, the popular character Pikachu is offered.*

This type of persuasive design aims to modify the child's behavior by rewarding them, sometimes excessively, and by exploiting their cognitive biases (loss aversion, "near-miss," etc.) in a similar way to games of chance and money (King et al., 2010; Drummond and Sauer, 2018; James et al., 2022; OECD, 2022; van der Hof et al., 2022).

Example of persuasive design leveraging the cognitive bias of loss aversion



In the game SuitU: Fashion Avatar Dress Up *(Everyone 10+/12+, the child is encouraged to participate in a simulated game of chance (gacha) to obtain the best clothes in the game to dress up their characters. These offers are time-limited, encouraging immediate purchase of tickets to increase the chances of obtaining desired rewards.*

In a context where the goal of design is to keep children connected for as long as possible, personal data is collected for various reasons. While information collection is necessary to ensure the proper functioning of the application, other data is collected to track game usage habits (game analytics), to establish general portraits of in-game consumption practices (business analytics), and also to share and sell data to third parties in order to create profiles for displaying targeted advertising and microtransaction offers (Bonenfant et al., 2023).

Persuasive design features, which can be highly effective when used on children, are numerous in this type of video game and are part of a techno-economic ecosystem that puts the rights of this young audience at risk (Bonenfant et al., 2023).

[1] Link to the research: https://crc-jeu.uqam.ca/wp-content/uploads/sites/90/2024/06/Rapport-jeux-mobiles-enfants.pdf

INDUSTRY SELF-REGULATION IN THE CONTEXT OF GAME CLASSIFICATION SYSTEMS

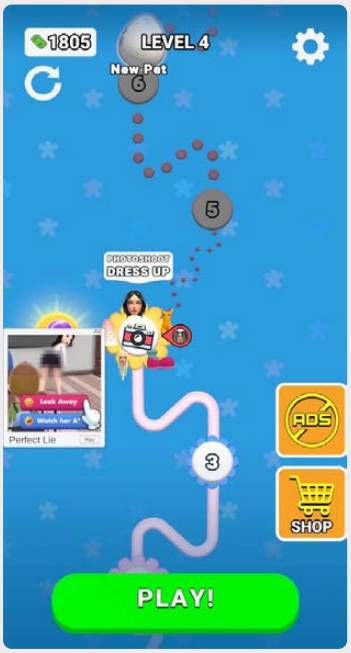
One of the central problems of this gap in child protection is the industry's self-regulation in defining and determining how games are classified.

The North American video game industry has always been the subject of numerous attempts at regulation, with little success. Among the bills and civil lawsuits that have been presented, efforts have been made to limit graphic violence in video games, to regulate suggestive content, and to prohibit the sale of certain games to minors. However, these efforts remain limited.

The US video game industry has managed to avoid the imposition of legislation regulating its activities by invoking the First Amendment of the United States Constitution, which guarantees freedom of expression, but more specifically by implementing self-regulatory measures overseen by various stakeholders in the industry.

The voluntary company classification system is one example, but the lack of expert and external assessment leads to many problems.

Example of a problem of classification of games based on self-regulation: the lack of consistency between the ratings of the same game distributed on different platforms



The game Build a Queen *is rated "Everyone" but on the App Store, it is rated 12+. Apple cites in particular the frequent presence of violent and sexual content and simulated gambling, while the first organization does not take this into account.*

In Canada, no independent organization classifies video games.

1.1 Classification of Children's Video Games

Unlike cinematic productions, video game classification is not done independently, and many inconsistencies and gaps are observed. Not to mention that several rating systems coexist within the same territory.

In North America, the ESRB (Entertainment Software Rating Board) is responsible for the general classification of video games. This organization, created in 1994, is a direct offshoot of the Entertainment Software Association, a video game industry lobby group.

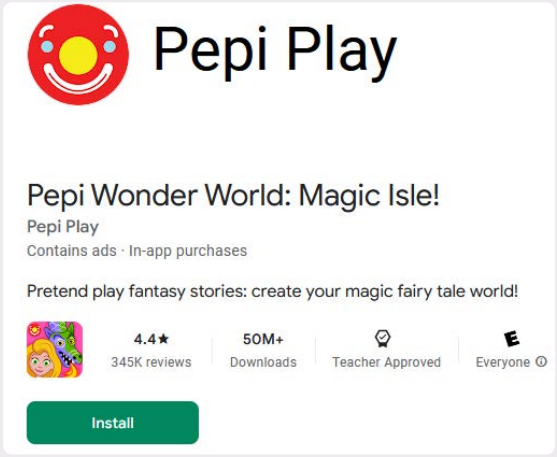
The content, rating process, and application of the ESRB rating system are based on the will of the video game industry and development studios. Its compliance and enforcement are not regulated by any law in the United States. In Canada, five provinces (Saskatchewan, Manitoba, Ontario, New Brunswick, and Nova Scotia) require its use, but given the ESRB's many problems, this classification does not guarantee age appropriateness (Grimes et al., 2023[2]).

The current seven ratings are based exclusively on content (violence, sexuality, language, etc.) and not, for example, on the protection of children's privacy.

Since 2018, information about interactive elements has been added to the ratings summaries, to notify players about the potential presence of online features, such as the presence of microtransactions, social interactions, internet access, or location data sharing. Despite the influence of these features on the experience offered and the potentially significant implications for child players, none of these features impact the actual rating assignment.

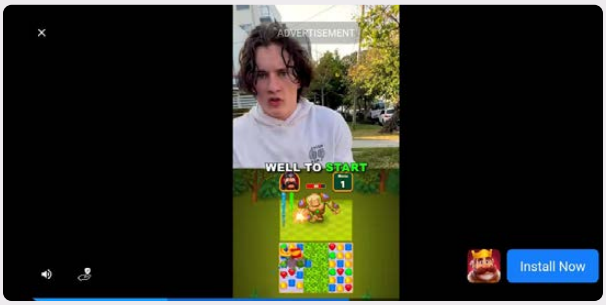
[2] Grimes, S. M., Jayemanne, D., & Giddings, S. (2023). Rethinking Canada's approach to children's digital game regulation. Canadian Journal of Communication, 48(1), 142-162.

Example of a game aimed at children that allows the collection of geolocation data (may collect, may share)



Pepi Wonder World: Magic Isle! *is rated Everyone/4+, but allows for the collection and sharing of geolocation data with third parties.*

1



2

This information can then be used to display targeted advertisements to the child (1) while additional commercial strategies, such as interstitial and rewarded advertisements, are exploited (2).

1.1.1 The Abolition of the "Early Childhood" Rating

The "Early Childhood" (3+) rating was created in 1994 to better protect toddlers and other children under 13. According to the description, games classified in this category contain content likely to be suitable only for children 3 years and older and do not contain any content that parents might consider inappropriate (MediaSmarts, n.d[3].).

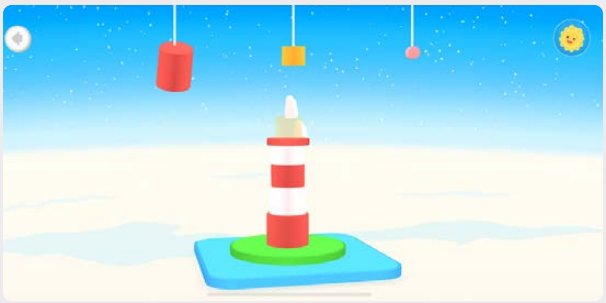
The "Early Childhood" rating was also designed based on the Children's Online Privacy Protection Act (COPPA), the U.S. law protecting children's online privacy. This rating was therefore the most restrictive of the ERSB's ratings.

However, as companies themselves rarely used it, the ESRB eliminated it in 2018[4].

> The most restrictive rating for companies, which protected children's privacy, was abolished by the industry itself.

Children are now generically included in the "Everyone" rating, which does not require that the game is suitable for children, but simply that no content harmful to a young audience is present (violence, sexuality, profanity, etc.) (Göksu et al., 2020; Canadian Centre for Child Protection, 2022).

Example of the problems associated with classification based only on content



Puzzle Shapes Toddlers & Kids (Wonderkind) *encourages children to match shapes, while* RFS - Real Flight Simulator (RORTOS SRL) *is an aviation simulation game. Both have the same rating: "Everyone" on the Google Play Store and "4+" on the App Store. However, even though it does not contain any violent, sexual, or offensive content, RFS is not intended for young children.*

[3] https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_Understanding_Rating_System_0_0.pdf https://www.pbs.org/kcts/videogamerevolution/impact/esrb.html

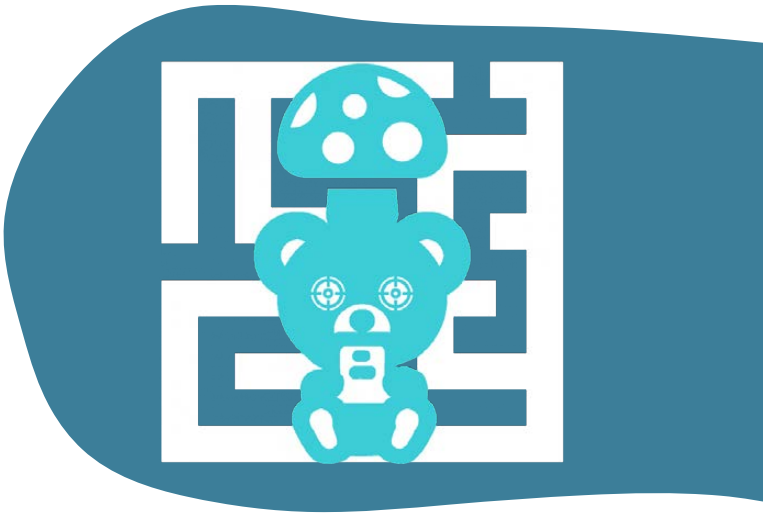
[4] https://web.archive.org/web/20220926012606/https://twitter.com/esrbratings/status/1120695817340321794

Furthermore, the “Everyone” rating, like all classifications defined by the ESRB, does not regulate data collection, and parents cannot trust that their children’s privacy is protected, particularly for children under 13.

This confusion regarding the elements covered in the rating process is compounded by the ESRB’s “children’s privacy” certification (Privacy Certified Kids Seal[5]) offered by the organization.

Studios seeking to obtain a children’s certification for their video games must comply with COPPA’s legal obligations regarding data retention, security, and deletion, as well as parental consent, by providing accurate, clear, and complete information, including information regarding access, review, correction, deletion, and protection of children’s personal information. While this seal could potentially compensate for the now-defunct "Early Childhood" rating in terms of protection, this additional certification to the ESRB rating is optional; its use is based on the voluntary compliance of companies and is in no way binding.

Similarly, the ESRB only offers "guidance" to companies on how to comply with Canadian privacy laws, the General Data Protection Regulation (GDPR) in Europe, and other legislation. The organization does not impose strict standards.



The industry does not impose any mandatory privacy standards for children under 13.

[5] https://www.esrb.org/privacy-certified-seals/#what-are-the-requirements-for-the-epc-kids-seal

1.1.2 Safe Harbor Program

In conjunction with the aforementioned regulating bodies, the Safe Harbor program, an initiative implemented by COPPA and the Federal Trade Commission (FTC), also has the potential to regulate children's privacy protection in games.

This program allows development studios to certify, through a pre-authorized external association, that the games they offer comply with COPPA. Accredited games can then display the seal associated with the organization that awarded their certification.

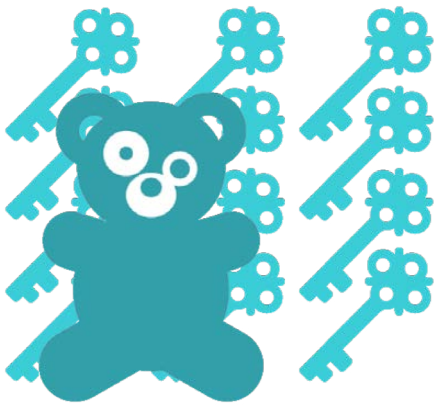
Once again, Safe Harbor remains optional. However, the confirmation of privacy law compliance that it represents should be mandatory for all children's games. Furthermore, certified games are difficult to identify; some are incorrectly or even fraudulently certified, violating COPPA. The Safe Harbor certification framework is also deficient.

In January 2025, amendments were made to COPPA. Some of these specifically address the previously listed shortcomings associated with the Safe Harbor program. These amendments took effect on June 23, 2025, and companies have until April 22, 2026, to comply. The Federal Trade Commission is currently evaluating compliance with the program[6].

[6] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

1.1.3 International Age Rating Coalition

Considering the immense number of games created and published every year, the ESRB and other regulating organizations have established the International Age Rating Coalition (IARC). The IARC aims to semi-automatically classify products distributed solely digitally, such as most video games nowadays. One of the appeals of such a system is its ability to classify a game while considering the regulations in place in the different countries where it is sold[7].



However, similar to the ESRB program, this classification system is limited to evaluating the content presented, without taking into account privacy concerns, designed mechanics, etc.

Furthermore, this classification system relies on statements made by the studios themselves. Although a random verification system exists, no independent entity validates the information submitted by companies, which instantly receive the self-declared classification. Thus, the studio obtains a rating that would be the same as if it had been obtained for a game for which an application had been validated by the ESRB (or another organization, depending on the region of the world): they use the same terminology and symbols (i.e. logos) to represent the rating, while the rules for obtaining them are not the same. This strategy, unfortunately, only further confuses parents when it comes to choosing games which they can confidently deem suitable for their children.

A system based on self-reporting presents many problems for the public.

[7] https://www.globalratings.com/about.aspx
https://cjc.utppublishing.com/doi/pdf/10.3138/cjc.2022-0008
https://royalsocietypublishing.org/doi/full/10.1098/rsos.230270

1.1.4 “Teacher Approved” Mobile Games

To regulate and validate a game’s age rating, Google employs the ESRB system (via the IARC), but also complements it with its own age categories and the "Teacher's Approved" program.

Developed and implemented by Google, the "Teacher's Approved" program aims to support parents in their search for games that are "enriching and entertaining for their children." Games are rated based on the quality and relevance of their content to the target age groups.

For advertising, games must comply with the list of third-party companies previously authorized by Google. Ads must also be distinct from the game environment, easy to ignore, and not interrupt the gaming experience.

However, even in "Teacher's Approved" games, ads and microtransactions are permitted, and certain persuasive mechanics are present. Even imagery specific to gambling is not prohibited.

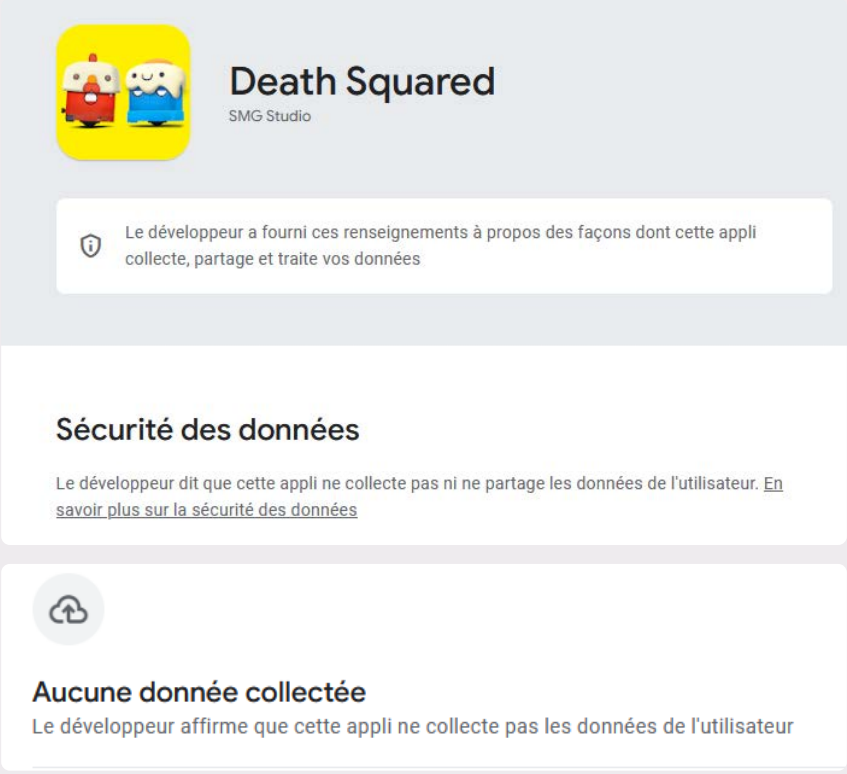
Examples of misclassification of games in the "Teacher Approved" program

Despite the program's restrictions, the game Miraculous Ladybug *(Everyone/ Budge Studios) displays ads for other video games, and the game* Car Wash & Race Games for Kids *(For Everyone/GunjanApps Studios) features certain persuasive mechanics, such as daily game bonuses.*

Generally speaking, "Teacher Approved" games feature fewer persuasive mechanics and fewer ads, but these will be integrated with a greater emphasis on the "experience limited by a paid access lock" mechanic. Furthermore, several of the games are actually ad-supported games branded with a pre-existing franchise.

Under this program, studios must also disclose the data collection they undertake and the personal information they collect. According to Google's terms, personally identifiable information includes: authentication data, microphone and camera sensor data, device data, Android ID, and ad usage data.

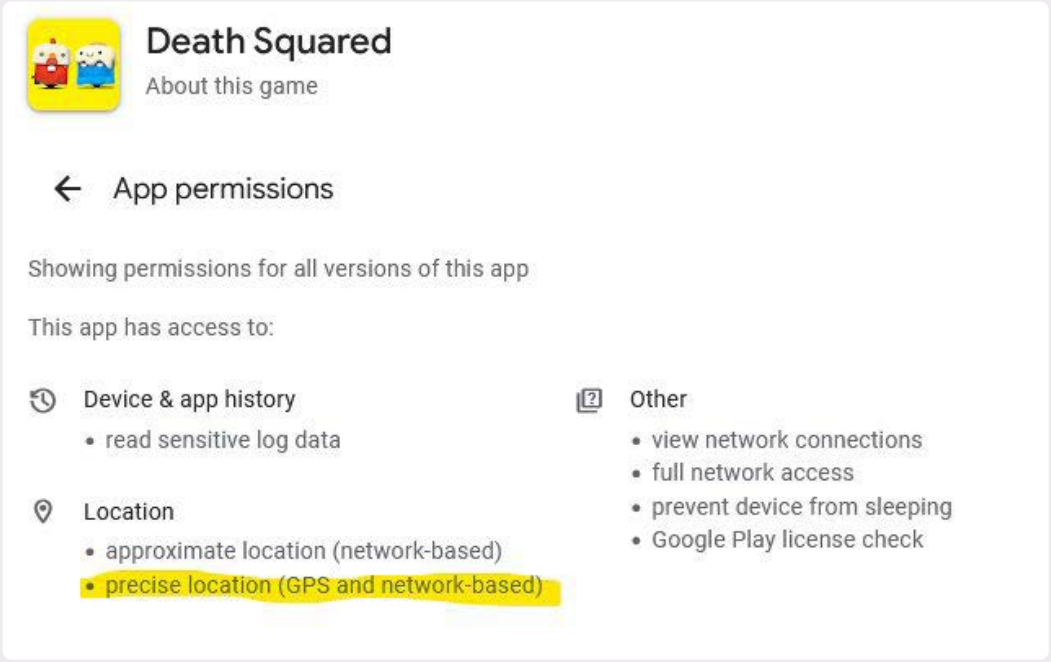
Example of a mismatch between Google's policies and their application on the Google Play Store (*translation below*)



The game Death Squared *(SMG Studio) declares that it does not collect or share any data.*

Top: "The developper has provided this information about how this app collects, shares and handles your data"
Middle: "The developper says this app doesn't collect or share user data"
Below: "The developper says this app does not collect any user data"

However, in the permissions requested in the About this game section, it is specified that this application can, among other things, access the "precise position (GPS and network)"



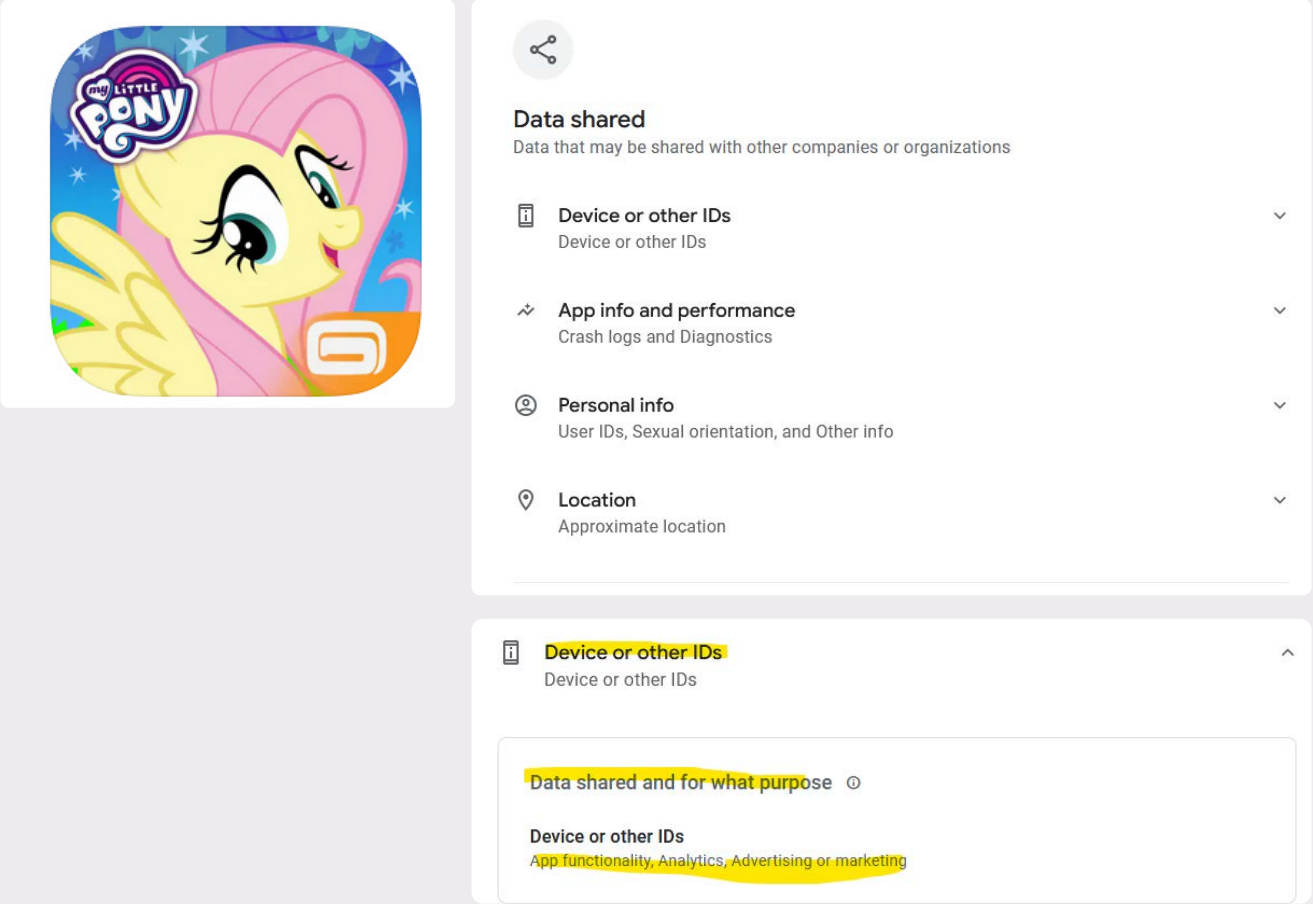
Google's policy rules state that: "If one of the target audiences for your app is children, you must comply with the following requirements. Failure to satisfy these requirements may result in app removal or suspension. [...] Data practices: [...] You must also ensure that your app follows the data practices below: [...] Apps that solely target children may not request location permission, or collect, use, and transmit precise location. [...]"

The studio could justify the use of this permission by arguing that the game is not aimed solely at children. However, the fact remains that the game is part of the "Teacher Approved" program (it is rated 4 years+ in the App Store).

Google Play Families policies state that: "Apps that target both children and older audiences must not transmit any of the following when associated with children or users of unknown age: Android advertising identifier, SIM card serial number, version serial number, BSSID, MAC address, SSID, IMEI, or IMSI."

However, the collection or sharing of these identifiers is not clearly communicated to parents. For example, the "Data Security" section, displayed on the app store page, covers all of these identifiers under the term "Device or other IDs." However, a computer analysis of these apps is required to confirm whether they indeed share these identifiers.

Example of data sharing in violation of Google Play Families policies

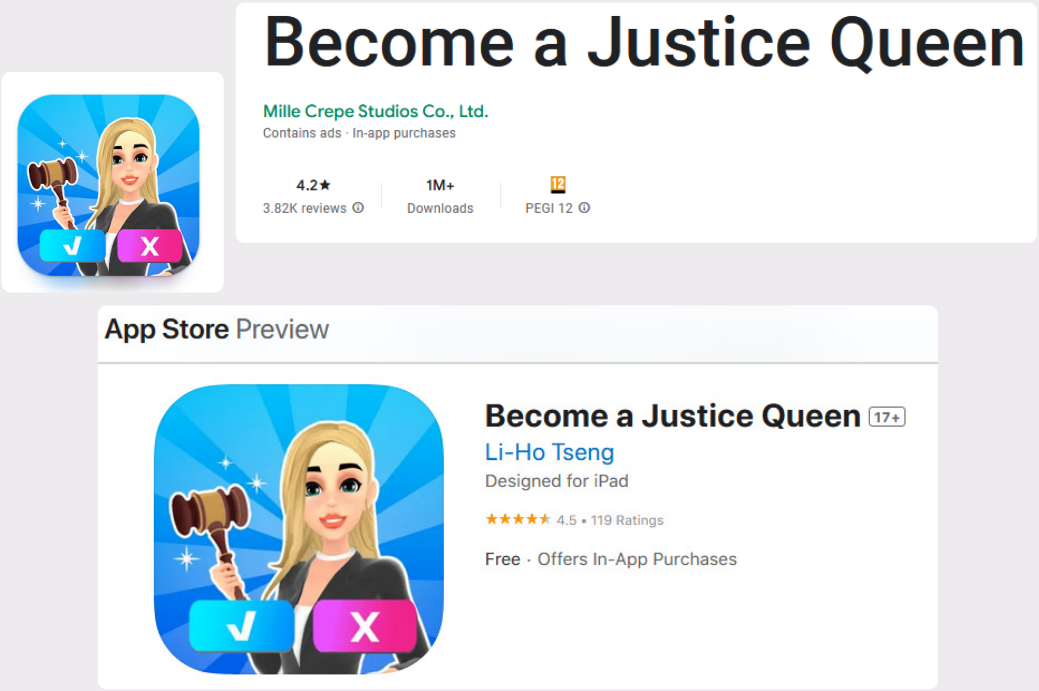


My Little Pony: Magic Princess (Gameloft SE) *states that it shares "Device or other ID" information with third parties for advertising and marketing purposes.*

1.1.5 Apple Store Ratings

In contrast, Apple has opted to develop and utilize its own rating system. Unfortunately, for the same games, Apple's rating categories do not fully align with those of the ESRB or Google. This inconsistency between the various ratings increases potential confusion for parents.

Example of a rating that does not match depending on the access platform



The game Become a Justice Queen *(Mille Crêpes/Li-Ho Tseng) is rated "All audiences/12+" on the Google Play Store and rated "17 years+" on the App Store.*

1.2 Misleading Information Provided by Game Classifications

A problem exists between the tools offered by the video game industry to support parents in selecting games they would deem to be suitable for their children and the compliance of games with laws designed to regulate their privacy.

In addition to all these different and insufficiently regulated classifications, the purpose of the ratings is also confusing, as some regulate content (i.e., ESRB) and others focus on data collection (i.e., Safe Harbor).

The rating assigned to a game does not guarantee its compliance with current laws regarding the protection of children's privacy.

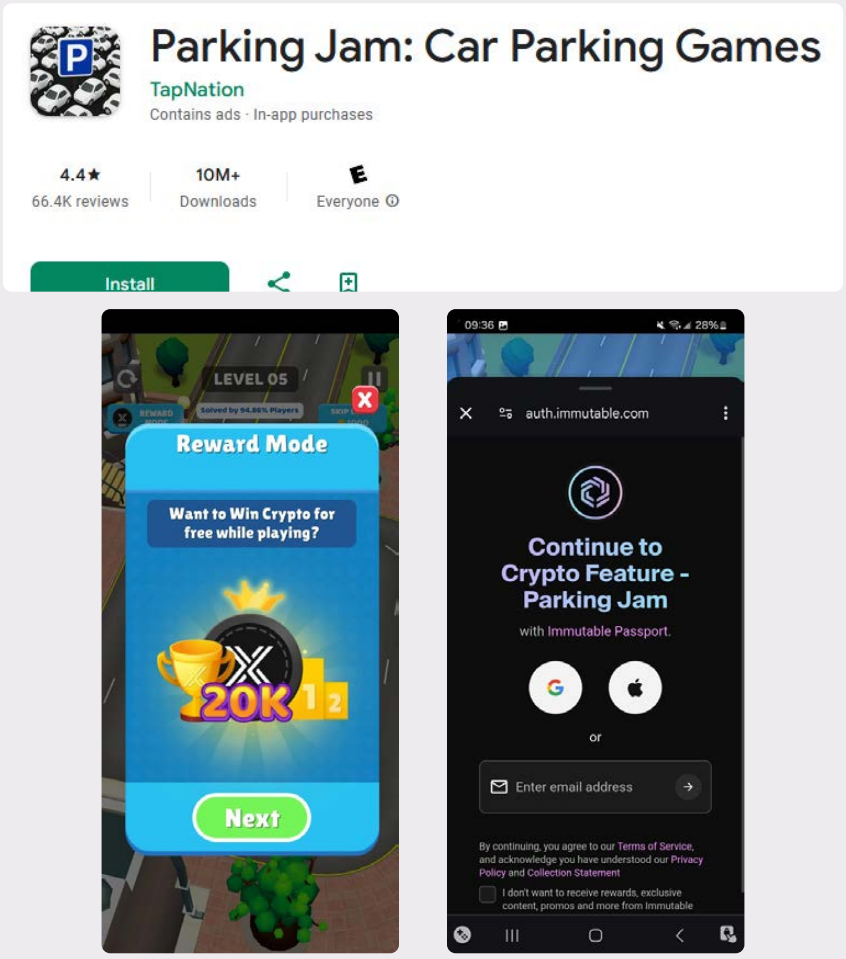
Not only is essential information, some of which can be deemed necessary for enabling parents to make informed choices, often missing, unclear, or varying considerably from one platform to another, but the various classification programs also contain certain misleading elements. Ultimately, these ratings give parents a false sense of security—as if the game were truly adapted to the needs of children and respectful of their rights.

The organizations 5Rights and Good Law Project have highlighed these issues, and recently filed a complaint with the UK Competition and Markets Authority to denounce the misleading nature of age classifications:

> *Big tech is making cash by hiding the age range for ads in the small print – it's time to take on this dangerous trick*[8].

[8] https://goodlawproject.org/campaign/stop-fake-age-ratings-on-app-stores/

An example of the false sense of security that the classification of specific mobile games for children can create



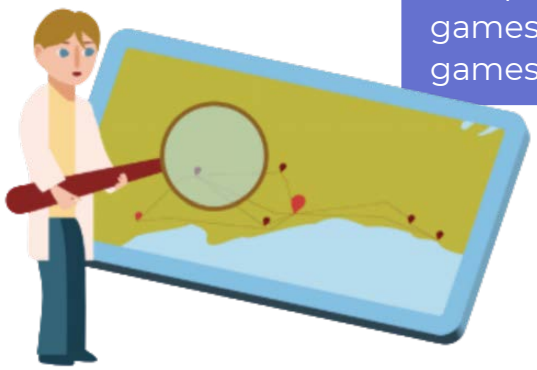
Parking Jam Car Parking *(COMPANY) is rated "Everyone," but during the game session, it offers the child the opportunity to obtain unregulated cryptocurrencies.*

The proliferation of classification systems, certification programs, and transparency initiatives led by various organizations and retailers is confusing for parents. Reading the terms of use and privacy policies of each game remains the only possible solution to ensure the safety and protection of their child's privacy.

GAME TERMS OF USE AND PRIVACY POLICIES

As part of a grant from the Office of the Privacy Commissioner of Canada (2024-2025), our research team notably analyzed the privacy policies of a sample of mobile video games for children (under 13 or 14 in Quebec) to evaluate their compliance with legal obligations in the United States, at the federal level in Canada, and at the provincial level in Quebec. We selected these jurisdictions due to the existence of legal frameworks for the protection of personal data, and specifically that of children, where applicable (in the United States).

A total of 139 policies were manually analyzed, including 84 policies related to free-to-play games, two policies related to free and paid (*freemium*) games, and 53 policies related to paid (*premium*) games.



2.1 The General Non-Compliance of Gaming Privacy Policies with Legal Frameworks

Determining whether policies comply with legal obligations in the United States, Canada, and Quebec proved more complex than anticipated. While it is possible to answer affirmatively regarding compliance with certain obligations, for others, it is more difficult to determine whether legal obligations are being met. In some cases, it seemed overly simplistic to answer yes or no.

This situation can be explained by the various ways in which policies are drafted and by the wording of legal obligations, which is sometimes very imprecise.

In some cases and for specific themes, a multiplicity of approaches allows us to conclude that legal frameworks are being respected (or not), but to varying degrees or in varying ways.

Generally speaking, the analysis of policies shows that none of them fully meet the requirements of the US, Canadian, and Quebec legal frameworks.

It is particularly worrying to note that none of the policies analyzed fully met all three sets of legal obligations, especially since some of these obligations are not particularly demanding of video game studios.

2.2 General Opacity of Privacy Policies

Privacy legislation generally requires all service providers to declare, in their privacy policies, the nature of the data collected, its purpose, and all third-party companies with granted access to personal information.

Children's game studios are also required to obtain free and informed parental consent before collecting, using, or processing children's personal data.

Despite these requirements, privacy policies present several opacity issues, and it remains difficult to obtain details regarding the use of personal data by third parties.

Privacy policies may at first glance address all legal requirements. However, our detailed study revealed severe limitations. For example, some policies describe the types of data collected, but use language that suggests this list is not necessarily exhaustive: using terms like "may include," "such as," or "but not limited to." We observe the same phenomenon about how data is used and collected.

As a result, parents do not have comprehensive information to give free and informed consent. Although privacy policies must be written simply and clearly under Quebec law, reading these legal texts is difficult for the uninitiated (but it is also tricky for third- and fourth-year law students who have had to work hard to understand all the intricacies of the policies).

The policies use both legal and technical jargon, which can be particularly complex for parents to grasp, even after devoting many hours to them. While some policies attempt to simplify their content, others make no effort and require parents to master several complex legal concepts, such as the notion of arbitration.

Regarding technical jargon, the types of data collected are, for example, very numerous and do not necessarily correspond to information with which parents are familiar: Internet Protocol (IP), Keystroke logs, IMEI, IMSI, device type, Android ID, MAC address, Device Token (Apple iOS), Advertiser ID, Persistent identifiers, Log Files, etc.

In addition to specific jargon, the visual format used can make the policies difficult or unpleasant to read, and may be intended to discourage parents from reading them. The length of policies also varies greatly: from a few paragraphs (especially for the rare policies specifying that no data is collected) to several dozen pages for the longest.

Some policies, however, make commendable efforts to offer well-structured content (e.g., with clearly identified headings) and are relatively pleasant to read (e.g., by using color and distinctive visual elements), but they do not represent the norm.

A standardized presentation of privacy policies should be made legally mandatory to make them easier for parents to read and understand.

Policies are also sometimes deliberately vague and imprecise, resulting in a lack of transparency. The previously mentioned expressions are often used: “may include," “such as," “not limited to.” This complexity stems in part from the deliberately incomprehensible and incomplete privacy policies of some development studios.

Several contradictions can be misleading and lead to companies[9] being held accountable. For example, policies in which the studio states that it does not collect data from players, while at the same time using data collected by third parties for its own purposes.

A strategy of accountability involves claiming not to collect personal data, while authorizing third-party companies to do so via the mobile app and then subsequently purchasing the information.

[9] https://www.priv.gc.ca/media/6298/cpvp-gpen-2024-fra.pdf

2.2.1 Variety of Data Collected by the Developer

Applications collect a wide variety of data according to the policies analyzed. We observe five main categories of data:

- Who?
  - For example: email, IP address, gender, country, etc.
- What hardware?
  - For example: device type, device name, internet service provider, etc.
- What type of use?
  - For example: game progress, playing time, playing styles, etc.
- What type of interactions with the platform?
  - For example: information contained in correspondence, financial and transaction data, etc.
- What other information can be shared?
  - For example: information is received by platforms when connecting to a third-party social media platform.

The policies studied use a wide variety of non-standardized phrasing or expressions to describe the data collected, which can hinder parents' understanding.

More than 240 different expressions (out of 112 policies) were listed to describe the data collected.

Certain types of data are the most frequently collected: email, IP address, connection and usage, game progress, operating system type, device ID, first and last name, country, age, and customer support correspondence.

2.2.2 Vague Language

Some of the terms used to describe the data collected are very vague and do not provide much transparency to the public:

> *Other data you choose to give us, other information we ask for, other information that helps us to identify you or helps us to provide or improve our services, information that your browser sends whenever you visit our Service, Log and usage data, game play statistics, types of content viewed, downloaded, or interacted.*

In some cases, policies provide a precise and exhaustive list of the data collected. In other cases, policies use terms such as "we may," "including," "such as," or "not limited to," which seem to indicate that the list of data described as collected is not exhaustive. The vagueness surrounding the possibility of collection raises concerns that this collection is actually taking place, perhaps systematically, and even that there could be other forms of data collection involved, since the list may not be exhaustive.

Thus, uncertainty remains as to precisely what information is actually collected by gaming platforms. These formulations do not contribute to the transparency of the relationship between mobile game studios and parents.

Parents can, if necessary, request their child's data collection history from the studio to determine what the applications have actually mined. However, the studio must still be able to certify that it is completely transparent in its disclosure.

During our research, we observed a possible discrepancy between what studios claim to collect and what they disclose in response to a data access request.

2.2.3 Varying Definitions of Personal and Non-Personal Data

The privacy policies studied do not systematically specify their definitions of personal and non-personal data. If they do, the definitions vary, increasing the confusion: a leeway for potential loopholes and misinterpretations.

Here is a sample of the diversity of definitions:

PERSONAL DATA:

- *Personal Data means data about a living individual who can be identified from those data (or from those and other information either in our possession or likely to come into our possession)*
- *Personal Information is information that may – in one way or another – refer to you, such as address, gender, name, email-address etc.*
- *Personal information refers to all kinds of information recorded electronically or otherwise that can identify a specific natural person or reflect the activities of a specific natural person, either alone or in combination with other information.*
- *Personal data is information about you and can include things like your full name, address, email or phone number.*

NON-PERSONAL DATA:

- *Non-Personal Information means information that is of an anonymous nature, such as the type of mobile device you use, your mobile devices unique device ID, the IP address of your mobile device, your mobile operating system, and information about the way you use the Applications.*
- *Non-personally identifiable information is every kind of information except for personal information. Under this Privacy Policy non-personally identifiable information includes server logs from your device ID and type, language, device operating system, access times, geographic location of device (if enabled) and other types of information that are transformed into a sequence of random-looking characters that are no longer recognizable ("Usage Information").*

Many privacy policies claim not to collect any personal data (which, it is imperative to note, is subject to their technical definition of this concept). However, they do indicate that they collect non-personal data, which, in some cases, may fall under the category of personal data under US, Canadian, and Quebec legal frameworks.

The classification made by the company can also potentially allow it to withhold all of the data collected when requested. Indeed, the company is only required to transmit what it deems personal data.

As long as the company itself defines what "personal data" is, it can claim not to collect any.

2.2.4 Broad and Underspecified Uses of Collected Data

The policies describe an expansive variety of uses for the collected data. Six main categories of data use were observed:

- *Enable access to the service.*
- *Analyze user activity, behavior, and preferences;*
- *Respond to player requests;*
- *Solicit players (through advertising);*
- *Prevent fraud, illegal, or dangerous activities;*
- *In the context of commercial relationships between companies.*

Certain types of use appear to be most popular among game operators:

"To create your account for the App as per your request," "Provide and deliver products and services you request," "display targeted ads," "Responding to your comments, questions and requests, including providing customer support," "To allow you to participate in interactive features (communicate with others)," "Enhance the experience with our Apps, detect fraud, security or technical issues in connection with the Apps."

Some of these expressions are very vague:

"To improve and tailor your experience on our apps, websites, and services," "To improve our Applications by analyzing aggregated data on how users engage with our Applications," "To know who our shoppers are," "Manage our relationship with you," "for other legitimate purposes."

In some cases, policies provide users with a precise and exhaustive list of data uses. In other cases, policies still use terms such as "we may," "for example," or "including," which seem to indicate that the use of the data mentioned is not systematic or that the list of uses is not exhaustive.

2.2.5 The "Legitimate Interests" of Development Studios as an Argument

Several policies mention the studios' legitimate interests in the context of data use. Once again, relatively vague formulations significantly expand (and even without apparent limits in some cases) the possible uses of the collected data:

- *"To meet our legitimate interests, for example improving our websites, apps, and other services"*
- *"Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests"*
- *"Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)"*
- *"Necessary for our legitimate interests (to develop our products/services and grow our business)."*

Furthermore, this notion of “legitimate interests” is not always defined in policies. Non-exhaustive examples are sometimes given, and when the notion is defined, the definitions vary greatly. Here are some examples:

- *"we have a legitimate interest to process necessary data to : Analyze and monitor use of the Service and its social features ; Moderate chats either automatically or manually ; Take action against fraudulent or misbehaving players";*
- *"we have a legitimate interest in using your Personal Information to provide the App in your preferred language, improve the safety, security, and performance of our App, and understand how the App is used, including through research studies that help us understand how people learn with ScratchJr.";*
- *"to meet our legitimate interests, for example improving our websites, apps, and other services";*
- *"for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise";*
- *"to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy";*
- *"to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy";*
- *"In order to promote and monetize our Services to you."*

2.2.6 Gap Between Data Collection and Intended Use

In the majority of cases, the list of data collected and the specifications of use are disjointed and unrelated to each other. It is therefore very complex, if not impossible, to determine precisely for what purposes the data is used (even if the data collected and the uses are described in the policy).

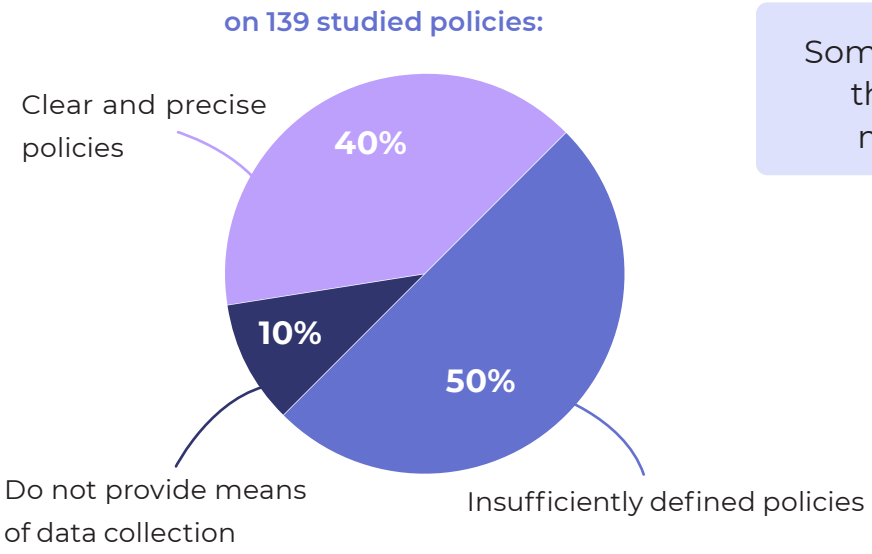
Failure to clearly specify the uses directly linked to the type of data collected potentially hinders parents understanding.

2.2.7 Description of Data Collection Methods

Privacy policies use a variety of terms to describe the means of data collection. We identified three main types of collection methods :

- Information provided by users;
- Information collected automatically;
- Information collected by third-party companies.

Major terminology found within these three categories include: "Cookies," "Google Analytics," "Online registration forms," and "Unity Analytics." It should be noted that some terms are very ambiguous and do not contribute to greater transparency: "Other sources," "other tracking mechanisms," "similar tracking technologies."



Some policies are more specific than others regarding the means of data collection.

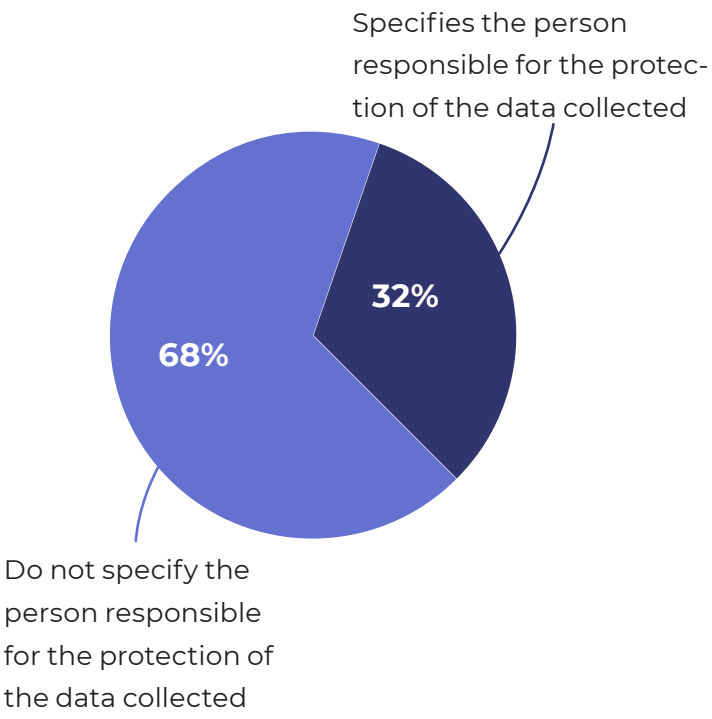
2.2.8. Nominal Designation of Data Protection Responsiblity

Not all policies specify who is responsible for the protection of the data collected.

95 policies do not, while 44 do.

Furthermore, when a person is identified, their contact information is not perspicously specified; it is also accompanied by uncertainty as to their availability or even status within the company.

on 139 studied policies:



Since professional email addresses are rarely used, services such as Gmail have been observed, which does not instill public trust.

2.3 Parental Consent

2.3.1 Terms of Parental Consent

In policies requiring parental consent for children accessing a game, the terms of this consent are not emphatically specified.

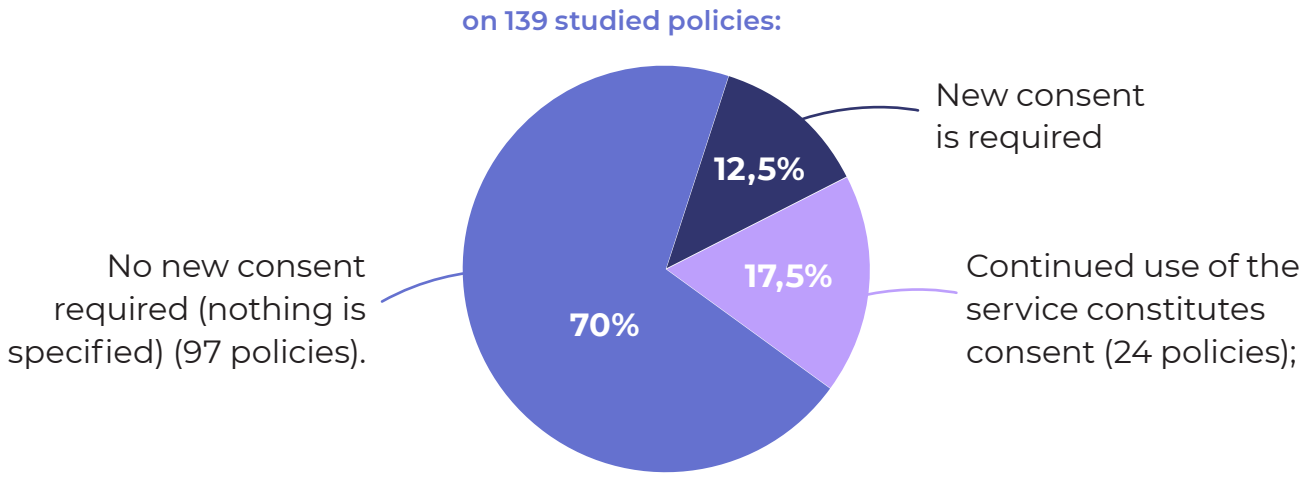
When these terms are specified, several scenarios can be identified in the policies studied:

- Credit card verification;
- Verification using parental identity documents;
- Collection by email;
- Self-declaration by users.

In this sense, the steps taken to verify parental consent appear very limited in some cases.

2.3.2 Parental Consent in the Event of Changes in Data Collection, Use, and Dissemination Practices

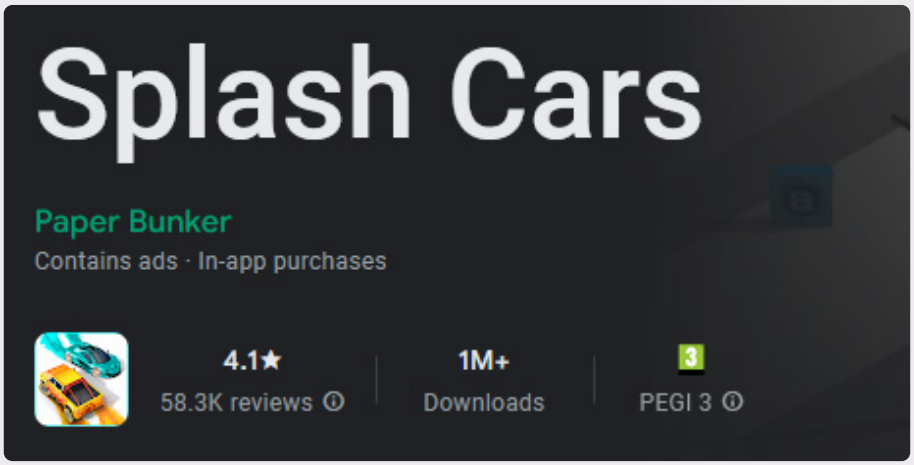
When personal data collection, use, and dissemination practices are changed, the policies provide for several scenarios:



Cases where new consent is sought by platforms when their policies change are therefore very rare.

Example of corporate shirking of responsibility for privacy policy updates

We reserve the right to update this policy. Any changes will be posted here with an updated effective date. Continue using our games after changes constitute acceptance of the updated policy.



While some privacy policy updates may impact actual parental consent, most studios either ignore this or shift the responsibility to parents to regularly check for potential changes (here : https://paperbunker.cz/privacy-policy)

2.3.3 Consequences of Exercising Parental Rights

If parents decide to exercise their rights, particularly the rights to view, modify, and/or delete personal data, most policies warn them of the consequences of doing so. Users may lose access to all or part of the service (and all unlocked content, as well as purchased content, if applicable). However, in many cases, these are not explicitly described.

Some policies, on the other hand, are silent on this point. This should not necessarily be interpreted as a lack of consequences if parents exercise their rights.

2.3.4 Possibility of Recourse

Regarding parental recourse, there are two types of approaches.
Designation of the applicable law (generally not in the country where the user uses the game). For example:

- The Terms will be interpreted in accordance with Japanese laws. In disputes between us and the users, Tokyo District Court will have exclusive jurisdiction in the first instance of said dispute.

The use of arbitration clauses:

- In the United States;
- Or abroad, in countries that are neither the country where the platform is located nor the country of the users.

This type of approach in a country outside Canada naturally limits the parents' possible recourse, thus infringing on their rights.

2.4 Disjunctures Between Declared Target Demographics and Privacy Policy Statements

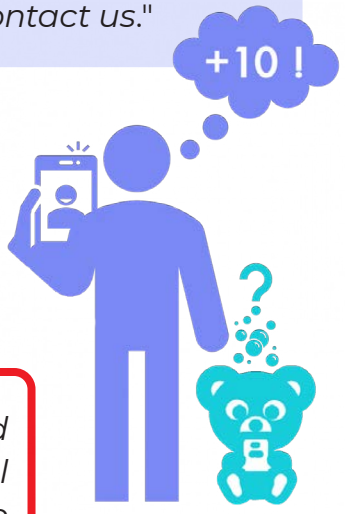
Some free mobile game development studios for children circumvent existing laws by failing to include the information required by existing legislation in their privacy policies.

Another circumvention technique relies on the categorization of apps, their titles, or even the names assigned to development studios. Since the main laws regarding the protection of children's personal information are based on the use and sharing of data knowingly collected from an audience under the age of 13, one strategy is to classify the game in the "Children and Adults" category.

Some mobile game development studios add keywords such as "kids," "toddlers," or "2 years old" to their titles or studio names to stand out in app search engines. However, a quick glance at the associated privacy policies indicates that these games are neither intended nor appropriate for a young audience but for people 13 years and older.

Here is an example:

"Our App is not intended for children under the age of 18. Therefore, we do not knowingly collect or solicit any personal information from children under 18. No one under age 18 may provide any personal information to the App. If you are under 18, do not use or provide any information on this App or through any of its features. Do not provide any information about yourself, including your email address. If we learn that we have collected personal information from a child under age 18 without verification of parental consent, we will erase that information as quickly as possible. If you believe that we might have any information from or about a child under 18, please contact us."



This malicious strategy has been observed frequently: the game is rated "General Audiences," but the privacy policies apply to ages 13 and up, which allows studios to collect data, young children in this case, since the product is clearly aimed at them.

Examples of deliberate inconsistency between the game's target audience and privacy policies

The game Happy Dessert Cafe *(Life Sim/净 邹) is listed as "For everyone/4 years+" even though the policies state that it is not intended for use by children:*

"The Services are not intended for use by children (aged 16 or such higher age as required by applicable law) [...] If you believe that we might have collected personal information from or about a child, please contact us at f693060089@gmail.com."

The Cookie Cats *game is advertised as age 9 and up, but the policies state that their "services are not directed at children":*

"Our Services are not targeted at children. The table below sets out the minimum age per country you must be to use our Services. If you are under the relevant age, you may not use our Services."

In other words, the terms of use may specify that "this game is not intended for an audience under 13 years of age," even though it is clearly targeted at young children and rated accordingly.

These actions are not just bad faith; they violate existing laws designed to protect children, as well as the usage policies of various app stores.

2.5 Failure to Consider Regional Specificities (in particular Quebec)

Privacy policies often take into account US law and the rules applicable in the European Union. Canadian frameworks, and more specifically the Quebec framework, are entirely ignored, which poses significant legal challenges.

For example, a significant number of policies state that personal data from children under 13 is not collected, but Quebec law applies to children 14 and below.

The privacy of children aged 13 in Quebec is not protected as it should be under Quebec law.

THIRD-PARTY COMPANIES

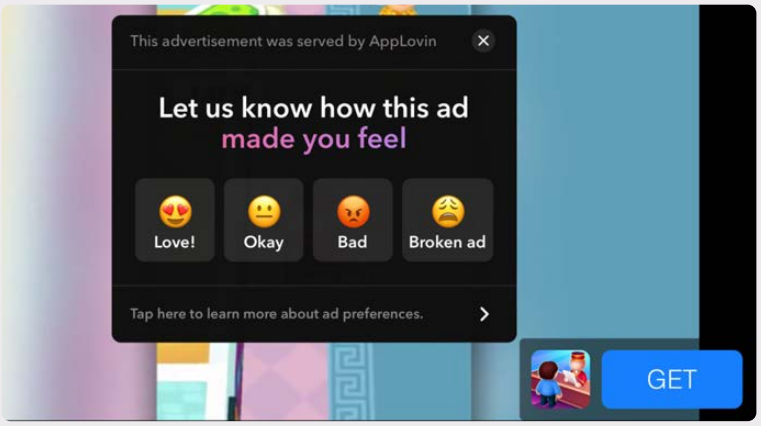
During the game development process, studios use various tools and services from external companies implemented in the game code. These various third-party companies thus gain access to personal data collected via the game application, potentially across the entire mobile device, including geolocation data, representing a hidden privacy issue (Reyes et al., 2018; Oehlenschlager, 2021; van der Hof et al., 2022; Pixalate, 2023).

One of the main privacy issues for children is third-party companies accessing the device at the time the game is downloaded, without explicit consent.

Given that third parties can access a large amount of personal data, children are therefore put at risk daily (Zhao et al., 2020; Alomar and Egelman, 2022).

One of the main privacy issues for children is third-party companies accessing the device at the time the game is downloaded, without explicit consent.

An example of a third-party company piggy-backing on the game app to sell its services



Companies work with third-party advertisers like AppLovin, who display in-game ads. Information about the data exchanged for these displays is not always clear.

In Quebec, the law requires service providers to inform individudals concerned about the data collection, the entities responsible for its collection, any third parties with whom this information is shared, as well as the person designated within these organizations who are responsible for the protection of personal data.

3.1 Exemption of Third-Party Companies from Game Developers' Terms of Service

This collection of user data occurs in part because third parties are not subject to the privacy policies issued by development studios (Myrstad & Tjøstheim, 2021; Reardon et al., 2019).

When a game studio indicates that it only collects data necessary for the game to function properly, this precaution applies only to the studio and not to third-party companies, which gain access to information through what we could call a "back door." This approach unfortunately limits parents' control since, before giving consent, they would need to:

1. Find the list of third-party companies associated with the game,
2. Access their websites,
3. Read and understand their terms of use.

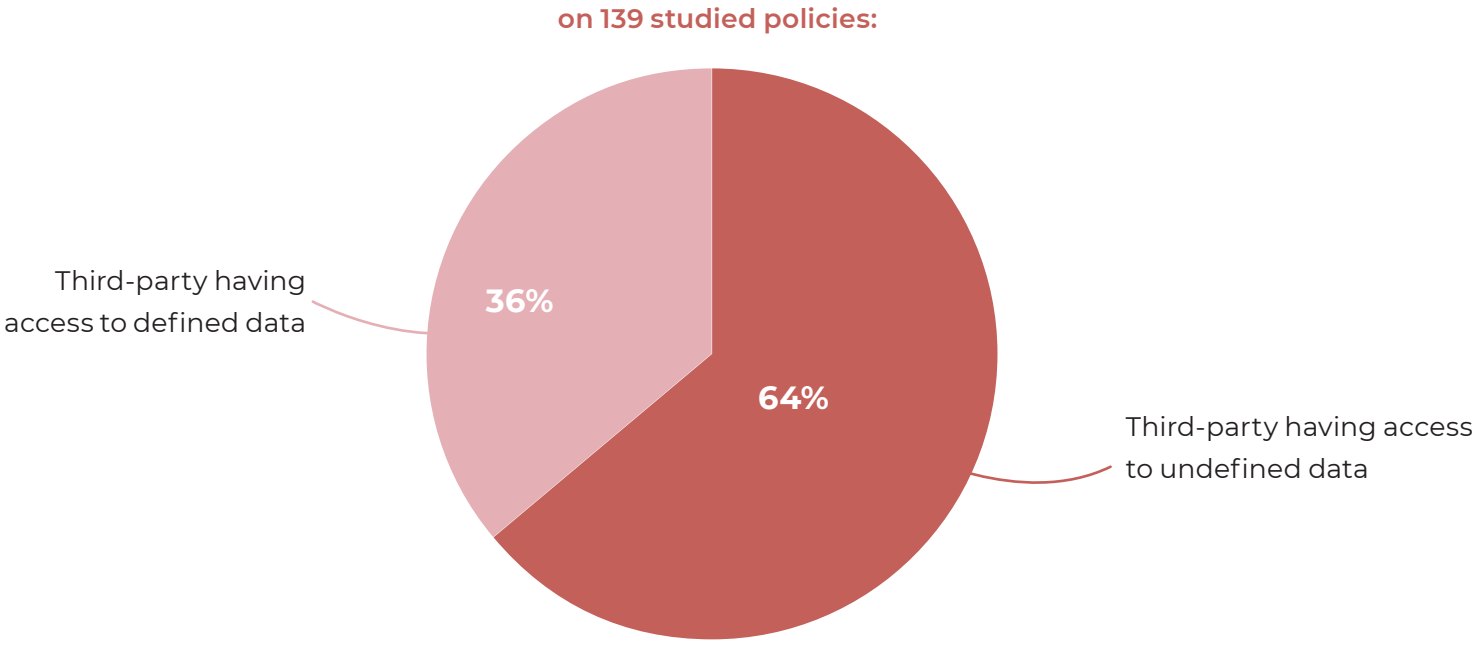
An example of wording that releases the studio from actions taken by third-party companies

7. Third-Party Services

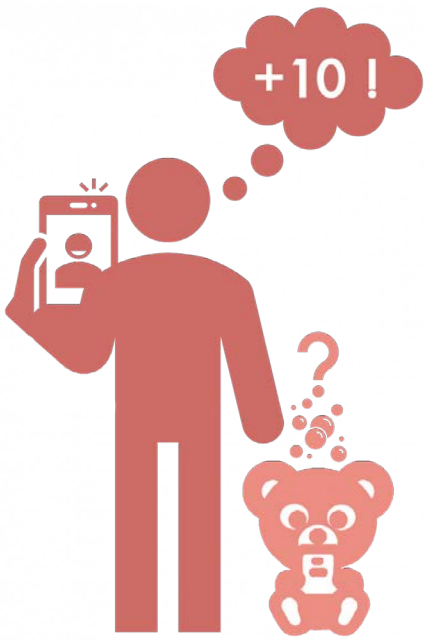
Our games may contain links to third-party services. We are not responsible for their privacy practices. Review their privacy policies before using their services.

The use of terms such as "may contain," "explicit disclaimer," and shifting the responsibility to the parent to read the privacy policies of third-party companies are very common.

This process often proves impossible to achieve at the first stage.



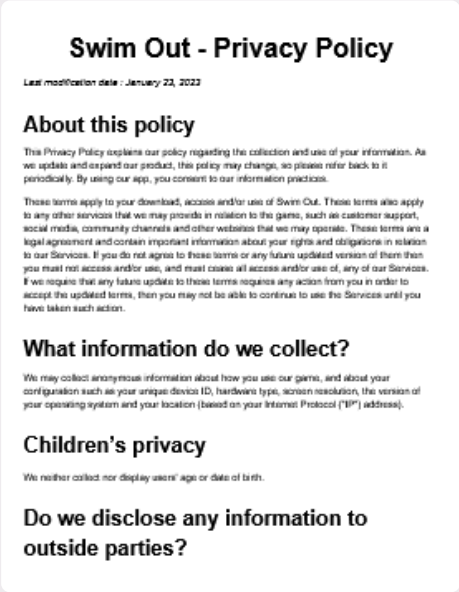
In 50 policies, the third parties who have access to the data are clearly specified, while in 88 policies, they are not.



Thus, the individual is forced to accept the game's terms of use in order to access it, creating a security breach regarding access to their personal data across their entire mobile device (Okoyomon et al., 2019).

Example of major problems in a privacy policy: the game *Swim Out* by Losange Lab, rated "General Audiences / 4 years+"

First, the policy is very short, and its version on Google Play is located in a Google Doc file, which does not seem very serious to the parent.



Swim Out - Privacy Policy

Last modification date : January 23, 2023

About this policy

This Privacy Policy explains our policy regarding the collection and use of your information. As we update and expand our product, this policy may change, so please refer back to it periodically. By using our app, you consent to our information practices.

These terms apply to your download, access and/or use of Swim Out. These terms also apply to any other services that we may provide in relation to the game, such as customer support, social media, community channels and other websites that we may operate. These terms are a legal agreement and contain important information about your rights and obligations in relation to our Services. If you do not agree to these terms or any future updated version of them then you must not access and/or use, and must cease all access and/or use of, any of our Services. If we require that any future update to these terms requires any action from you in order to accept the updated terms, then you may not be able to continue to use the Services until you have taken such action.

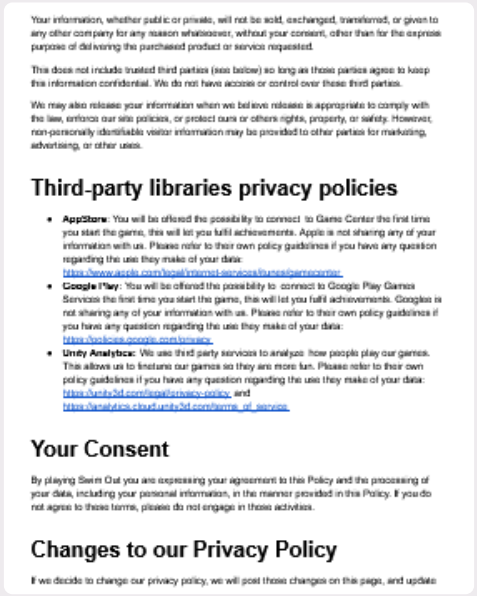
What information do we collect?

We may collect anonymous information about how you use our game, and about your configuration such as your unique device ID, hardware type, screen resolution, the version of your operating system and your location (based on your Internet Protocol ("IP") address).

Children's privacy

We neither collect nor display users' age or date of birth.

Do we disclose any information to outside parties?



Your information, whether public or private, will not be sold, exchanged, transferred, or given to any other company for any reason whatsoever, without your consent, other than for the express purpose of delivering the purchased product or service requested.

This does not include trusted third parties (see below) so long as those parties agree to keep this information confidential. We do not have access or control over these third parties.

We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others' rights, property, or safety. However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

Third-party libraries privacy policies

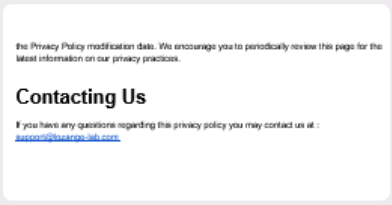
- **AppStore**: You will be offered the possibility to connect to Game Center the first time you start the game, this will let you fulfil achievements. Apple is not sharing any of your information with us. Please refer to their own policy guidelines if you have any question regarding the uses they make of your data:
https://www.apple.com/legal/internet-services/itunes/gamecenter/
- **Google Play**: You will be offered the possibility to connect to Google Play Games Services the first time you start the game, this will let you fulfil achievements. Google is not sharing any of your information with us. Please refer to their own policy guidelines if you have any question regarding the uses they make of your data:
https://policies.google.com/privacy
- **Unity Analytics**: We use third party services to analyze how people play our games. This allows us to finetune our games so they are more fun. Please refer to their own policy guidelines if you have any question regarding the uses they make of your data:
https://unity3d.com/legal/privacy-policy and
https://analytics.cloud.unity3d.com/terms_of_service

Your Consent

By playing Swim Out you are expressing your agreement to this Policy and the processing of your data, including your personal information, in the manner provided in this Policy. If you do not agree to these terms, please do not engage in these activities.

Changes to our Privacy Policy

If we decide to change our privacy policy, we will post those changes on this page, and update

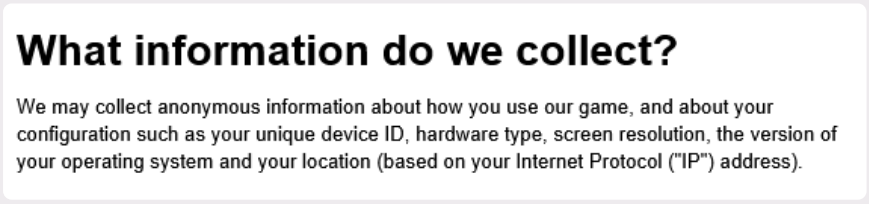


the Privacy Policy modification date. We encourage you to periodically review this page for the latest information on our privacy practices.

Contacting Us

If you have any questions regarding this privacy policy you may contact us at :
support@losange-lab.com

Next, to the question "what information do we collect?," this studio claims to collect anonymous data. However, contrary to what it claims, this data is not "anonymous" since it represents potentially identifiable information (the device's unique ID number and IP address).



What information do we collect?

We may collect anonymous information about how you use our game, and about your configuration such as your unique device ID, hardware type, screen resolution, the version of your operating system and your location (based on your Internet Protocol ("IP") address).

Furthermore, it disclaims responsibility for the potential collection of data on children by claiming "not to know" the age of players. This approach raises the possibility that children's personal data may be present in the databases.

Children's privacy

We neither collect nor display users' age or date of birth.

Without any guarantee of protecting children's privacy, the studio nevertheless shares (discloses) information with "trusted" third-party companies (Google, Apple, and Unity), but again disclaims responsibility for what these companies do. It may also share "non-identifying information" (according to its own definition) with third parties in the context of advertising or other activities.

Your information, whether public or private, will not be sold, exchanged, transferred, or given to any other company for any reason whatsoever, without your consent, other than for the express purpose of delivering the purchased product or service requested.

This does not include trusted third parties (see below) so long as those parties agree to keep this information confidential. We do not have access or control over these third parties.

We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others rights, property, or safety. However, non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or other uses.

The parent has no choice regarding consent, since refusal is tantamount to not being able to play.

Your Consent

By playing Swim Out you are expressing your agreement to this Policy and the processing of your data, including your personal information, in the manner provided in this Policy. If you do not agree to these terms, please do not engage in those activities.

Finally, if the policy changes, parents are responsible for "periodically" reviewing it, which is unrealistic considering the average number of mobile apps on each device.

Changes to our Privacy Policy

If we decide to change our privacy policy, we will post those changes on this page, and update

In summary, this example demonstrates the lack of privacy protection for children (potentially as young as 4 years old) and the blatant lack of accountability of mobile gaming companies.

Children's apps reportedly include a median of 7 third parties, but one-fifth of them have more than 10 third parties, and these numbers could rise to 40 for some game studios (Sun et al., 2023).

Furthermore, studies highlight that games aimed at children generally include more third parties than apps in other categories (Reyes et al., 2018; Binns et al., 2018).

For all these reasons, the process designated to grant free and informed consent is seriously compromised.

3.2 Identification of Third-Party Companies That Have Access to Data

According to the policies analyzed, a wide variety of third-party companies may have access to user data. The main categories are:

- Affiliated companies
- Service providers
- Marketing, advertising, and analytics partners
- Public authorities
- Consultants (lawyers, bankers)

Some policies use different terminology for different types of third parties, which makes it difficult for parents, notably, to understand. Some of the terms employed are extremely vague, such as "our affiliate," "third parties," or "advertising partners." These categories of third-party companies have different data access rights.

Example of sharing personal data with third-party companies

ADVERTISING

"Creatures of the Deep" shows ads to provide content free of charge. When launched on your device, the game will automatically send certain information to our advertising partners. That information may include the name of the app, the device type, and the advertising ID.

In its privacy policy, Infinite Dreams Studio automatically shares identifying information such as the unique advertising ID number with third-party advertisers. (https://www.idreams.pl/privacy/CotD_PrivacyPolicy.html).

ADVERTISING ID

The advertising ID number is a unique code present on the mobile device that allows it to be recognized in order to aggregate all the information collected from various sources. It enables the creation of a user "identity" to profile and target them with targeted advertising. Claiming that this information is "anonymous" is misleading since it allows for the identification of an exact usage profile (not to mention the fact that, by cross-referencing databases, including public databases, the individual's contact information is easily associated with the advertising ID number).

SOFTWARE DEVELOPMENT KIT

An SDK, or Software Development Kit, is a set of mobile application development tools designed to facilitate the work of studios. Third-party companies can be added to the SDK and then integrated into the game application. When the game is downloaded, the third-party companies are also downloaded.

Furthermore, some game studios evade their obligations under the three legal frameworks analyzed by claiming that third parties have direct access to data (for example, via SDKs) and that they do not act as intermediaries or data collectors. Once again, the studios refer parents to the privacy policies of these third-party companies.

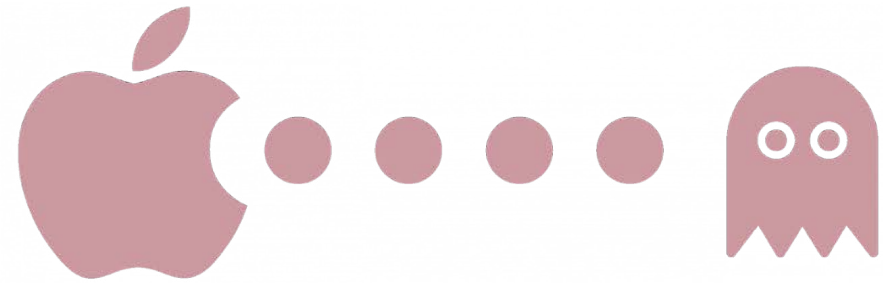
3.3 Direct Data Collection by Third-Party Companies

In practice, a large amount of data is not initially collected by the studios, but instead by third parties, notably with various business objectives, such as advertising profiling, in mind.

These third-party companies then provide game studios with information from their personal data collection, through a figure of "sleight of hand": the game application serves as a pretext for various third parties to attach themselves to it, which then collect data more broadly on the device. In return, the studio purchases this information collected by third parties.

Game developers declare this data collection as being collected from and for a generic third party. However, since the data analyzed is statistical and not individualized, the privacy policies indicate that this is not the collection of personal data, but rather analytical data on all users.

This way of operating, where third-party companies collect personal data and then sell the results of the analyses to game studios, is a sleight of hand, allowing these studios to claim that they collect little data.



3.4 Types of Data Collected by Third-Party Companies

While game developers focus data collection on only certain types of data necessary for the proper functioning of the application, third-party companies potentially collect data from the entire device.

We observe this same phenomenon with the lists of data collected by the studios that provide the game. The types of data collected by third parties are sometimes specified in detail. In other cases, the applications do not provide the list, and parents must refer to the policies of the relevant third parties to try to determine what data is collected (with the aforementioned problems of identifying third parties and accessing their policies).

Finally, policies sometimes provide non-exhaustive lists of data types, again using terms like "may include."

3.5 Corporate Concentration

Even though hundreds, if not thousands, of video game studios exist, a few giant corporations actually own many companies. Similarly, third-party companies concentrate the services offered to studios.

The high concentration within this techno-economic ecosystem does virtually nothing to protect children's privacy and reinforces daily online surveillance (Christl et al., 2017).

Google and Meta stand out as sources of data voluntarily offered by users (Reviglio, 2022: 4).

However, they are also important intermediaries due to the services they offer (advertising, payment processes, etc.), but also due to the various partnerships existing between these companies and data brokers (Abrardi et al., 2025).

These two giants have even acquired a special status as Super SDKs (or a super set of mobile application development tools) by offering various third-party services that have become indispensable to studios and by playing a central role in the circulation of personal data (Pybus and Coté, 2024).

This entire techno-economic architecture, now well established, does not take sufficient account of children's privacy needs, for example, by including protective barriers in the structure itself that are impossible for delinquent companies to overcome.

CONCLUSION

VIOLATION OF CHILDREN'S PRIVACY PROTECTION LAWS

A gap exists between the need to protect children from the commercial exploitation of their personal data and the regulation of mobile game studios for minors.

Furthermore, the legal framework appears to primarily focus on the responsibility of parents to read privacy policies, exercise their judgment, and take necessary measures to protect their children's data, which is herculean given the many issues raised in this report.

Thus, in the mobile gaming sector, parents lack the tools or knowledge necessary to make an informed choice regarding the protection of their children's privacy. Not only are the necessary framework and information lacking, but parents are also provided with information that can confuse or even deceive them, giving them false assurances that their children's privacy is protected.

Various malicious strategies are also deployed by companies in their terms of use:

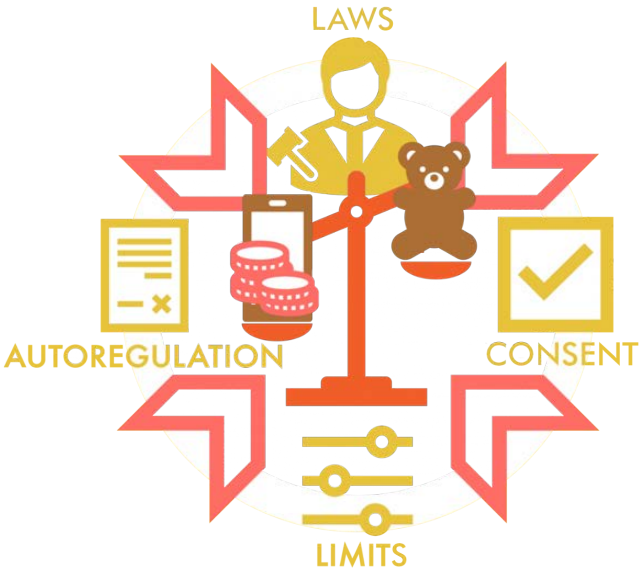
- stating that the game is intended for ages 13 and up in the privacy policies (even if the game is clearly aimed at toddlers and young children);
- omitting certain legally required information;
- using vague language that allows for the widespread collection of personal data;
- failing to inform parents of changes to privacy policies;
- making it difficult to link the types of data collected with the types of uses made of it.
- referring the responsibility of third-party companies if personal data is collected via the mobile game, etc.

These results demonstrate the gaps in privacy protection for children playing mobile games. These problems can stem from several sources, such as:

- legal clauses are individually flawed (e.g., "the user transfers their personal data");
- a combination of clauses that creates a loophole (e.g., clause A states "no data is transferred without user authorization," clause B states "authorization is granted by default unless explicitly refused");
- an incomplete list of third-party companies, intentionally or not;
- third-party companies that mislead about the use of data;
- unrealistic expectations regarding parental obligations: parents are unable to locate the third-party companies concerned, to read all their terms of use before accepting the mobile game's terms, etc.

To enable everyone to make informed decisions about their children's privacy and the processing of their personal data, it is essential to raise public awareness about the technological environment that supports this type of product, while proposing new standards for companies.

Various recommendations are made to legislators, the video game industry, parents, and children. We must, first and foremost, address children directly to ensure that they can be equipped and ready to grow up healthily in this digital world.



BIBLIOGRAPHY

Abrardi, L., Cambini, C., & Pino, F. (2025). Data brokers competition, synergic datasets, and endogenous information value. International Journal of Industrial Organization, 103146.

Alha, K. (2020). The Rise of Free-to-Play: How the revenue model changed games and playing. (Tampere University Dissertations - Tampereen yliopiston väitöskirjat ; Vol. 345). http://urn.fi/URN:ISBN:978-952-03-1774-4.

Alha, K. (2020). The Rise of Free-to-Play: How the revenue model changed games and playing. (Tampere University Dissertations - Tampereen yliopiston väitöskirjat ; Vol. 345). http://urn.fi/URN:ISBN:978-952-03-1774-4.

Alomar, N., & Egelman, S. (2022). Developers Say the Darndest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. Proceedings on Privacy Enhancing Technologies, 4(2022), 24.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., & Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. Proceedings of the 10th ACM Conference on Web Science, 23–31. https://doi.org/10.1145/3201064.3201089

Bonenfant, M., Dumont, A., & Lafrance St-Martin, L. I. (2023). Chapter 1. Being played in everyday life : Massive data collection on mobile games as part of ludocapitalist surveillance dispositif. Dans L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (dir.), Everyday Life in the Culture of Surveillance (p. 21-44). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-1

Bryant, J. (2020, 27 mai). Are COPPA safe harbor programs getting the job done?. IAPP. https://iapp.org/news/a/oversight-transparency-of-coppa-safe-harbors-debated

Buijsman, M. (2025, juin 2024). How did the global games market reach $182.7B in 2024—and what's next?. Newzoo. https://newzoo.com/resources/blog/global-games-market-update-q2-2025

Canadian Centre for Child Protection. (2022). Reviewing the Enforcement of App Age Ratings in Apple's App Store and Google Play. [Rapport]. https://protectchildren.ca/en/resources-research/app-age-ratings-report/

Christl, W., Kopp, K., & Riechert, P. U. (2017). Corporate surveillance in everyday life. Cracked Labs, 6(1), 1.

Commissariat à la protection de la vie privée du Canada. (2024, 9 juillet). Rapport sur le ratissage du Commissariat à la protection de la vie privée du Canada de 2024 :

Mécanismes de conception trompeuse [Rapport]. Commissariat à la protection de la vie privée du Canada. https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-internationale/reseaux-internationaux-de-protection-de-la-vie-privee/ratissage-international-pour-la-protection-de-la-vie-privee/2024_ratissage/rapport-ratissage-cpvp-2024/

Data.ai. (2024, Janvier). State of Mobile 2024. [Rapport]. https://www.data.ai/en/go/state-of-mobile-2024/

Drummond, A., & Sauer, J. D. (2018). Video game loot boxes are psychologically akin to gambling. Nature human behaviour, 2(8), 530–532. https://doi.org/10.1038/s41562-018-0360-1

Entertainment Software Association of Canada. (2022, Novembre). Rapprocher les Canadiens par le jeu : Faits essentiels 2022. [Rapport]. https://essentialfacts.ca/wp-content/uploads/2022/11/EF2022_FR.pdf

Entertainment Software Rating Board [@ESRBRatings]. (2019, 23 Avril). Yes, we retired the eC rating last year around this time. There were SO few games that fit the criteria, and the argument could almost always be made that E was also applicable for those titles! [Gazouillis]. Twitter. https://twitter.com/esrbratings/status/1120695817340321794

ESRB. (s.d). Privacy Certified Seals. Entertainment Software Rating Board. https://www.esrb.org/privacy-certified-seals/#what-are-the-requirements-for-the-epc-kids-seal

Fogg, B. J. (2002). Persuasive technology : Using computers to change what we think and do. Ubiquity, 2002(December), 5:2. https://doi.org/10.1145/764008.763957

Göksu, İ., Aslan, A., et Turgut, Y. E. (2020). Evaluation of mobile games in the context of content: What do children face when playing mobile games? E-Learning and Digital Media, 17(5), 388-407. https://doi.org/10.1177/2042753020936785

Good Law Project. (s.d.). Campaign: Stop fake age ratings on app stores. Good Law Project. https://goodlawproject.org/campaign/stop-fake-age-ratings-on-app-stores/

Grimes, S. M., Jayemanne, D., & Giddings, S. (2023). Rethinking Canada's Approach to Children's Digital Game Regulation. Canadian Journal of Communication, 48(1), 142–162. https://doi.org/10.3138/cjc.2022-0008

IARC. (s.d). About IARC. International Age Rating Coalition. https://www.globalratings.com/about.aspx

James, A., Gordon, R et Mills, S. (2022). Between Gaming and Gambling: Children, Young People, and Paid Reward Systems in Digital Games. Loughborough University. https://hdl.handle.net/2134/21640190.v1.

King, D., Delfabbro, P., & Griffiths, M. (2010). The convergence of gambling and digital media: Implications for gambling in young people. Journal of Gambling Studies, 26, 175-187.

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.

Mathur, A., Kshirsagar, M., & Mayer, J. (2021). What makes a dark pattern... Dark? : Design attributes, normative considerations, and measurement methods. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 1–18. https://doi.org/10.1145/3411764.3445610

MediaSmarts : Canada's Center for Digital Media Literacy. (s.d). Understanding the Rating Systems. MediaSmarts. https://mediasmarts.ca/sites/default/files/pdfs/tipsheet/TipSheet_Understanding_Rating_System_0_0.pdf

Myrstad, F. et Tjøstheim, I. (2020). Out of control: How consumers are exploited by the online advertising industry [Rapport]. Forbrukerrådets. https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf

Nieborg, D. B. (2016). From premium to freemium: The political economy of the app. Dans T. Leaver, & M. Willson (dir.), Social, casual and mobile games: The changing gaming landscape (pp. 225–240). https://doi.org/10.5040/9781501310591.ch-016.

Oehlenschlager, M. (2021). Online Games Are Gambling With Children's Data. [Rapport]. IDA et DataEthics.eu. https://dataethics.eu/online-games-are-gambling-with-childrens-data/.

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.

Pixalate. (2023). Q1 2023 Children's Online Privacy Risk Report: Age Screening & Parental Consent On Mobile Apps. [Rapport]. Pixalate. https://www.pixalate.com/hubfs/Reports_and_Documents/Mobile%20Reports/2023/Childrens%20Privacy%20Age%20Screening/Q1%202023%20Childrens%20Privacy%20Age%20Screening%20Report.pdf?_hsmi=251951782

Pybus, J., & Coté, M. (2024). Super SDKs: Tracking personal data and platform monopolies in the mobile. Big Data & Society, 11(1), 20539517241231270.

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

Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview. Internet Policy Review, 11(3), 1-27.

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., et 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

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., et 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

Statista. (2022, Avril). Mobile phone usage among children and teens in Canada as of April 2022, by age group. https://www.statista.com/statistics/1319950/canada-mobile-usage-kids-and-teens-by-age

van der Hof, S., van Hilten, S., Ouburg, S., Birk, M. V., & van Rooij, A. J. (2022). "Don't Gamble With Children's Rights"—How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment. Frontiers in Digital Health, 4, 822933. https://doi.org/10.3389/fdgth.2022.822933.

Xiao, L. Y. (2023). Beneath the label: Unsatisfactory compliance with ESRB, PEGI and IARC industry self-regulation requiring loot box presence warning labels by video game companies. Royal Society Open Science, 10(3), 230270. https://doi.org/10.1098/rsos.230270

Zagal, J. P., Björk, S., & Lewis, C. (2013). Dark Patterns in the Design of Games. Foundations of Digital Games 2013. https://urn.kb.se/resolve?urn=urn:nbn:se:ri:diva-24252

Zhao, F., Egelman, S., Weeks, H. M., Kaciroti, N., Miller, A. L., et Radesky, J. S. (2020). Data Collection Practices of Mobile Applications Played by Preschool-Aged Children. JAMA Pediatrics. https://doi.org/10.1001/jamapediatrics.2020.3345

RECOMMENDATIONS

LEGISLATORS

Dangerous Game

Protecting the privacy of children under 13 years in mobile games

UQÀM
McGill
uOttawa

Context

Mobile gaming is incredibly popular among children in Canada. According to the Entertainment Software Association of Canada (ESAC), young people aged 6-to-17 play an average of 13 hours of digital games per week and, for the youngest (6 to 12 years old), 49% of girls and 31% of boys play on mobile platforms (ESAC, 2020). Overall, 39% of young Canadians aged 2-to-6 years use smartphones, while 50% of 7- to 11-year-olds own their own mobile device (Statista, 2022).

The mobile gaming industry is booming. In 2023, mobile games accounted for 50% of the global video game market (Newzoo, 2023) and it is now the most lucrative sector of the video game industry (Data.ai., 2024). Mobile games make money in many ways, but three economic models dominate: paid games (premium), games where part of the content is free and other parts are paid (freemium), and games that are "free-to-play" (F2P). Freemium and F2P, as well as many premium games make money from microtransactions, paid advertisements, and the collection and sale of player data (Nieborg, 2016; Oehlenschlager, 2021).

These trends extend to mobile games targeted to players aged 12 and under, raising serious privacy issues that not all parents or children are aware of. Previous research shows that even games rated for "ages 4+" might contain data collection and tracking, advertising, and microtransactions (Reyes et al., 2018). Other studies found that children's games can contain "persuasive design" features built to convince or even compel young players into buying items, playing for longer, or sharing more data (5Rights, 2023). Until now, little was known about how prevalent these trends are in mobile games targeted to children in Canada.

Mobile games carry age ratings that are determined by industry associations or by the app stores themselves. Notably, these ratings do not reflect privacy practices or regulatory compliance—even in countries with laws that protect children's privacy and limit what data can be collected from them. While descriptions of a game's privacy practices and policies are (usually) available in the app stores, they are notoriously vague, hard to find, and largely go unread (Pew Research Center, 2019). Children and their parents are making decisions about which games are appropriate without knowing the full picture.

Are mobile games targeted to children under 13 years following the rules when it comes to children's privacy and consumer protection laws? Our study shows that they are not.

The Current Study

We analyzed 750 mobile games across two major platforms and all three economic models to find out. Our sample included titles promoted on the Google Play "Teacher Approved" list and the Apple Store's "Kids & Family" list. Both lists are described as curated collections of titles that are age-appropriate and recommended for children.

Our comprehensive content analysis tracked the presence of ads and other commercial elements in 500 children's mobile games, in addition to 250 games previously analyzed. Our design analysis investigated the underlying software programs (i.e., code) of a subset of Android games. Our legal analysis examined the privacy policies of 54 premium games, 84 F2P games, and 2 freemium games (140 games total).

We looked at if and how the games' policies met the child privacy requirements established in three pieces of legislation: the Children's Online Privacy Protection Act (COPPA) (California, United States), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and Quebec's Act respecting the protection of personal information in the private sector (P 39.1).

Acknowledgement

This project was made possible thanks to financial support from the Office of the Privacy Commissioner of Canada (OPC) through its Contributions Program 2024-2025.

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Research Team

Maude Bonenfant, Full Professor in Social and Public Communication, Université du Québec à Montréal (UQAM)

Sara M. Grimes, Full Professor in Communication Studies, McGill University

Thomas Burelli, Associate Professor in Civil Law, University of Ottawa

Hafedh Mili, Full Professor in Computer Science, UQAM

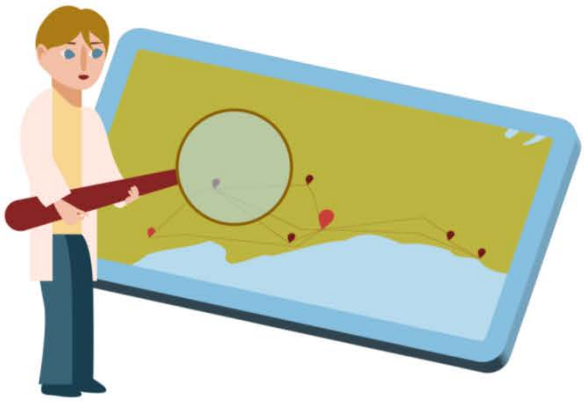
Here's what we found:

Sweeping non-compliance:

None of the 140 policies we analyzed fully meet the requirements of the Californian, Canadian, and Quebec legal frameworks. The policies of paid games were not of any higher quality or compliance than the freemium or F2P games. It is particularly worrying that none of the policies fully meet legal obligations, given that many of these obligations are not particularly demanding. The bar is relatively low, yet all these games failed to meet it.

Ratings vs. privacy policies:

Although we only looked at games that were rated as appropriate for children under 13 years, a huge number of their privacy policies listed the minimum age required to use the app at 13 years or even 18 years. This raises urgent questions about the privacy practices of these companies and if and how they are safeguarding younger users. This disconnect is problematic on many levels, as kids and parents are unlikely to read the privacy policy and very likely to assume apps classified by storefronts as child-friendly will be. Ratings and privacy policies need to be consistent when it comes to user age and comply with applicable regulations.



Lack of clarity on how data is used:

The privacy policies described a very wide range of uses for the data collected through game apps, some functional (e.g., user experience research to improve design) and some commercial (e.g., advertising, sharing data with other companies). Descriptions of how data is used are often vague. In fact, most policies were also unclear and inconsistent about what counts as personal or non-personal data. In some cases, data that would in some cases qualify as personal under existing privacy laws was miscategorized as non-personal (i.e., not protected).

Lack of clarity on how data is shared:

According to the privacy policies analyzed, a wide variety of third parties may have access to player data. This includes: Affiliated companies; Service providers; Marketing, advertising, and analytics partners; Public authorities; and Consultants (lawyers, bankers). In 52 policies, the third parties who (may) have access to player data are clearly specified. In many more (87) policies, however, they are not.

Parental consent?:

Although companies are supposed to seek parental consent before collecting data from or about kids, very few of the policies specified if or how this was done. Very few described renewing consent after changes are made to data practices– even though this too is mandatory.

Recommendations for Policy Makers

1. Policies need to be legible to children and parents: Develop tools to enable players and parents to read and understand mobile video game privacy policies.
2. Many children's game apps are made by small developers without the resources to hire law professionals to draft policies. Develop privacy policy templates for gaming platforms to standardize practices and ensure compliance with certain obligations.
3. Make reporting problems and non-compliant service providers much easier and more accessible. Enforcement of existing regulation depends on citizen complaints but the process is obscure and arduous.

4. Current ratings are inadequate and not covering privacy and many other rights. Develop a more robust system for rating games that considers content but also business practices and interactions that happen in and through the game. This system should be monitored and enforced by government or civil society, not industry.
5. More robust regulation is required. Look to existing examples advancing privacy-by-design or rights-by-design, such as the UK Age-Appropriate Design Code.
6. Call for widespread investigation of privacy and data practices in children's apps. This should start with an investigation of games rated as appropriate for children, but whose policies specify that they are intended for ages 13 and older.
7. Increased literacy for kids, parents, and teachers about hidden privacy risks and common data practices in the mobile games sector. Provide practical tips and strategies for making more informed decisions aimed at protecting children's privacy.

RECOMMENDATIONS

GAME DEVELOPMENT STUDIOS

Dangerous Game

Protecting the privacy of children under 13 years in mobile games

UQÀM McGill uOttawa

Context

Mobile gaming is incredibly popular among children in Canada. According to the Entertainment Software Association of Canada (ESAC), young people aged 6-to-17 play an average of 13 hours of digital games per week and, for the youngest (6 to 12 years old), 49% of girls and 31% of boys play on mobile platforms (ESAC, 2020). Overall, 39% of young Canadians aged 2-to-6 years use smartphones, while 50% of 7- to 11-year-olds own their own mobile device (Statista, 2022).

The mobile gaming industry is booming. In 2023, mobile games accounted for 50% of the global video game market (Newzoo, 2023) and it is now the most lucrative sector of the video game industry (Data.ai., 2024). Mobile games make money in many ways, but three economic models dominate: paid games (premium), games where part of the content is free and other parts are paid (freemium), and games that are "free-to-play" (F2P). Freemium and F2P, as well as many premium games make money from microtransactions, paid advertisements, and the collection and sale of player data (Nieborg, 2016; Oehlenschlager, 2021).

These trends extend to mobile games targeted to players aged 12 and under, raising serious privacy issues that not all parents or children are aware of. Previous research shows that even games rated for "ages 4+" might contain data collection and tracking, advertising, and microtransactions (Reyes et al., 2018). Other studies found that children's games can contain "persuasive design" features built to convince or even compel young players into buying items, playing for longer, or sharing more data (5Rights, 2023). Until now, little was known about how prevalent these trends are in mobile games targeted to children in Canada.

Mobile games carry age ratings that are determined by industry associations or by the app stores themselves. Notably, these ratings do not reflect privacy practices or regulatory compliance—even in countries with laws that protect children's privacy and limit what data can be collected from them. While descriptions of a game's privacy practices and policies are (usually) available in the app stores, they are notoriously vague, hard to find, and largely go unread (Pew Research Center, 2019). Children and their parents are making decisions about which games are appropriate without knowing the full picture.

Are mobile games targeted to children under 13 years following the rules when it comes to children's privacy and consumer protection laws? Our study shows that they are not.

The Current Study

We analyzed 750 mobile games across two major platforms and all three economic models to find out. Our sample included titles promoted on the Google Play "Teacher Approved" list and the Apple Store's "Kids & Family" list. Both lists are described as curated collections of titles that are age-appropriate and recommended for children.

Our comprehensive content analysis tracked the presence of ads and other commercial elements in 500 children's mobile games, in addition to 250 games previously analyzed. Our design analysis investigated the underlying software programs (i.e., code) of a subset of Android games. Our legal analysis examined the privacy policies of 54 premium games, 84 F2P games, and 2 freemium games (140 games total).

We looked at if and how the games' policies met the child privacy requirements established in three pieces of legislation: the Children's Online Privacy Protection Act (COPPA) (California, United States), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and Quebec's Act respecting the protection of personal information in the private sector (P 39.1).

Acknowledgement

This project was made possible thanks to financial support from the Office of the Privacy Commissioner of Canada (OPC) through its Contributions Program 2024-2025.

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Research Team

Maude Bonenfant, Full Professor in Social and Public Communication, Université du Québec à Montréal (UQAM)

Sara M. Grimes, Full Professor in Communication Studies, McGill University

Thomas Burelli, Associate Professor in Civil Law, University of Ottawa

Hafedh Mili, Full Professor in Computer Science, UQAM

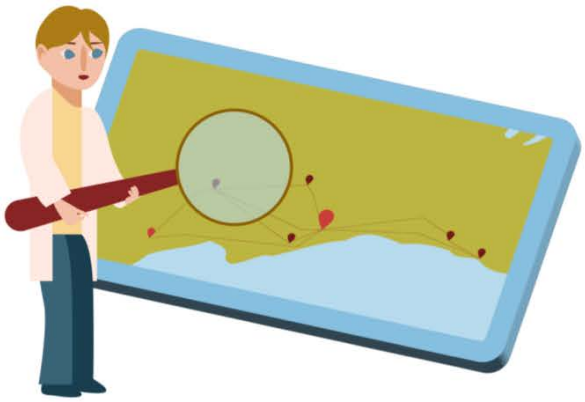
Here's what we found:

Sweeping non-compliance:

None of the 140 policies we analyzed fully meet the requirements of the Californian, Canadian, and Quebec legal frameworks. The policies of paid games were not of any higher quality or compliance than the freemium or F2P games. It is particularly worrying that none of the policies fully meet legal obligations, given that many of these obligations are not particularly demanding. The bar is relatively low, yet all these games failed to meet it.

Ratings vs. privacy policies:

Although we only looked at games that were rated as appropriate for children under 13 years, a huge number of their privacy policies listed the minimum age required to use the app at 13 years or even 18 years. This raises urgent questions about the privacy practices of these companies and if and how they are safeguarding younger users. This disconnect is problematic on many levels, as kids and parents are unlikely to read the privacy policy and very likely to assume apps classified by storefronts as child-friendly will be. Ratings and privacy policies need to be consistent when it comes to user age and comply with applicable regulations.



Lack of clarity on how data is used:

The privacy policies described a very wide range of uses for the data collected through game apps, some functional (e.g., user experience research to improve design) and some commercial (e.g., advertising, sharing data with other companies). Descriptions of how data is used are often vague. In fact, most policies were also unclear and inconsistent about what counts as personal or non-personal data. In some cases, data that would in some cases qualify as personal under existing privacy laws was miscategorized as non-personal (i.e., not protected).

Lack of clarity on how data is shared:

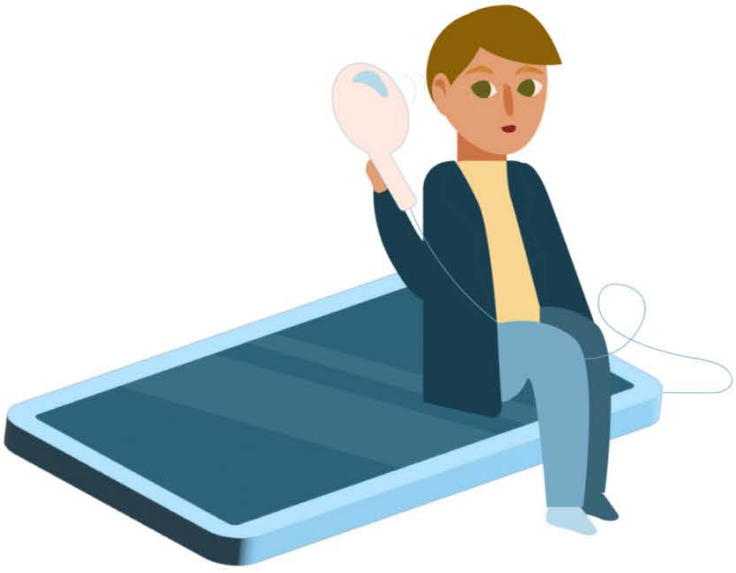
According to the privacy policies analyzed, a wide variety of third parties may have access to player data. This includes: Affiliated companies; Service providers; Marketing, advertising, and analytics partners; Public authorities; and Consultants (lawyers, bankers). In 52 policies, the third parties who (may) have access to player data are clearly specified. In many more (87) policies, however, they are not.

Parental consent?:

Although companies are supposed to seek parental consent before collecting data from or about kids, very few of the policies specified if or how this was done. Very few described renewing consent after changes are made to data practices– even though this too is mandatory.

Recommendations for Mobile Game Developers

1. Make sure your game, business operations, game rating, privacy and terms of service policies are all aligned when it comes to age and privacy protections. A game rated and promoted as suitable for children must ensure that its data, monetization, and privacy practices and policies comply with applicable child privacy and consumer protection laws.
2. Even so, remember that ratings are not enforceable and that kids often play games that are not rated "for" them. Act accordingly whenever this is discovered.
3. Higher standards need to be in place for in-game ads and monetization when children are involved. Children's best interests should always be prioritized. Consult existing age appropriate design guidelines for best practices.
4. Localize policies, practices, and jurisdictions to child players. For example, in Quebec, children under 14 years are protected by law C-25, which requires explicit opt-in consent for tracking.
5. During the development of apps for or otherwise used by children, use the Child Rights Impact Assessment (CRIA) tool to assess the potential impact of your game on children's rights. The tool and online training to use it are free and available to all. E.g. https://www.unicef.org/reports/mo-cria-child-rights-impact-self-assessment-tool-mobile-operators



RECOMMENDATIONS

PARENTS

Dangerous Game

Protecting the privacy of children under 13 years in mobile games

Mobile gaming is extremely popular among kids of all ages and around the world. But many of the games that kids play collect a lot of data from them – data that companies might then use to track and profile them, or even to persuade them to make purchases or play for longer than they want to. Previous studies show that this is even true in some games rated as appropriate for children aged 4 years and over.

Are mobile games targeted to Canadians under 13 (14 in Quebec) following the rules when it comes to children's privacy? Our study shows that many are not.

The Current Study

We analyzed 750 mobile games across two major platforms to find out. Our sample included titles promoted on the Google Play "Teacher Approved" list and the Apple Store's "Kids & Family" list. Both lists are described as curated collections of titles that are age-appropriate and recommended for children.

From this sample, we did a deep dive legal analysis of the privacy policies of 54 premium games, 84 free-to-play games, and 2 freemium games (140 games total). We looked at if and how these policies comply with relevant privacy laws in Canada, the US (where many tech companies are based), and Quebec. Here's what we found:

Sweeping non-compliance: None of the 140 policies we analyzed fully meet the requirements of all three legal frameworks.

Ratings vs. privacy policies: Even though we only looked at games that were rated by the app stores or ESRB as appropriate for children under 13 years, a huge number of the privacy policies we read stated that the minimum age to play was actually 13 years. Some said the minimum age was 18!

Lack of clarity on how data is used: The policies described collecting a wide range of types of data from players for an even wider range of uses. These descriptions were often vague and sweeping.

Lack of clarity on how data is shared: The policies suggest that a large number of third parties may also have access to your child's data. This includes affiliated companies, service providers, marketers and advertisers, among others. Most of the policies don't clearly specify who they share player data with.

Parental consent?: Although companies are supposed to seek parental consent before collecting data from or about kids, very few of the policies revealed if and how this was done. Have you ever actively consented to an app collecting your child's data?

UQÀM McGill uOttawa

Tips for parents

Talk to your kids about game apps and privacy.

Learning how and why games collect data helps build children's digital literacy. This in turn empowers kids to make better choices and to play a more active role in protecting their privacy. Kids also have insights and knowledge that can help build parents' digital literacies. Open communication about the privacy implications of mobile games can foster trust, cooperation, and family resilience.

Don't rely on content ratings alone.

When making decisions about which apps to buy, and before agreeing to buy or download one, make sure you (and your kids) read the privacy/ data use warnings on the app store and in the privacy policy. This information is usually found after the description, reviews and tech specs, and sometimes requires you to visit a company's website. Pay special attention to minimum age, the type of data collected and how it is used.

Review the privacy settings

on your child's device and accounts to make sure their data is protected and that apps don't have too much access. In addition to reviewing privacy and security settings, check access settings and permissions. Which apps have access to the device's camera, mic, or photos? Which apps are using geolocation features? Why? You might also consider deleting your child's Advertising ID.

Financial support for this project provided by the Office of the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Report worrisome data practices.

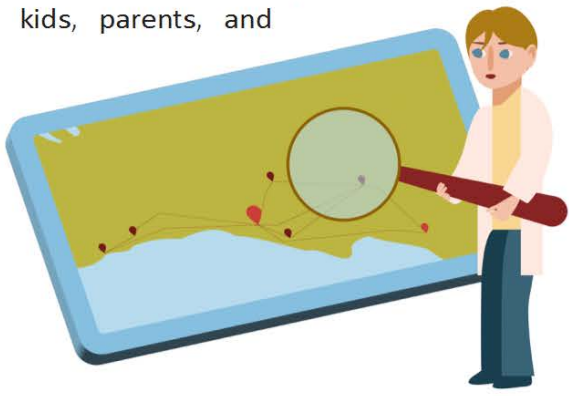
If you find a game or other app that is not complying with children's privacy laws or that you otherwise find to be concerning, be sure to report it. You can contact the developer to flag questionable practices or ask to see the data they've collected from your child or even ask to have it deleted. You can also file a complaint with federal and/or provincial privacy commissioners:

Call on regulators to strengthen children's privacy protections

Children's privacy protections in Canada are improving but there are still big gaps and lots of work to do. Other countries have much more robust protections in place, and some require companies to develop technologies with privacy-by-design, safety-by-design and children's rights at the forefront.

Watch this space

Our study is still underway, but we will soon be sharing the results of our content analysis of all 750 mobile games. This includes important findings about ads and monetization in children's games, and how these things connect to children's data and privacy. We're also working on recommendations and resources for rethinking how mobile games are rated and regulated in ways that put kids, parents, and privacy first.



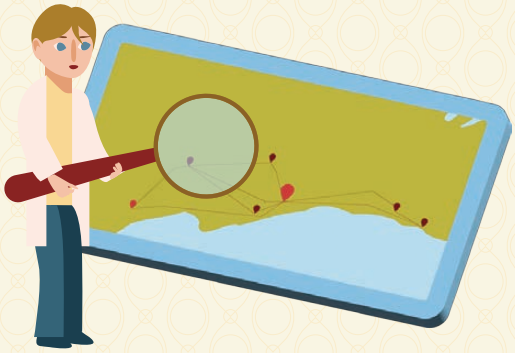
RECOMMENDATIONS

CHILDREN

A Dangerous Game

Mobile game apps are popular and fun to play. But did you know that many apps for kids are **breaking the rules** when it comes to your privacy? Rules that are in place to make sure your rights are protected and that your data isn't used against you?

We looked at the policies of **140 mobile games** to see how well they follow the rules about children's privacy in Quebec, Canada and the United States. Here's what we found.



- **None** of the games we looked at follow all of the rules when it comes to children's privacy.
- Very few games ask parents for permission to collect kids' data–even though they are supposed to.
- Companies must also tell kids and their parents about the types of data they collect and who they will share it with. But **most of them** either don't or are very vague about it.

- Some games **share and sell your data** with dozens of other companies. They use your data to **track you**, **watch** how you use your device, **see** what you buy, and more. Some might even use your data to try and trick you into **buying more stuff** or **playing for longer**.
- Many games that are rated for kids aged 4+ or 9+ actually ban players under the age of 13 years in their privacy policy. This means they might not be protecting kids' privacy at all.

We think apps and app stores need to do a better job when it comes to kids' privacy. Apps need to follow all the rules and respect kids' privacy rights. They need to tell kids and parents the truth about how they are collecting, using, and sharing your data.

UQÀM McGill uOttawa

Financial support for this project provided by the Office of the Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

2025.