YOUTH MEDIA
ALLIANCE
MÉDIAS JEUNESSE

DIGITAL TOOLKIT

A practical tool addressing the ethical and legal issues faced by producers of digital content for kids

Researcher & Author: Sabrina Dubé-Morneau

Translator: Lesley McCubbin

Contributors: Guillaume Aniorté, Christiane Asselin, Judith Beauregard, Chloé Benaroya, Chantal Bowen, Geneviève Brault, André H. Caron, Amy Dam, Sophie Dufort, Caroline Julien, François Larose, Jean-Phillipe Marin, Sandrine Pechels de Saint Sardos.

Thank you to CBC/Radio-Canada's Linguistic Services Department, Nathalie Jackson from Quebec's Office de la protection du consommateur, TVO's Jessica McLaughlin, and Myriam Amzallag from Université de Montréal's Center for Youth and Media Studies.

DIGITAL TOOLKIT

The Digital Toolkit was designed as a clear, concise response to the issues and challenges faced by youth content producers working on digital platforms.

Created by specialists in the production and distribution of content for the very youngest audiences, the kit pragmatically explores the ethical and legal questions — safety, moderation, online payment, advertising, marketing, personal information and more — that arise when operating a kids' website or mobile app on the Canadian and international markets.

Each backgrounder also offers recommendations formulated by the editorial team and validated by the legal team to help producers adopt best practices in the field of youth digital media.

October 19, 2015

Main Sponsors

Funding for this digital toolkit was provided by Ontario Media Development Corporation and the Canada Media Fund. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Ontario Media Development Corporation, Canada Media Fund, the Government of Ontario or the Government of Canada. The funders, the Governments of Ontario and Canada and their agencies are in no way bound by the recommendations contained in this document.

Additional funding provided by the Bell Fund, the Canadian Media Production Association, Bereskin & Parr and mbiance.

© YMA All rights reserved 2015

ABOUT

Over the past decades, Canadian producers and broadcasters have developed unique know-how and expertise when it comes to creating and broadcasting quality children's programming. This quality is apparent not only in the production values invested in youth content, but also in a profound respect for young viewers and their right to high-calibre television productions. Promoting the highest standards in Canadian youth production has always been a key part of our mission at Youth Media Alliance, a commitment enshrined in our Quality Charter.

With the proliferation of digital technologies, we felt it was just as important to adopt these same high standards for the new media sector. From virtual communities, personal data and privacy, to social networks, online advertising and user-generated content, new forms of communication are now part of children's daily lives. But there are also new rules and regulations that must be followed if we want to guarantee the same level of quality and excellence in our offering to young audiences.

This Digital Toolkit is therefore a valuable resource that will help guide you through the various content and platform types, providing advice and references on the current state of the regulatory landscape both in Canada and abroad (the United States, the European Union, France and Australia). It also underscores specific legislation like the U.S. Children's Online Privacy Protection Act or Québec's Consumer Protection Act that may have a broader scope in certain contexts. We are also committed to updating the kit regularly to keep pace with the changing digital media and content environment. Developed jointly with industry-leading youth content producers and broadcasters, this kit complements YMA's Quality Charter, which now covers digital media and new distribution platforms.

We hope it serves you well!

Guillaume Aniorté,
VP / Strategic Development & Acquisitions
Frima

For over 25 years, Université de Montréal's Center for Youth and Media Studies (CYMS) has worked to better understand and harness the potential of conventional media and digital environments for young people at home and abroad. Throughout these years, we've enjoyed a highly productive relationship with Youth Media Alliance, conducting innovative research that has not only yielded valuable scientific insights, but has also translated into practical applications in the professional market.

This new "Digital Toolkit" is yet another shining example of what the creative, production and scientific research sectors can accomplish by working together.

André H. Caron,
CYMS Director
Université de Montréal

Ever since this project got under way, everything has moved very quickly.

If we hadn't all shared the same vision and commitment, The Digital Toolkit wouldn't even be a shadow of what it is today. Your unwavering cooperation, enthusiasm and support were critical to its success. We're grateful to the Ontario Media Development Corporation, the Bell Fund, the Canada Media Fund, and the Canadian Media Production Association.

Youth Media Alliance would also like to highlight the outstanding contribution of Guillaume Aniorté and the team of producers and broadcasters who shared their insights during the project's planning and drafting phases.

Thank you as well to our web and legal partners, mbiance and Bereskin & Parr, for their valuable assistance.

Lastly, special thanks go to André Caron, Director of Université de Montréal's Center for Youth and Media Studies, who found the ideal person to help us with a project of this magnitude – Sabrina Dubé-Morneau.

Kudos, Sabrina! Your enthusiasm, good humour and thoroughness in developing The Digital Toolkit were appreciated by all.

Allow me to express my deepest gratitude and warmest regards to everyone who made this project a reality.

Chantal Bowen,
Executive Director,
Youth Media Alliance

TABLE OF CONTENT

BACKGROUNDER 01. COLLECTION OF PERSONAL INFORMATION

Explains the term "personal information" and the legal framework governing the collection and handling of such data when a user population includes children.

DEFINITION

1.1 What is personal information?

Any personally identifiable information about an individual; i.e. information that, alone or in combination with information from other sources, could lead to the identification of that person*:

- Last name and first name
- Physical address, including the name of the street, neighbourhood or city
- Online contact information (e.g., email address, instant messaging ID)
- Telephone number
- Place and date of birth
- Social insurance number
- Audio, video or photographic documents containing the person's likeness or voice
- Geographic location information, including GPS data
- Persistent identifiers, such as IP, MAC addresses or a cookie number, unique device identifier for telephones and tablets, etc.
- Data on the individual's online activity, browsing history, bookmarks
- Data created by the user or social networks, e.g. comments, reviews, "Likes," Twitter feeds, interactions with customer-service pages

Information about an individual can be divided into two types of identifier:

- **Direct identifiers**: last name and first name, social insurance number, photo or video, etc.
- **Indirect identifiers**: date and place of birth, mother's maiden name, school name, school board name, teacher's name, etc.

***Beware** of the risk of re-identification of anonymized data: discrete elements of information from several sources, when combined, can lead to creation of detailed profiles that can be used to identify someone.

1.2 What are metadata?

Metadata are data that lend meaning and context to other data. Often, this means usage statistics about your product, like the number of tries that it took a user to complete a level in a game.

Anonymized metadata, i.e. **data stripped of direct and indirect identifiers, are not considered personal data.** For example, you can use and analyze the city of residence of competition entrants as long as you dissociate it from the direct and indirect identifiers. Use of anonymized metadata does not require consent.

1.3 What is meant by "collection of personal information"?

This refers to all practices surrounding the handling of users' personal data; in other words, the actual gathering of the data, but also use and storage as well as sharing and/or sale of the data with/to a third party.

REGULATIONS

Among Canada, the United States, the European Union (EU), France and Australia, only the United States has specific legislation governing the collection of personal information about children under 13 years of age.

Canada, the EU, France and Australia all deal with the issue of personal information under general-scope laws covering the entire population. Each of these laws applies to companies doing business in the respective territories.

CANADA

Personal Information Protection and Electronic Documents Act (PIPEDA)

Federal statute defining the rules for the personal information handling practices of private-sector organizations. Under PIPEDA, every private-sector company must obtain valid or meaningful consent to collect, use or share personal information. In addition, the company must **notify any individual affected by the theft or loss** of personal information, indicating whether there is a risk of harm (e.g. identity theft) and informing them of the safeguards they can apply. Furthermore, the company must **report the incident** to the Office of the Privacy Commissioner of Canada.

Companies must use clear and simple language to ensure that vulnerable Canadians, **particularly children**, fully understand the possible consequences of sharing their personal information online.

Careful! The Act does not apply to companies operating exclusively in a province that has essentially similar provincial legislation:

- Alberta
- British Columbia
- Québec

Additional information:

Office of the Privacy Commissioner of Canada:

Securing Personal Information: A Self-Assessment Tool for Organizations

Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law that sets high standards for the protection of personal information about children collected online. Its goal is to enable parents to supervise personal information handling practices with respect to their children under 13 years of age.

It applies to products that collect personal information about U.S. children under 13 years of age, **including collection by companies based outside the U.S.** and **products for use by the general public** that include U.S. children aged under 13 among their users (i.e. casts a wider net than youth products).

- If you know that you are collecting personal information about U.S. children under 13 years of age, you must **obtain verifiable parental consent before beginning collection**.
- If you make any changes to the practices to which the parent has consented, you must notify the parent in a direct notice and again request their verifiable parental consent before resuming collection.
- Upon request from a parent, you must be able to provide:
    - A description of the personal information collected about the child and a clear explanation of how it is used, stored and shared.
    - The opportunity to revoke consent, refuse any further use and collection of the child's personal information, and have previously collected information deleted.

Additional information:

Federal Trade Commission (FTC): COPPA Rule: A Six-Step Compliance Plan for Your Business

FTC: Complying with COPPA: Frequently Asked Questions

FRANCE

Act on Information Technology, Data Files and Civil Liberties

Law defining the principles with which companies must comply when collecting, handling and storing personal information. It covers companies that do business in France or conduct data processing there.

Before collecting any personal information online, you must **make a declaration stating each purpose for which personal data is processed** to the Commission nationale de l'informatique et des libertés (CNIL). This must be validated by issuance of a registration number to be posted on your website along with contact information for the department that will be handling the data.

This law **forbids collection by illegal means.** For example, cookies may only be installed on a user's browser if they agree to it beforehand (opt-in basis).

Additional information : Commission nationale de l'informatique et des libertés

EUROPEAN UNION

Directive on Protection of personal data

Directive on Privacy and Electronic Communications

These directives frame privacy protection for residents of the EU and cover companies that do business in one or more EU Member States.

Safe Harbor Framework: This is a **joint U.S.–EU program** under which **U.S. companies** are required to comply with European confidentiality principles when handling European data. It **does not apply to Canadian companies** because the EU considers **Canada's legal framework for privacy protection to be compatible with its own framework.**

Additional information: Handbook on European Data Protection Law

AUSTRALIA

Privacy Act

Federal law, general in scope, on the protection of personal information as it affects companies engaged in business activities in Australia. It states that a company must have an easily accessible privacy policy explains its overseas data disclosure practices.

Additional information: Office of the Australian Information Commissioner: Privacy law reform

MOBILE APPLICATION DISTRIBUTION PLATFORMS

Apple App Store

The App Store has a Kids section featuring applications for young users. Developers wishing to distribute apps through that section of the store must comply with specific rules, including:

- Incorporating a mechanism allowing the user to provide their date of birth so as to comply with COPPA
- Obtaining parental consent or using a parental gate before allowing the user to link out of the app and/or engage in commerce

Additional information

Amazon Appstore

Amazon rates the applications in its Appstore using a number of parameters to define appropriate ages for each. Various criteria serve to safeguard children's privacy: for example, apps rated "All Ages" cannot collect personal information or use location data.

Apps for children aged under 13 cannot link to the Amazon Mobile Ad Network because it uses behavioural advertising, which is forbidden under COPPA.

Additional information:

- FAQ
- App Distribution and Service Agreement

Google Play store

Google Play uses a content-based applications rating system. A number of child privacy safeguards have been implemented; for example, an app that can be used to locate a user cannot be rated for "Everyone." These instructions apply to all of an app's content, including user-generated content and embedded ads.

Additional information:

- Google Play Content ratings for apps & games
- Google Play Developer Program Policies
- Developer Distribution Agreement

SELF-REGULATION

This backgrounder does not address self-regulation since the collection of personal information is an area well covered by legislation.

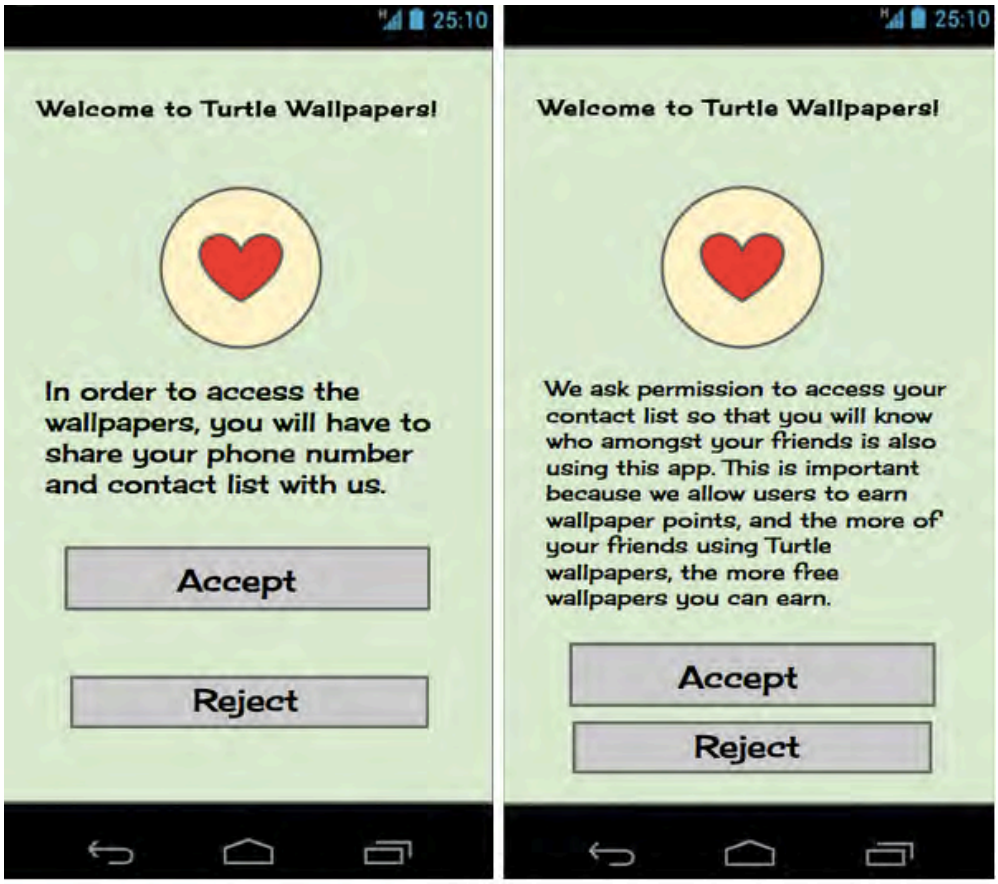
OUR RECOMMENDATIONS

- Prefer a transparent approach: **post a privacy policy even if you do not collect any personal information**.
- Do not require users to provide any more personal information than is necessary to take part in an activity. For example, if possible, give children the option to not identify themselves and/or use an alias.
- Make sure your privacy policy is visible and easily accessible: use a large typeface and/or a contrasting colour.
- Ensure your privacy policy is **up to date,** and provide clear, concise explanations of your personal data collection and handling **Avoid legal jargon and superfluous information**.
- Your privacy policy should provide the names of any third parties that collect personal information using your product.
- Periodically review the personal information handling practices of service providers and third parties with whom you share data.
- Although you are not required to obtain parental consent to use anonymized metadata, we do recommend that you explain this practice transparently in your privacy policy.
- Obtain parental consent **before** beginning collection. Provide parents with a link to your privacy policy to help them provide informed consent.
- Use personal information solely for the purposes for which parental consent has been secured.

- Avoid collecting precise location data on the child. If such data are necessary for your product to function, explain to parents why this is so and for what purposes location data will be collected, and obtain verifiable parental consent.
- **Help the child understand what will be done with their personal information**; for example, if the product is about to use the location data, a symbol can be activated to alert the user to what is happening.
- You must be able to provide access to the personal information collected about a child to parents who request it. Explain the procedure for doing so in your privacy policy.
- Notify parents of any changes you make to your personal information handling practices.
- Implement procedures to protect the confidentiality, security and integrity of the personal information that you store. In the event that the data are compromised, notify parents and explain what actions you are taking to remedy the situation.
- Delete all data that you no longer need.
- ***United States***: COPPA requires the implementation of mechanisms such as verifiable parental consent. There are FTC-approved accreditation programs that can help you achieve compliance.
    - iKeepSafe
    - Privo

MOBILE

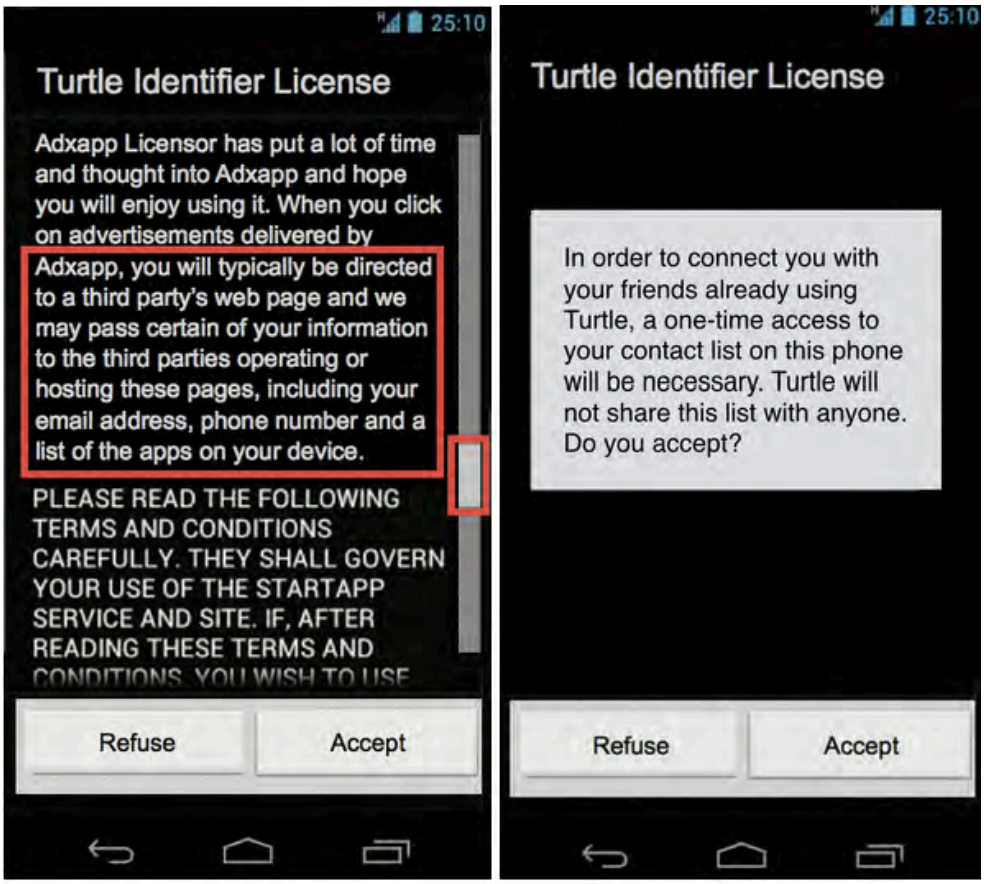
- Inform users of the data required by the application and explain why they are required.
- Post a simple, clear notice explaining how the personal information will be used.
- Obtain the user's consent when the application is first launched: present the notice in a dialogue box prompting the user to agree to the conditions before using the app:



1 2

1. NO: The information is hidden in the EULA (End-User Licence Agreement). The user has to scroll far enough to find it.
2. YES: The information is presented up front, transparently and clearly. The user doesn't have to go looking for it.

- Make sure the information on collection of personal information remains available in the privacy policy and/or easily accessible via a link on the home screen or the section reserved for parents.
- It is your obligation and responsibility to understand users' rights and comply with local laws wherever your product is available via an online app store.



3 4

3. NO: Explains how the app uses the information, but doesn't state clearly how it will be used and why it will be collected.
4. YES: Clearly states why the app must access personal information, how it will be used, and why.

**Images from Android Developer Console Help

Bibliography.

BACKGROUNDER 02. PARENTAL CONSENT

Introduces and explains the concept of "consent."

DEFINITION

1.1 What is consent?

Consent essentially consists of granting permission. Under the law, for **consent to be valid or meaningful**, it must result from **an informed decision**based on the person's full understanding of why their consent is being requested.

The ability of children to provide meaningful consent depends greatly on their level of cognitive and emotional development. It can be **unrealistic to expect a child to understand the complexities and potential risks associated with certain online practices**. Accordingly, in some cases it may be preferable to obtain valid consent through an authorized person like a parent or legal guardian.

1.2 Types of consent and ways of obtaining it

Consent falls into two main categories:

- **Express** (explicit): the user grants consent explicitly through a specific action (e.g. an electronic signature) that indicates their understanding of what they are consenting to.
- **Implicit** (tacit): when consent may be reasonably inferred from the circumstances of a particular situation, relationship or transaction. For example, consent can be implied from an existing business relationship with the user.

There are various mechanisms for obtaining consent, based on the situation:

- **Positive** (opt-in): a specific action on the part of the user to express positive agreement to the identified purpose (e.g. "If you agree to let your child participate in our contest, check this box.")
- **Negative** or passive (opt-out): a specific action on the part of the user to express non-agreement to the identified purpose (e.g. "Your child would like to enter our contest. If you do not consent to this, check the box.")

1.3 What is parental consent?

Parental consent is when the parent or legal guardian provides the producer or operator with the authorization needed to allow the child to engage in certain activities.

When is it required? While regulations can vary between countries, parental consent is rarely required by law. However, the law often encourages producers to seek parental consent for anything involving the collection of personal information.

1.4 What is "verifiable" parental consent?

Verifiable parental consent aims to have the producer adopt measures that are reasonably calculated to ensure that the person providing the consent is indeed the child's parent. One such measure is to have parents call a telephone number staffed by trained personnel.

1.5 What is direct notice to parents?

Direct notice is when the producer contacts the parent, normally through the email address provided by the child. Direct notices are used for various reasons, but generally to seek parental consent or to inform parents of changes to practices to which parents have previously consented.

1.6 The right to revoke consent

Parents have the right to revoke their consent. Doing so prevents the future collection and use of personal information and in some cases, allows previously collected information to be deleted.

REGULATIONS

In the digital space, the notion of consent is most commonly linked to **personal information handling practices** and online transactions. For more information on the regulatory framework governing online consent, consult backgrounders Collection of personal information and Online transactions.

The United States is the sole country among those presently studied with specific legislation (COPPA) based on obtaining verifiable parental consent to collect personal information about children under 13 years of age.

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

COPPA is a federal law that protects the privacy of children under 13 years of age. **Based on verifiable parental consent**, its goal is to enable parents to supervise and intervene in the online collection of personal information about their children. It applies to products that collect personal information from U.S. children under 13 years of age, **including collection by companies based outside the U.S**.

Before collecting any personal information about a child, you must send a **direct notice** to the parents. The direct notice must:

1. State that you are contacting them for the purpose of obtaining their consent
2. State that you wish to collect personal information about their child
3. State that their consent is required for the collection, use and disclosure of this information
4. Specify the type of information you wish to collect and how it will be shared
5. Include a hyperlink to your privacy policy
6. Indicate the means by which the parent can provide their consent
7. Indicate your time frame for deleting their online contact information from your records should you fail to secure their consent

Since children are quick to learn how to bypass typical parental consent mechanisms, **the law requires you to take "reasonable measures" to ensure that it is the parents you have contacted**. COPPA sets forth a number of non-exhaustive options for obtaining verifiable parental consent — for example, mailing parents a consent form to be signed and returned.

Should you make changes to the personal information handling practices for which consent has previously been secured, you must **notify the parent with a direct notice and again request their verifiable parental consent** before resuming collection.

For more information on verifiable parental consent and direct notice under COPPA

MOBILE APPLICATION DISTRIBUTION PLATFORMS

App stores incorporate parental consent systems but disclaim any responsibility regarding compliance with different privacy policies. Because of this, you must ensure that your product complies with the regulations in effect wherever it is available.

OUR RECOMMENDATIONS

- Parental consent and direct notices are useful tools for building and maintaining relationships of trust with parents. Obtain **parental consent** for:
    - Collecting personal information about a child
    - Contest participation
    - Social media allowing users to exchange content
- Parents must provide express consent for all online transactions carried out using their credit card.
- Use a **direct notice** to maintain contact with parents and keep them informed in the event of any changes to your practices.
- **Email is an effective way of obtaining parental consent**. Before children can access your services, ask them to provide their parents' email address. Then send the parents a message **clearly and concisely presenting the information that will allow them to provide informed consent along with a link to your privacy policy.** For example, if you are contacting them about a contest, include the contest rules and other conditions. In

answering the email, the parent either provides or withholds their consent. This will determine whether or not the child can access your service.

- Parental consent for the collection of personal information and privacy policies go hand-in-hand. In your policy, clearly and concisely present all the information needed to enable the parent to provide informed consent.
- **Direct notices to parents must be concise and clearly worded**: avoid legal jargon and superfluous information.
- Remember that parents have the right to revoke their consent: indicate your procedures for doing so in your privacy policy.
- ***United States*:** If your product is used by U.S. children aged under 13 and you collect personal information, **COPPA requires that you provide a mechanism for obtaining verifiable parental consent. If possible, incorporate this mechanism during the product development phase**, since this will be easier than trying to do so once your product is finalized.
- ***United States*:** various COPPA accreditation programs approved by the Federal Trade Commission (FTC) can help you achieve compliance with verifiable parental consent: iKeepSafe, Privo
- If you distribute content through a mobile app market and use that market's parental consent mechanism, stay abreast of local regulations and how they affect consent.

Bibliography.

BACKGROUNDER 03. PRIVACY POLICY

Explains what a privacy policy is and what it must include.

DEFINITION

1.1 What is a privacy policy?

A privacy policy is a legal document whose purpose is to inform your users about your personal information collection and protection practices.Having a privacy policy that's easy to find, uses clear and comprehensible language and is transparent about personal information handling practices is an excellent means for a youth enterprise to gain parental trust.

1.2 What information should a privacy policy include?

Your privacy policy should clearly lay out your practices concerning how you handle personal information (collection, tracking tools, usage, sharing, protection, storage, deletion, etc.). **The challenge lies in presenting this mass of information concisely and in terms simple enough for the average consumer to read and understand.**

While there is no one universal approach, your communication style must be appropriate to your audience and the nature of your platform. For youth production professionals, this could mean adapting your level of language (i.e. avoiding legal jargon) and limiting the information you provide to only what is strictly necessary (i.e. excluding superfluous information).

See our recommendations for more on what your privacy policy should contain.

1.3 Where should the privacy policy be posted?

Privacy policies are generally posted on the home page. For mobile apps, if the distribution platform allows this, you can include a link to your privacy policy on your product description page. This shows transparency, since you are enabling parents to consult your policy before downloading your app. You can also post it in a dialogue box that appears when users visit for the first time.

Regardless of the platform, the privacy policy must be easy to find: users shouldn't have to go looking for it.

REGULATIONS

The privacy policy is a **universal tool** that works in tandem with parental consent for the collection of personal information. Producers must assume that the user's consent rests on their full understanding of the information contained in the policy. Every country requires websites who

collect personal information to post a privacy policy; however, the **United States imposes stricter requirements as to what the policy must include.**

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law to protect personal information about children collected online. COPPA applies to products that collect personal information from U.S. children aged under 13, **including collection by companies based outside the U.S.**

Under COPPA, your privacy policy must be clear and easy to read. The policy must **feature on the home page** and **in each section where personal data is collected**. Links to your privacy policy must be readily apparent (a link in small font at the bottom of the page is not considered "apparent"). **Your policy cannot include promotional materials**.

The contents of a COPPA privacy policy are divided into three main categories:

- The **contact information of third parties** who collect personal information through your platform
- A description of the personal information you collect and how you use it
- A description of **parents' rights** and the procedures to follow to exercise these rights

For details on what to include in a COPPA privacy policy, see our recommendations.

Additional information:

Federal Trade Commission: COPPA Rule: A Six-Step Compliance Plan for Your Business

iubenda: service for generating COPPA-compliant privacy policies

CANADA, EUROPEAN UNION, FRANCE & AUSTRALIA

All of these countries require you to post a clearly intelligible privacy policy describing your personal information handling practices.

Additional information per country:

Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

Office of the Privacy Commissioner of Canada, Getting Accountability Right with a Privacy Management Program

Office of the Privacy Commissioner of Canada, Mobile – Good Privacy Practices for Developing Mobile Apps

France: Act on Information Technology, Data Files and Civil Liberties

Commission nationale de l'informatique et des libertés (CNIL), Rights and Obligations

European Union: Directive on Privacy and Electronic Communications

European Union Agency for Fundamental Rights, Handbook on European Data Protection Law

Australia: Privacy Act

Office of the Australian Information Commissioner: Privacy law reform

MOBILE APPLICATION DISTRIBUTION PLATFORMS

Apple App Store

Apple **requires apps in the Kids Category to display a privacy policy** that complies with applicable local children's privacy laws.

Additional information

Amazon Appstore

If you and/or any third party plug-ins or services you use collect personal information, **you must provide *legally adequate* privacy notices.**

Additional information

Google Play

Google asks you to publish a disclosure informing users what information the app would like to access and how such information will be used.

Ensure that users are aware of this by putting your disclosure in a prominent place. Display your disclosure in an **End User License Agreement (EULA) so that the user can provide their consent at first launch**. The disclosure should be clear and succinct and **displayed in a modal window that asks the user to consent to the terms** before using the app.

Additional information

OUR RECOMMENDATIONS

- **The privacy policy is a legal document: consult a professional to ensure that your policy adequately covers your platform.**
- **The privacy policy must cover the following:**
- Your company's contact information
- A description of the types of data collected and the methods used to collect them (e.g. children's information, use of cookies, etc.)
- The reasons why you collect information
- How the information will be applied (e.g. used to inform contest winners)
- How the information will be safeguarded
- How long you intend to store the information
- Practices from which the user can withdraw (e.g. behavioural advertising)

- For data shared with third parties:
    - Type of business or service (e.g. web analytics)
    - The third party's use of the data gathered
- ***COPPA policies must also include:**
- **A complete list of all third parties who collect personal information through your platform**, including contact information (address, telephone number, email)
- A description of **parents' rights** and the procedures to follow to exercise them. These rights stipulate that:
    - The child will not be asked to provide more data than is reasonably required to participate in an activity.
    - Parents can consult the data collected on their child, ask to have them deleted and refuse future collection.
    - Parents can agree to have their child's data collected and used but withhold their consent to have the information shared with third parties.
- **Find ways of inciting the user to consult your policy. For example, use illustrations that convey the essentials of your privacy parameters, with a link to detailed explanations.**
- You should still post a privacy policy even if you do not collect personal information.
- Ensure that your privacy policy is easily accessible from your home page or home screen.
- Though the information it contains should be presented as concisely as possible, your privacy policy can also be used to share any other specifications about user information. For example:
    - Though metadata do not qualify as personal information, you can include an explanation of how you use them.
    - Indicate whether your platform allows children to make information publicly accessible — a particularly crucial consideration for sites with community features like bulletin boards, forums, chat rooms or text fields to be filled in (e.g. "Describe your character").
    - Explain how users can access the personal information you have about them.
- Periodically check your personal information handling practices to ensure they continue to align with your privacy policy.
- Transparency in personal information practices is a dynamic process that doesn't stop once the privacy policy has been posted. Update your policy as needed.
- Include the date of the most recent update at the end of the policy.
- Find ways of informing users of any updates to your privacy policy.

*****MOBILE*****

For ease of reading on the small screen, draft your policy using a layered or "tiered" approach, stating the most essential information up front with links leading to the specifics.

Bibliography.

BACKGROUNDER 04.
USAGE ANALYSIS AND TRACKING DATA

Explains usage analysis, tracking data and tracking tools.

DEFINITION

1.1 What is "usage analysis"?

It's when data collected from users and generated by their interactions with your platform are analyzed based on specific objectives like assessing the platform's effectiveness, quantifying usage with statistical reports, personalizing the user experience or optimizing marketing efforts.

Different data will be harnessed based on the analysis to be performed: personal information provided by the user, data from user interactions with the platform or other data collected by **web analytics tools** like Google Analytics or Flurry.

1.2 What are "tracking data"?

These are data that track user activity through time and across platforms, **thus enabling in-depth analysis**. For example, by analyzing a user's browsing history, content can be personalized according to their preferences. Tracking data are collected through **the device's unique identifier** or via tracking (monitoring) tools. Below are the most common:

- **Cookies** (also called web cookies, browser cookies or HTTP cookies): small encrypted text files placed by a website on a user's hard drive that let the website identify the user and track the browsing history. A given website can have different kinds of cookies. **First-party cookies** come directly from the publisher's domain, whereas **third-party cookies** come from other domain sources (g. an advertising network or web analytics service) and are embedded in the actual page the user is visiting.
- **Web beacons** (also known as web bugs, pixel tags or clear GIFs): typically a transparent graphic image coded into a web page. Web beacons monitor the user's journey through a single website or series of sites and can be used in combination with cookies.

The device's unique identifier and the tracking tool both have a **persistent identifier** that **identifies a user through time and across platforms**.

REGULATIONS

Apart from the United States, usage and user activity analyses are fairly unregulated. In general, the explanation provided in your privacy policy on how you use the data collected, including tracking data, is sufficient. **The use of tracking tools is restricted by law** in certain countries.

CAREFUL!! Click **here** for information on **profiling for behavioural advertising**.

CANADA

Personal Information Protection and Electronic Documents Act (PIPEDA)

Federal statute defining the rules for the personal information handling practices of private-sector organizations in the course of commercial activities. You must obtain valid or meaningful consent to collect, use or share personal information, **regardless of the collection technology used**.

Canada's Anti-Spam Legislation (CASL)

Federal law establishing the regulatory framework for the sending of commercial electronic messages and the installation of computer programs as part of business activities. It is prohibited to install software on a user's computer system without obtaining their consent. However, **you do not need consent to install a cookie, HTML code or Java Scripts.**

Additional information:

Office of the Privacy Commissioner of Canada: Securing Personal Information: A Self-Assessment Tool for Organizations

Canada's Anti-Spam Legislation

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law to protect personal information about children collected online. COPPA applies to products that collect personal information from U.S. children aged under 13, **including collection by companies based outside the U.S.**

You are responsible for all personal information collected through your platform, **including any collection by third parties.** Because of this, you must**choose services that comply with COPPA**. For example, on mobile platforms, the SuperAwesome advertising network and analytics tools Flurry and PreEmptive Solutions are COPPA-compatible.

If **the persistent identifier is the only personal information** collected and **is needed to support the platform's internal operations**, **you do not have to seek verifiable parental consent**. COPPA defines "internal operations" as the activities necessary for:

- Maintaining or analyzing the functioning of the site or service
- Performing network communications
- Authenticating users or personalizing content

- Issuing and/or capping the frequency of contextual advertisements
- Protecting the user's security or integrity
- Ensuring legal or regulatory compliance
- Fulfilling a request from a child

If you and/or a third party use a **persistent identifier for purposes other than to *support internal operations*** — for instance, for **behavioural advertising**, **you must obtain verifiable parental consent** prior to collection and **provide a clear explanation of your practices in the privacy policy**.

Additional information:

Federal Trade Commission: COPPA Rule: A Six-Step Compliance Plan for Your Business

FRANCE & THE EUROPEAN UNION

Directive on Protection of personal data and Directive on Privacy and Electronic Communications

These directives frame privacy protection for residents of the European Union and cover companies that do business in one or more EU Member States. France's *Act on Information Technology, Data Files and Civil Liberties* is based on these directives.

Tracking tools are authorized provided you obtain the user's consent and **offer them the option to refuse**. Information on the installation of tracking tools along with the right to refuse should be offered the first time the user connects and cover future use. **You are also responsible for the collection of information by third-party cookies**.

Cookies that facilitate navigation (e.g. user authentication, content personalization, shopping carts) constitute an exception: **they do not require consent.**

Additional information:

European Agency for Fundamental Rights, Handbook on European Data Protection Law

Act on Information Technology, Data Files and Civil Liberties

AUSTRALIA

Privacy Act

Federal law, general in scope, on the protection of personal information as it pertains to companies that do business in Australia.

If you collect personal information using a tracking tool, you must inform the user — a notice on the home page is sufficient — and explain what the information is used for in the privacy policy. Consent is not required.

Additional information : Office of the Australian Information Commissioner, The Privacy Act

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Amazon Appstore

The app distribution agreement states that Amazon reserves the right to "modify and add to your Apps so that we can collect analytics."

Additional information : Amazon Appstore App Distribution Agreement

SELF-REGULATION

The Digital Advertising Alliance of Canada

This organization advises its members not to use tracking tools or any other means to gather data liable to be used for behavioural advertising with children known to be under 13 years of age.

Additional information on Canadian self-regulatory principles for online behavioural advertising

OUR RECOMMENDATIONS

- If your practices involve the collection of personal information and/or tracking data, explain how they apply to usage and activity analyses in your privacy policy.
- Provide users with clear notification if your platform uses tracking tools.
- A banner on the home page specifying that the site uses cookies, providing a clickable link

to the privacy policy and specifying that continued navigation will be taken as the user's

consent to the use of cookies.

- Offer parents the right to refuse consent to the use tracking tools.
- The means used to communicate with parents and offer the right to refuse consent should be as user-friendly as possible.
- Be transparent regarding your use of tracking tools: on your privacy policy, describe your information collection practices and provide the names of third-party operators who use tracking tools through your platform.
- Keep the number of tracking tools on your platform to a minimum.
- If you accept plug-ins (additional software), verify whether they incorporate tracking technologies. If so, draw up agreements to restrict the collection of tracking data.
- Periodically review the terms and conditions of service and the privacy policies of any third parties on your platform to ensure that their practices meet your requirements.
- **Careful!!!** If you use **tracking data** for the purposes of **profiling** and/or **behavioural advertising**, be sure to consult our backgrounder on this topic.
  Bibliography.

BACKGROUNDER 05.
ONLINE BEHAVIOURAL ADVERTISING

Explains online behavioural advertising and profiling.

DEFINITION

1.1 What is online behavioural advertising?

It's the collection of tracking data through tracking tools that record users' online activity and habits through time and across non-affiliated websites. The data gathered are used to **infer the user's preferences with a view to showing them ads that may interest them** (known in the industry as "interest-based ads"). Such practices allow companies to deliver advertisements or content they believe to be more relevant to the user.

Online behavioural advertising raises **ethical questions** since the data on which it is based are often collected without the user's knowledge.

1.2 Profiling

Profiling consists of aggregating data from various sources (tracking tools) to build a user profile. Tracking data are combined with other types of information to create detailed profiles. Two elements make **profiling** possible: the **persistent identifier** that's part of the device's unique identifier; and the **tracking tools that recognize a user through time and across websites**. The more **third-party cookies** there are on sites visited by the same user, the more detailed that user's profile will be.

Profiling is one of the **cornerstones of digital marketing**. It is used to detect market trends **as well as for behavioural advertising**.

REGULATIONS

Apart from the province of Québec, most countries monitor advertising through self-regulatory programs. However, since behavioural advertising is based on collecting user data, it is also covered by laws that govern the protection of personal information.

CANADA

Personal Information Protection and Electronic Documents Act (PIPEDA) — Policy Position on Online Behavioural Advertising

Federal statute defining the rules for the personal information handling practices of private-sector organizations in the course of commercial activities. The **Policy Position on Online Behavioural**

Advertising represents the application of PIPEDA to the collection and use of **data** for the purposes of online behavioural advertising.

PIPEDA considers data collected for such purposes to be **personal information**. Accordingly, you must **obtain valid or meaningful consent** to collect such data; you must also give the user a chance to opt out. PIPEDA **does not refer to specific age thresholds for providing consent**, but underscores that practices need to correspond to the user's cognitive and emotional development.

Children's personal information **should not be tracked for the purposes of behavioural advertising.** This practice is deemed inappropriate, since children cannot be expected to understand or appreciate the issues associated with tracking their data and are thus unable to provide meaningful consent. Simply put, platforms aimed at children **should avoid including any third-party tracking technologies.**

****QUÉBEC: Consumer Protection Act**

Québec's *Consumer Protection Act* prohibits commercial advertising directed at children aged under 13, **regardless of the platform, barring certain exceptions prescribed by regulation.** Accordingly, it is **prohibited to use data from Québec children under 13 years of age for the purposes of behavioural advertising**. This prohibition is also applicable to companies based outside the province. For more information about advertising directed at children in Québec, click here.

Additional information:

Office of the Privacy Commissioner of Canada: Policy Position on Online Behavioural Advertising

Consumer Protection Act – Advertising Directed at Children Under 13 Years of Age

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law that governs the online collection of information about children. It applies to products that collect personal information about U.S. children aged under 13, **even if the company in question is based outside of the U.S.**

COPPA does not consider **behavioural advertising** as **necessary to supporting internal operations**). Consequently, if you and/or a third party **collect data for the purposes of behavioural advertising**, you must **obtain verifiable parental consent before starting collection**. Furthermore, you must clearly outline your practices linked to behavioural advertising in your privacy policy.

Seek COPPA-compliant services. For example, for mobile apps can use the "kid-safe" marketing platform SuperAwesome as well as the analytics services Flurry and PreEmptive Solutions.

*The U.S. self-regulation program Your AdChoices is similar to its Canadian counterpart AdChoices.

Additional information:

Federal Trade Commission: COPPA Rule: A Six-Step Compliance Plan for Your Business

Your AdChoices

EUROPEAN UNION & FRANCE

Directive on Protection of personal data and **Directive on Privacy and Electronic Communications**

These directives frame privacy protection for citizens of the European Union and cover companies that do business in one or more EU Member States.

With the exception of cookies that are used to facilitate navigation (e.g. user authentication, content personalization, shopping carts)**, any use of tracking tools requires the user's consent**. You must also offer the option of refusal. Information about the use of tracking tools along with the right to refuse should be offered the first time the user connects and cover future use.

Additional information:

European Union Agency for Fundamental Rights, Handbook on European Data Protection Law

Your Online Choices: A guide to online behavioural advertising

AUSTRALIA

Privacy Act

Federal law, general in scope, on the protection of personal information as it affects companies engaged in business activities in Australia. **If you collect personal information using a tracking tool, you must inform the user** (a notice on the home page is sufficient) and explain what the information is used for in your privacy policy.

Additional information : Office of the Australian Information Commissioner, Privacy fact sheet 4: Online behavioural advertising – know your options

MOBILE APPLICATION DISTRIBUTION PLATFORMS

Apple App Store

Apps in the Kids Category may not use behavioural advertising.

Additional information

Google Play

Apps cannot include features that track user behaviour or incite the user to click them inadvertently. These must be clearly identified at all times by an icon and accompanying notification.

Additional information

SELF-REGULATION

The Digital Advertising Alliance of Canada (DAAC)

Consisting of Canadian advertising and marketing trade associations, the DAAC is a national self-regulation program launched to increase consumer understanding of online behavioural advertising. Its proposed **system is based on the opt-out mechanism**. Under this system, the AdChoices icon appears near an ad whenever data is collected and/or used for behavioural advertising purposes. By clicking on the icon, users can see the name of the company collecting the data, a description of its usage practices and a link to a consumer opt-out page.

The DAAC **advises** its members **not to use tracking tools** or any other means **to collect personally identifiable information from children known to be under 13 years of age for the purposes of behavioural advertising**.

Additional information:

Canadian Self-Regulatory Principles for Online Behavioural Advertising

Advertising Standards Canada

Unless authorized by law, advertisers cannot disclose personal information collected from children to any third party without first obtaining parental consent. The exception to this is third parties who support the platform's internal operations and neither use nor disclose personal information for any other purposes.

Additional information: Interpretation Guideline # 2 – Advertising to Children

Canadian Marketing Association

Marketers must not participate in the use of behavioural advertisements that knowingly or directly target websites aimed mainly at audiences under 13 years of age, nor do so through a third party, except in situations where a parent or legal guardian grants their explicit consent.

Additional information: Code of Ethics and Standards of Practice, see section K. Special Considerations in Marketing to Children

OUR RECOMMENDATIONS

- If possible, avoid integrating third parties who collect information for behavioural advertising purposes.
- Before allowing third-party cookies to be placed on your site, review the terms of service and privacy policy of the party in question to ensure that its practices meet your requirements.
- Be transparent about your behavioural advertising practices: contact parents and notify them using clear and simple language when collecting tracking data — for example, with a banner or interactive tool.
- Give parents the choice to opt out of behavioural advertising without preventing their children from accessing your platform. The opt-out must take effect immediately and apply to future connections.
- If appropriate, use your privacy policy to explain your practices with regard to behavioural advertising and explain the roles of the various parties involved.
- Periodically review the terms of service and privacy policies of any third-party services on your platform.
- **Québec: **All advertising directed at children under 13 years of age is strictly prohibited in Québec, barring certain exceptions prescribed by regulation**. This should factor into your decision to host an advertising network on your platform.

Bibliography.

BACKGROUNDER 06. PERSONALIZATION AND PROFILING

Explains the issues related to personalization and profile creation in youth production.

DEFINITION

1.1 What do "personalization" and "profiling" mean?

Personalization is a broad term encompassing the features that let users adjust items to their tastes and preferences — for example, choosing their page colour, creating an avatar, filling in a free text field, selecting a profile photo, saving links, etc.

Personalization data are what let children create online profiles (avatars) or manage personal spaces according to their preferences ("My home page").

Be careful when personalization enables personal information to be *publicly* shared. For example, in the "About you" field on a personal page that other users can view, a child might be tempted to disclose personal information that identifies her/him. To protect users who are children, you must be attentive to this and **regulate your personalization options**.

1.2 What aspects of profile creation require particular attention?

Creating a user profile can involve personal information. **The golden rule is to limit the collection of personal information to the minimum necessary to provide your service.** For example, during registration, it's better to ask for an alias (username) rather than someone's real name. Click here for details on registering through third-party sites (e.g. Facebook Login).

It is also essential to link profile creation and personalization to privacy policies and the protection of personal data. In this sense, parents should be informed of these practices and asked to provide their consent, especially when such practices target sites or applications aimed at users under 13 years of age. For users aged 13 and up, the personalization and profile creation processes can be considered as similar to those authorized for social networks.

REGULATION

Personalization and profile creation both affect the protection of personal data. For more information on this topic, click here.

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law to protect personal information about children collected online. COPPA applies to products that collect personal information from U.S. children under 13 years of age, **including collection by companies based outside the U.S.**

Under COPPA, you cannot ask a child for more information than what is required to take part in the activity. Ensure that the information requested for profile creation is "reasonable."

COPPA **holds you responsible for all personal information collected through your platform**. This includes information that you request from the child as well data **colleted inadvertently** — for example, personal information revealed while filling out fields. Ensure that children share no personal information for which you have not obtained verifiable parental consent.

Additional information:

Federal Trade Commission: COPPA Rule: A Six-Step Compliance Plan for Your Business

Collection of Personal Information

CANADA, EUROPEAN UNION, FRANCE & AUSTRALIA

Personalization and profile creation both affect the protection of personal data. For more information on this topic, click here.

Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

Getting Accountability Right with a Privacy Management Program

European Union: Directive on Privacy and Electronic Communications

Handbook on European Data Protection Law

France: Act on Information Technology, Data Files and Civil Liberties

Commission nationale de l'informatique et des libertés (CNIL)

Australia: Privacy Act

Office of the Australian Information Commissioner: Privacy law reform

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Apple App Store

An application cannot require users to provide personal information in order to use it.

Additional information

SELF-REGULATION

Personalization and profile creation are not covered by any self-regulatory programs. Users can rely on the regulation in effect.

OUR RECOMMENDATIONS

- When your website or app requires personalization or profile creation, make sure you obtain parental consent and clearly indicate these practices in your privacy and personal information protection policies.
- Consider how you will present your profile section **in terms of your audience's maturity** (e.g. creating a parent's login, the information to which parents have access, whether this access is total or partial, etc.).
- If possible, allow users to enjoy your platform without requiring them to create a profile (optional registration).
- When profile creation is required for your operations, explain why. For example: "This lets us save your game progress."
- During creation of the profile and/or in personalization areas, **post a reminder specifying the kinds of information users must not disclose**.
- Install **preventive mechanisms** to avoid having children publicly disclose personal information. For example:
    - Offer a tool for generating usernames.
    - Replace free text fields by drop-down menus with pre-selected options.
    - Block numbers on the keypad to prevent having the street address and/or phone number revealed.
    - Implement verification measures to clear all personal information before the user submits the data online.

Bibliography.

BACKGROUNDER 07. THIRD-PARTY AUTHENTICATION

Explains identification through third-party websites and the ethical questions this raises for youth production.

DEFINITION

1.1 What is identification through a third-party website?

It's when a digital platform wholly or partly delegates the user authentication process to a third party. For example, users who download your application are offered the option of signing in through their Facebook account and thereby skipping the registration process. Simplified authentication of this kind is offered by most mainstream social networks like Facebook, Google+ or Twitter.

1.2 Identification of children through third-party websites

While third-party authentication can be convenient for the user and of interest to the owner of a platform, the practice raises ethical questions when it comes to youth production.

The regulatory framework is designed to protect children who do not necessarily understand all the risks and issues associated with the collection and use of their personal information. To comply with this framework, most mainstream social networks prohibit users under 13 years of age from opening accounts. However, a number of studies have shown that young people regularly lie about their age in order to create a profile.

REGULATIONS

The United States addresses the question of third-party authentication in the Children's Online Privacy Protection Act (COPPA).

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law to protect personal information about children collected online. COPPA applies to products that collect personal information from U.S. children under 13 years of age, **including collection by companies based outside the U.S.**

COPPA applies equally to social media. If your target audience is exclusively within the "under 13 years of age" group, integrating authentication through a public social network into your platform is strongly discouraged.

Additional information : Federal Trade Commission: Complying with COPPA: Frequently Asked Questions

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Apple App Store

Applications that propose using an existing account for user authentication must have a privacy policy.

Additional information

SELF-REGULATION

The major Canadian self-regulatory organizations do not mention third-party authentication.

OUR RECOMMENDATIONS

- You can integrate registration through a third-party website if your platform is designed for **preschoolers (0–5) and the parent is required to register in order to supervise or monitor their child or make recommendations related to their child's profile (for example, monitoring the child's progress through a learning website)**.
- If your platform exclusively targets users under 13 years of age, do not integrate third-party authentication or registration through mainstream social networks
- If your platform partially targets users under 13 years of age, install an age-screening mechanism. This lets you only offer third-party authentication to users over 13 years of age.
- If your target audience is in the "6–12 years of age" group and you integrate authentication through a social network (which is prohibited for minors under 13 years of age), **you're sending parents an odd message.** Indirectly, you're encouraging your users to create a profile on platforms that they are prohibited to access. **This positions you in conflict with regulations designed to protect children**.

Bibliography.

BACKGROUNDER 08. COLLECTION AND USE OF DATA GENERATED IN SCHOOL SETTINGS

This backgrounder concerns products destined exclusively for the educational market. For commercial products, refer to Backgrounder Collection of Personal Information.

DEFINITION

1.1 What are some of the particularities of the educational market?

Among Canada, the United States, the European Union, France and Australia, currently, **the United States is the sole country with federal and state legislation** (FERPA and COPPA) governing the handling of student personal information. **If your educational product is not marketed in the United States, refer to the backgrounder on** the collection of personal information.

1.2 What is an EdTech product?

Current U.S. legislation identifies two categories of EdTech (educational technology) products:

1. Formal: educational material developed based on a curriculum and sold to schools on a contractual basis. **Any student information collected therein is solely for the school's use and benefit**.
1. Informal: educational material developed in whole or in part based on the learning objectives of a curriculum. Distributed to the general public through various business models, these products can also be used in the classroom. How **the information collected through such platforms is used remains at the producer's discretion.**

1.3 The notion of consent with regard to educational data mining

In an educational setting, schools are recommended to obtain parental consent as soon as the collection of personal information is involved. Teachers can send parents an explanatory note describing the application they wish to use. Parents could then be asked to register their child online, which would give them the opportunity to review the producer's privacy policy. However, it must be remembered that **in Canada, there is no law obliging educational institutions to take this approach**.

***In the United States* For "formal" products, schools can act on parents' behalf and consent** to the collection of personal information, since the data collected is solely for the school's use and benefit. **For "informal" products, parental consent must be obtained**.

REGULATIONS

Among Canada, the EU, France, Australia and the United States, the United States is the sole country with specific legislation governing the management of personal information collected from students.

Canada, the EU, France and Australia all deal with the issue of student privacy under more general laws governing the protection of personal information:

- **Canada**: Personal Information Protection and Electronic Documents Act (PIPEDA)
- **European Union:** Directive on Protection of personal data and Directive on Privacy and Electronic Communications, Handbook on European Data Protection Law
- **France**: Act on Information Technology, Data Files and Civil Liberties
- **Australia**: Privacy Act

United States

1. **Family Educational Rights and Privacy Act (FERPA)**

The FERPA is a federal law that **protects the personally identifiable information of students who attend federally funded schools**.

For "formal" educational products, schools can act on parents' behalf and consent to the collection of personal information from students, since the data gathered is solely for the school's use and benefit. The FERPA requires schools to maintain direct control of any information they share with a producer. **Ensure that the data you store can be easily accessed at all times.**

Additional information : U.S. Department of Education. Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices

2. **Children's Online Privacy Protection Act (COPPA)**

COPPA is a federal law that governs the online collection of information about children. It applies to **products that collect personal information about U.S. citizens under 13 years of age in a private or educational context, even if the company in question is based outside of the U.S.**

Schools cannot grant consent on the parent's behalf for "informal" educational products. For example, should a teacher want students to use a virtual world in a school project, he or she must obtain verifiable parental consent for each student.

Additional information : Federal Trade Commission: *Complying with COPPA: Frequently Asked Questions*

See Backgrounder Collection of Personal Information

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Apple App Store

The Volume Purchase Program (VPP) provides educational institutions with flexible distribution options

Google Play

*In March 2015, Google Play for Education was available in Canada, the United States and England.

Google Play for Education, a service available to primary and secondary schools, offers teacher-approved educational content categorized by subject and level.

Apps must meet certain criteria to be part of the selection. For details.

SELF-REGULATION

In the United States, various pledges issued by the EdTech industry demonstrate its commitment to protecting the confidentiality and security of personal information collected from students.

- K-12 School Service Provider Pledge to Safeguard Student Privacy
- Student Data Principles

OUR RECOMMENDATIONS

- In an educational setting, teachers can act as parents' agents and provide consent for applications they wish to use in the classroom. To keep communications with parents transparent, post a clear, detailed, up-to-date and easily accessible privacy policy explaining your personal data collection and handling practices.
- Limit your collection of personal information to the requisite minimum. For example, if possible, offer students the option of registering under an alias rather than their first and last names.
- Limit your use of data to the purposes for which consent has been secured, and store the data for only the minimum amount of time necessary.
- Parents who request it must be allowed to access the personal information collected about their child; you must also honour their right to revoke their consent for future collection.
- Should you change your privacy policy, inform parents and schools and again request consent.
- It is your responsibility to ensure that any tracking tools embedded in your product are acceptable. For example, behavioural advertising is prohibited under FERPA and COPPA as well as in products aimed at the Québec market.
- ***United States***: many states have their own laws regarding the protection of student information. Be sure to remain abreast of local regulations.

- ***United States***The legal definition of “personal information” can vary. Different obligations and restrictions apply to “personally identifiable” and “aggregated” data.

Bibliography.

BACKGROUNDER 09. CONTESTS

A backgrounder for developers who want to organize a contest or draw.

DEFINITION

1.1 What's a contest?

A contest entails the drawing of one or more prizes from among the contestants. Companies are legally entitled to stage contests, provided they meet certain conditions. Above all, you must **comply with the applicable regulations governing the jurisdictions where your contest is held**. For example, producers who do not wish to translate their promotional materials into French can open their contests to residents of Canada with the exclusion of Québec residents.It is important to **distinguish between a contest and a lottery**. The latter is a **game of luck** where players must purchase their chance to **win a prize**. Lotteries are **operated by the government** of a given region and as such, are strictly regulated.
To avoid being considered an "**illegal lottery," a contest cannot combine more than two of the following three elements**:

- Valuable consideration or participation costs (e.g. mandatory product purchase)
- Winner determined by random chance
- Prizes to be won

For example, eliminating the element of random chance makes the contest partially skill-based (e.g. by requiring contestants to correctly answer a general-knowledge question or mathematical problem).

1.2 Contests and children

Generally speaking, few specific provisions exist for children beyond the fact that the **prize cannot consist of a product that is illegal to sell to minors** (alcohol, tobacco, etc.).

While parental consent is not a legal requirement for contest participation, it is nonetheless strongly recommended.

In Québec, you must comply with the principles of the *Consumer Protection Act* prohibiting commercial advertising directed at children under 13 years of age, barring certain exceptions prescribed by regulation. When the prize is a product or item of particular interest to children (e.g. a toy), you must be very careful about how you choose to promote the competition.

1.3 Contests that employ user-generated content

A contest that features user-generated content — i.e. that requires contestants to submit content they create in order to participate — raises the question of **rights and licenses**. If you intend to use such content on your website or in your newsletter, the contestant must grant you certain permissions.

In Canada, for example, **copyright** involves two kinds of rights: **economic rights**, which include the right to use the work; and **moral rights**, which are linked to authorship. To authorize you to use their content for promotional purposes, participants must **assign you their economic rights** or **grant you a user license** and **waive their moral rights**.

You can obtain some of these authorizations directly through the contest rules; others may require a written signature. **Seek the advice of a legal professional** to help you deal with the question of user rights and licenses.

1.4 Personal information and spam

Some contests require participants to disclose personal information. Be sure to comply with applicable laws on the collection of personal information. Similarly, if you promote your contest by email or text messaging, you must abide by regulations governing commercial electronic messages.

REGULATIONS

You must comply with the **applicable laws of each jurisdiction where your contest is open**. Note that the rules can differ between provinces or states within the same country.

CANADA

Criminal Code and Competition Act

The legal apparatus that oversees competitions is the same across Canada except in Québec, where the **Act Respecting Lotteries, Publicity Contests and Amusement Machines** also applies (see below).

- Pursuant to the *Criminal Code*, you cannot require contestants to pay money or other valuable consideration (e.g. product purchase) as the sole condition for participation. Offer a **"no purchase necessary"** entry option that offers **precisely the same chances of winning as all other modes of participation**.
- The *Criminal Code* requires **that winners be selected using a method other than pure chance**. Accordingly, you must include a **"skill-testing question"** in the entry form — for example, a simple mathematical equation or a general knowledge question. Only participants who answer the question correctly will be eligible for the prize draw.

- You must obtain a **waiver of moral rights** and the **transfer of economic rights** or a **license to use any content generated by a participant** for promotional purposes (e.g. posting user content on your site's home page).
- You cannot unduly delay distribution of the prizes.
- Other information required pursuant to the *Competition Act* include the approximate value of the prizes, the number of prizes, the regional allocation of the prizes, the chances of winning and any other important information relating to the chances of winning.

Additional information: Competition Bureau – Guidelines: Promotional Contests

*****QUÉBEC**

1. **The Act Respecting Lotteries, Publicity Contests and Amusement Machines and Rules respecting publicity contests**

When the contest is open to Québec residents, you must:

- **Notify the** Régie des alcools, des courses et des jeux within the stated deadline; **pay the required fees**; and **include obligatory legal notices** in the contest rules pursuant to the Rules respecting publicity contests (e.g. the contest entry deadline, a description of the method of awarding the prizes, the number and a detailed description of the prizes offered along with the value of each prize, and the place, date and precise time the prizewinner will be named).
- Display contest rules and advertisements in French.

Certain requirements may vary depending on the total prize value. For example, when the total prize value exceeds $100, the promoter must pay the required fees and include obligatory legal notices. When the total prize value exceeds $1,000, the promoter must also notify the Régie that a contest is being held and file the prescribed form. If the total prize value exceeds $2,000, the promoter must file the text of the rules prior to the start of the contest as well as a written report after the prizewinner is named.

2. **Consumer Protection Act**

Québec's *Consumer Protection Act***prohibits commercial advertising to children under 13 years of age** on **all media platforms, barring certain exceptions prescribed by regulation.** This law governs **the promotion of contests with children.**

Apart from products that cannot legally be sold to children, **there are no a priori restrictions on the prizes your contest offers.** To prevent your contest from being considered as a commercial advertisement directed at children, consider the relationship between the following three factors:

1. The nature of the advertised prize (is it particularly attractive to children?)
2. How the contest is presented (is the focus on the contest itself or the prize?)
3. Where the contest is promoted (is there a simple mention on the home page, or is the message "hammered home" to children throughout the site?)

The nature of the prize is crucial: if it is a "children's product" — i.e. something attractive to young audiences like a toy or platform subscription — **you must be very careful in how you promote your contest**. The contest must not be an advertising tool for a product intended for children. **Contest promotion should focus on the competition itself rather than on the prize/product.** Allusions to the product and brand should be discreet.

> *An example of good practices Your youth website focuses on plants and wildlife. You launch a contest where you ask children to submit a text about their favourite animal based on information from your site. The winners will receive four tickets to the Museum of Nature. Your promotional materials emphasize the pleasure of using new knowledge about wildlife ("Show us your skills as a biologist!"). The logo and name of your commercial partner — for example, the Museum — are discreetly displayed at the bottom of the ad.*

For any questions, contact the Office de la protection du consommateur and refer to Backgrounder Embedding Advertising.

Additional information:

Régie des alcools, des courses et des jeux: Publicity Contest Notice

Office de la protection du consommateur: Advertising Directed at Children under 13 Years of Age

UNITED STATES

Contests are governed by an array of federal and state laws. Generally speaking:

- A competition must have official rules.
- If you offer different entry procedures, the opening and closing dates must be the same for each (e.g. entries postmarked with the closing date must be accepted).
- Winners cannot be charged any fees for claiming their prize.

There is an important distinction to be made between a "contest," where a skill-testing question is involved in determining the winner, and a "**sweepstakes,**" where the winner is selected at random (e.g. through a draw).

For a contest:

- Winner selection must be based on skill.
- You can charge contest entrants a fee or require them to purchase a product, but be careful: not only will you need a permit, but you must also be sure to comply with rules that can differ between states.

For a sweepstakes:

- You cannot require entrants to purchase a product or other valuable consideration to participate. Adopt a “no purchase necessary” entry option.
- Allentry methodsemployedmust provideentrants withthe same chances of winning.

EUROPEAN UNION & FRANCE

The **Unfair Commercial Practices Directive** is fairly broad with regard to contests. The Directive states that all contests must be organized lawfully. Accordingly, it provides a list of commercial practices considered “misleading” or “aggressive” that are to be avoided when organizing a contest. For example, it is considered dishonest to launch a contest and state that prizes can be won without awarding the prizes described.

Unfair Commercial Practices Directive

AUSTRALIA

Contests are the responsibility of the states and territories, which means that regulations vary across the country. Australia is flexible with regard to contests:

- You have the right to require that participants purchase a product or service in order to enter the contest.
- Competitions that do not determine the winner based purely on chance do not require licenses (e.g. a drawing competition).
- Contests based on chance may require a license in certain states.

Additional information:

Australian Government: Gaming (gambling) authorities

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

The **Apple App Store** requires official rules for sweepstakes and contests to be presented in the App, clearly indicating that Apple is not a sponsor or involved in the activity in any manner.

Additional information

SELF-REGULATION

Advertising Standards Canada recommends that you:

- Collect **only** the information sufficient to determine the winner in contests, games or sweepstakes-type of advertising to children.
- Limit the advertiser’s right to deal with anyone other than the parents or guardians of children who win a promotional contest, game or sweepstakes.

Additional information

The **Canadian Marketing Association** states that the marketing agent can collect personal information from children for contests without needing to obtain explicit parental consent, provided that the agent:

1. collects only the amount of personal information needed to determine the winner
2. communicates only with the winner's parent or guardian
3. does not retain personal information after the contest
4. only uses personal information to determine the winner
5. does not transfer personal information or make it available to a third party

Contest rules must be presented in a manner that is clear, visible and easy to locate, read and understand. The rules must also continue to be available for a reasonable period after the contest closes.

Additional information

OUR RECOMMENDATIONS

- You must **abide by the laws that apply in each jurisdiction where your contest is open**. **Careful!** The regulatory framework can vary within a given region.
- If you are designing a product for a company or a broadcaster, check to see whether they have an internal policy regarding contests.
- The **contest** is a **marketing practice tightly controlled by law**. As needed, seek legal assistance when drafting your official contest rules. In general, the rules must include the following points, **using language able to be understood by children:**
- Prize description: number, approximate value, support for related costs (i.e. travel, accommodation, delivery, etc.)
- Contest opening and closing dates
- Terms of entry and restrictions (e.g. age, region, parental consent, entry limit per child, etc.)
- Description of the methods for submitting the entry form (including the "No purchase necessary" option)
- Description of the skill-testing question
- Description of the method used to select and contact the winner
- The odds of winning
- Any other known facts that may significantly alter the chances of winning
- Your contact information and those of your contest partners
- If the contest has an age limit, this must be clearly indicated.
- The official rules must be available for the duration of the contest.
- Collect only the minimum required personal information and include a link to your privacy policy in the entry form.
- It is **strongly recommended that you request parental consent** (Backgrounder 2) for contest participation.

- Request the parent's contact information on the entry form: it is the parent you must contact, not the winner.
- **Contest participation must hinge upon compliance with the official contest rules.** For instance, have the rules appear when the user opens the entry form and include a statement like "I have read and understood the contest rules" with a checkbox that must be ticked before the form can be submitted.
- If the contest involves sending user-generated content, your contest rules must include the following:
    - Your policies on copyright and inappropriate content
    - A waiver of moral rights and assignment of economic rights
    - The procedures for withdrawing content displayed online
    - Content return policy (e.g. will the child's drawing be returned after the contest?)
- For safety reasons, delete the metadata encrypted in digital content (e.g. photos and videos).
- The promotional strategy "Invite your friends to enter to increase your chances of winning!" should be absolutely avoided.
- Forego contest formulas that invite children to share content on a social network.

Bibliography.

BACKGROUNDER 10. SURVEYS

For products that propose surveys to their users.

DEFINITION

1.1 Seeking user feedback through surveys

Surveys generally aim to **elicit user preferences and attitudes** toward a range of topics. When surveys are presented as games or quizzes, children might respond just for fun; they might also respond in exchange for some form of compensation — for example, an amount of virtual currency that can be used on the platform.

1.2 How are survey data used?

Data gathered through surveys are used **in different ways, based on the objectives of the party commissioning the survey**, e.g. the platform's operator or business partners.

Surveys can be used to develop a platform in a direction that better aligns with the interests expressed by respondents. For example, a survey may seek to find out what themes or features children would like to see on the platform.

Market research firms and/or business partners can pay to have their surveys presented to users of a given platform. Afterwards, marketers will apply the data derived to different business strategies. The editor of a magazine aimed at preteens could, for example, launch a survey about pop culture (fashion trends, music groups, etc.) to better inform the magazine's editorial content and marketing.

REGULATIONS

If you collect personal information (name of city, email address, etc.) through a survey, be sure to consult Backgrounder Collection of Personal Information.

When you do business with a partner, your survey can become a form of advertising. Consult Backgrounder Embedded Advertising.

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Mobile app stores have no particular regulations regarding user surveys.

SELF-REGULATION

Self-regulation does not address the question of user surveys.

OUR RECOMMENDATIONS

Be transparent with regard to your use of the data collected through surveys:

- Explain how you use survey data in your privacy policy as well as in the parents' section.
- Your explanation of how you use respondents' data must be presented in clear and comprehensible terms. For example, in the survey window, post a short text to the effect of "We use your answers to improve the user experience and develop fun new games!" followed by a link to your privacy policy.
- If the survey causes the child to interact with third-party content (which means that the survey is the initiative of a business partner), indicate this clearly.
- If you need to collect personal information, limit yourself to what is strictly necessary.
- Delete personal information once you no longer need it.
- Whenever possible and in a spirit of respect for individual privacy, dissociate survey responses from personal information.
- Avoid doing business with business partners who direct the user away from your platform — for example, requiring the user to click on a link to the partner's site to complete the survey.
- Also avoid doing business with partners who set out to recruit respondents with offers of compensation such as "Complete this short and fun survey in exchange for 10 units of virtual currency exchangeable in the virtual world!" This form of advertising is hard for children to detect and **in Québec, is prohibited** under the *Consumer Protection Act*, apart from a few exceptions prescribed by regulation.

Bibliography.

BACKGROUNDER 11. MAILINGS AND NEWSLETTERS

Presents the framework surrounding communications with the user (emails, newsletters, instant alerts, etc.)

DEFINITION

1.1 What's a newsletter?

Newsletters, whose content can vary from informative to promotional to a mixture of both, are a means of maintaining regular or occasional contact with users.

From the moment **a company draws on its database to contact its users,** communications are **considered "commercial electronic messages" in the eyes of the law**, even if their content is purely informative.

1.2 Are commercial electronic messages governed by law?

Commercial electronic messages are **governed by anti-spam legislation.** These laws cover the general public **without specific provisions for children**.

1.3 What's the difference between "commercial electronic messages" and "spam"?

A **commercial electronic message** is a message whose purpose is to encourage participation in a commercial activity by transmitting information on the product (i.e. the platform).

Spam is an unsolicited commercial electronic message.

In general, to avoid having your newsletter considered as spam, you must meet the following criteria (see Regulations for further details):

1. Obtain parental consent
2. Identify your company properly in the message
3. Include an unsubscribe mechanism

1.4 Consent and commercial electronic messages (opt-in/opt-out)

Users must consent to receiving commercial electronic messages. There are three types of consent:

- **Express,** explicit or positive (opt-in): the user must take concrete action to subscribe to the mailing list (e.g. complete a subscription form). Consent is valid until the user makes an unsubscribe request.
- **Implied**, tacit or inferred: based on an existing business relationship with the user (e.g. if the user has contacted you to request information). **Valid for a limited period:** you must obtain express consent before this period expires.

- **Negative** or passive (opt-out): users must take action to inform the sender that they do not wish to receive commercial electronic messages.

Generally speaking, express consent is preferred. Note that this entails providing separate consent to the sender of each commercial electronic message. Lines that "bundle" consent (e.g. "Check this box to receive our newsletter as well as those of our partners") are therefore to be avoided.

1.5 Unsubscribe mechanisms

Commercial electronic messages must **offer users the means to cancel their subscription**. The unsubscribe mechanism must be stated in clear terms, be visibly prominent and easy to use: it shouldn't involve more than two steps. For example:

- An "unsubscribe" link at the bottom of the newsletter, which opens a window where the user can check to confirm cancellation of their subscription
- A text message containing the word "STOP"

REGULATIONS

Each country has regulations governing commercial electronic messages. While there are minor variations, the legislation is essentially similar and aims to**protect the public against spam** by providing a legal framework for online commercial transactions. **Note that anti-spam laws do not contain specific provisions for children.** Generally, whenever you contact your users and/or their parents, your message must touch on the following.

1. **User consent**: include a statement specifying that consent can be revoked at any time.
2. **Identification**: you must clearly identify yourself and provide a method through which the recipient can readily contact you.
3. **Unsubscribe mechanism**: unsubscribe requests must be processed promptly.

CANADA

Canada's Anti-Spam Legislation

CASL applies to all commercial electronic messages (email, instant messaging, SMS, etc.) sent to Canadians. **Its approach is based on obtaining the user's express consent.** Implied consent is acceptable in some cases but is generally time-limited. You must be able to show how you obtained consent from each user.

****QUÉBEC****

Québec's ***Consumer Protection Act*** **prohibits commercial advertising directed at children under 13 years of age, barring certain exceptions prescribed by regulation**. Pay close attention to the content of your commercial electronic messages to avoid having them considered as advertising. For example, you cannot promote a subscription to your platform in a newsletter aimed at Québec children. For more information, see BackgrounderEmbedded Advertising.

Additional information:

- Government of Canada
- Office de la protection du consommateur: Advertising Directed at Children under 13 Years of Age

UNITED STATES

1. The **CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing) Act** applies to emails that promote a product or service, including web platform content. Its **approach is based on negative consent**, meaning that a company can send email offers until the recipient (the user) signals that they no longer wish to receive them. Email offers must be clearly identified as ads.
2. The **Children's Online Privacy Protection Act (COPPA)** provides that while there are some exceptions for mobile apps, in most cases, if you want to send push notifications, you need to obtain parental consent. This is because the contact information gathered from the mobile device to send the alerts constitutes personal information.

Additional information:

- CAN-SPAM Act: A Compliance Guide for Business
- Federal Trade Commission, Complying with COPPA: Frequently Asked Questions

EUROPEAN UNION & FRANCE

The **Directive on Privacy and Electronic Communications (also known as the E-Privacy Directive)** advocates express consent whereby users must signal their consent prior to receiving your commercial electronic messages. Implied consent is acceptable provided each message contains an unsubscribe mechanism.

Additional information:

Directive on Privacy and Electronic Communications

AUSTRALIA

The **Spam Act** targets commercial electronic messages that originate or are commissioned in Australia or are sent from an "Australian link." It is based onexpress consent but accepts implied (inferred) consent under certain conditions. Companies must be able to show how they obtained the consent of each user they contact.

Additional information:

Australian Government, Spam Act 2003: An overview for business

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Apple App Store/Amazon Appstore

- You must obtain the user's consent to send push notifications.
- It is prohibited to use push notifications or real-time alerts to send spam, advertisements or promotional offers.
- Do not abuse push notifications: send them at a *reasonable* frequency.

Additional information:

Amazon Distribution and Service Agreement

Apple Developer Guidelines

SELF-REGULATION

The **Canadian Marketing Association** lays the groundwork for industry self-regulation through its **Code of Ethics and Standards of Practice**. The CMA states that mailing list subscription must comply with the requirements of Canada's Anti-Spam Legislation:

- **Emails and text messages**: do not send marketing communications without first **obtaining the recipient's express or implicit consent**.
- **Internal do-not-contact list:** at the consumer's request, promptly add email addresses and cell phone numbers to your internal do-not-contact list and cease all marketing to those addresses/numbers within 10 working days.

Additional information: consult section N4 of the Code of Ethics and Standards of Practice

OUR RECOMMENDATIONS

- Mailing list subscription involves collecting the child's email address, which is a form of personal information. Since this is considered sensitive information, you are advised to obtain parental consent before starting to send commercial electronic messages to a child.
- Always favour express consent: it's the most transparent form and remains valid until the user decides to unsubscribe.
- Indicate the frequency of your mailouts or messages so that users clearly understand what they are consenting to (e.g. say whether your newsletter is monthly, weekly or daily).
- If possible, allow users to define the frequency with which they receive your messages.
- Clearly identify your company in each message (contact info and physical address).

- Your unsubscribe mechanism must be simple and efficient: **one click should be all it takes to cancel subscription to a mailing list.**
- Send an automated unsubscribe confirmation message.
- If you issue a range of communications (e.g. weekly newsletter, occasional notifications for special events, etc.), you can create a "consent menu" where users select the types of messages they wish to receive.
- *In Québec, commercial advertising aimed at children under 13 years of age is against the law, barring certain exceptions prescribed by regulation.**Messages to Québec children cannot therefore contain promotional offers, advertisements or self-promotion** for products or services that are attractive to children. Messages containing advertisements are strictly destined for parents.
- *United States: Careful! Some states have their own anti-spam legislation that diverges from the federal framework.

Bibliography.

BACKGROUNDER 12. TERMS OF USE

Explains what terms of use consist of and what they must cover.

DEFINITION

1.1 What are "terms of use"?

Also known as "terms and conditions" or "terms of service," they're the **rules that the user must agree to in order to use a platform**. Terms of use constitute a **legally binding document** that describes your expectations toward users as well as your obligations as an operator. In most cases, the document is not required by law; however, it helps release you of certain liabilities, thus protecting your company from potential litigation.

1.2 What must terms of use include?

While their content will vary based on the features offered by the platform, terms of use normally cover the following:

- User rights and responsibilities
- Operator rights and responsibilities
- A link to your privacy policy
- Your policy regarding cookies and other tracking tools
- Intellectual property on your platform
- Procedures in the event of changes to your terms of use

Participatory platforms must address user-generated content in their terms of use, while paid services must provide information about their market activities. For more information, see our recommendations.

1.3 Where should terms of use be posted?

In general, terms of use are posted in the same place as the privacy policy, i.e. at the bottom of each web page (for a website) or in the descriptive text on the app's home page. You can also post them in the parents' section.

REGULATIONS

While legally required in the European Union and France, terms of use are not required by law in Canada, United States or Australia.

EUROPEAN UNION & FRANCE

The **Directive on Privacy and Electronic Communications (also known as the E-Privacy Directive)** (European Union) and the **Loi pour la confiance dans l'économie numérique** (Law for Trust in the Digital Economy) require a "**legal notice**" whose purpose is to inform the user about the platform's operator.Legal notices must be accessible from the home page and include:

- Company information and coordinates (name, legal form, business addressor registered office, email address, telephone number)
- Person responsible forpublication
- Web host's contact details: name, denominationor company name,address andtelephone number
- France: CNIL simplified declaration number for the collection of personal information
- Cookie policy

Various other conditions apply to commercial sites. Consult France's civil service website for more information:

- Official French civil service website: Quelles sont les mentions obligatoires pour un site web? (in French only)
- Directive on Privacy and Electronic Communications

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

App stores do not require mobile applications to post terms of use.

SELF-REGULATION

The leading Canadian self-regulatory bodies make no mention of terms of use.

OUR RECOMMENDATIONS

- While terms of use are not obliged by law in Canada, United States and Australia, **we strongly recommend all platforms to draft terms of use adapted to their product or service**, since they constitute valuable **legal protection** for your company.
- Terms of use are an **important legal document** that must be adapted to each product in order to protect your company: **consult a lawyer**.
- **For non-participatory platforms:** in the interests of making browsing easier, your terms of use can be worded so as to have users **implicitly accept them** without being obliged to perform a specific action like checking a box or clicking "Accept." For example:
  Use of this platform is contingent upon compliance with these terms of use. By accessing, browsing and/or using this platform, you acknowledge having read the terms of use and agree to comply with them as well as abide by the applicable laws and regulations.

- As far as possible, present your terms of use in language that can be easily understood by your readers or their parents.
- Terms of use normally include the following:
- Contact information of the company responsible for the platform
- User rights and responsibilities
- Operator rights and responsibilities (personal data protection and security measures, limitation of legal liability, etc.)
- System requirements
- Description of your use of cookies and other tracking tools
- A link to your privacy policy
- Intellectual property on your platform (your own content, third-party content licenses, etc.)
- The applicable laws in the event of litigation (e.g. "These terms of use are governed by federal Canadian legislation and applicable provincial statutes")
- Your contest management policy, if applicable
- Date of most recent update and terms of use version number (e.g. "Version 2.4. Last updated: June 12, 2015")
- Procedure in the event of changes to the terms of use (e.g. "Should these terms of use be amended, users will be notified of the new terms within 10 working days of their coming into effect")
- In the interests of transparency, make all previous versions of your terms of use accessible to users.
- For participatory platforms, **participation can be made contingent upon compliance with the terms of use**. For example, during the account creation process, post a dialogue box with a statement to be checked, such as "I have read and accept the terms of use." This is a precaution that can **help prevent certain kinds of violations**.
- The terms of use of a participatory platform must include:
- A reminder of the rules of conduct between users as well as what constitutes "unacceptable" content (e.g. "Content should not be illegal, obscene, defamatory, threatening, infringe upon intellectual property rights, violate privacy or be otherwise injurious or objectionable")
- A link to your digital code of conduct
- A request for **license to use content** (e.g. "By sharing the content on this platform, you grant [*company name*] license to…")
- A legal disclaimer expressing disaffiliation with content (e.g. "Despite our efforts to moderate the content posted on this site, we do not endorse any statements made by our users")
- An arrangement through which you reserve the right to terminate a user's account, remove any content displayed through that account and restrict that user's access to the platform

Bibliography.

BACKGROUNDER 13. USER-GENERATED CONTENT (UGC)

Applies to platforms that allow users to publish content created or referenced by users.

DEFINITION

1.1 What are the characteristics of user-generated content?

User-generated content (UGC) is broadly defined as "material uploaded to the Internet by website users." As such, it encompasses both original content and links to other content posted by users. In general, UGC is when the user is the content's author. Such content can be created offline and downloaded on your platform (e.g. photos) or created using tools available on your platform (e.g. designing an item for a virtual world or leaving a comment on a forum). Content that users share but have not created — for example, newspaper articles, YouTube videos and so on — can also be considered UGC.

Media or platforms that publish UGC are known as **interactive** or **participatory**. Such platforms have varying implications with regard to the collection of personal information, intellectual property and user and content moderation.

1.2 What risks to personal information are associated with UGC?

With young audiences, particular attention needs to be paid to the *inadvertent* collection of personal information, i.e. when children publicly share information allowing them to be personally identified. A child may, for example, divulge his or her physical address in a public forum. In this sense, to ensure the safety of young users, you should consider incorporating content moderation mechanisms.

For further details on the collection of personal information, click here.

1.3 Should a participatory youth platform be moderated?

Allowing users to post content on a given platform implies a certain loss of control: there's nothing to stop reprehensible conduct like sharing offensive content or infringing upon intellectual property rights. **Making interactive youth media "safe"** means implementing **mechanisms to moderate content and users**.

1.4 What are the implications for intellectual property on participatory media?

To avoid intellectual property breaches, including copyright breaches, as well as secure adequate rights to use content generated by users, operators of participatory platforms must monitor all

content posted. The information pertaining to intellectual property is set out in the platform's terms of use, which is a legal document.

REGULATIONS

User-generated content as it pertains to personal information is addressed specifically in the section on the United States. For other countries, refer to the general information on the collection of personal information. User and content moderation on participatory platforms is addressed in depth in Backgrounder 14. The section below mainly addresses intellectual property.

CANADA

Copyright Act

On January 2, 2015, Canada adopted a new "notice and notice" regime that gives copyright owners a certain amount of control over how their works published online, including UGC, are used. Under the regime, when a copyright owner thinks that a user might be infringing their copyright, they can send a notice of alleged infringement to the platform operator. The platform operator must then forward the notice to the user who has allegedly infringed the copyright. An operator who refuses to send the notice may be held responsible for allowing copyright to be breached.

Additional information:

Government of Canada, Office of Consumer Affairs: Notice and Notice Regime

****Québec: An Act to Establish a Legal Framework for Information Technology**

Québec is the only province **offering platform operators legal protection with regard to user-generated content.** Operators are not liable for the activities of those who use their services unless they are aware that the UGC is serving illicit purposes. At that point, the operator must promptly remove the content. However, **operators are not responsible for overseeing content stored or shared through their service nor for investigating whether or not the content is used for illicit purposes.**

Additional information:

Copyright Act

Québec – *An Act to Establish a Legal Framework for Information Technology*

UNITED STATES

Communications Decency Act (CDA) and Digital Millennium Copyright Act (DCMA)

The United States has a legal apparatus that protects participatory media operators fairly well.

Where platform content is **created entirely by third parties**, the operator may qualify for immunity under the *Communications Decency Act*. This **shields the operator from all liability for disseminating UGC**, including cases of alleged defamation, misrepresentation, negligent, fraudulent

or misleading statements, false advertising and other crimes. However, the immunity does not cover **intellectual property infringement**.

The *Digital Millennium Copyright Act* protects operators from allegations of intellectual property violation: under this law, the operator cannot be held responsible for distributing and/or storing copyright-infringing UGC. To qualify, operators must publish a copyright policy, **notice and takedown procedures**, and notification to the effect that users who repeatedly violate copyright will have their accounts closed.

Children's Online Privacy Protection Act (COPPA)

Federal law that applies to products that collect personal information from U.S. children under 13 years of age. COPPA considers photos, videos and audio files containing a child's image or voice to be personal information. If your platform enables content of this kind to be shared, you must obtain verifiableparental consent before allowing children to take part in the activity. You must also be aware of collecting personal information inadvertently.

N.B. COPPA applies only to data collected directly from children. For example, if you were to invite an adult (parent, teacher, etc.) to share a photo of a child, COPPA would not apply.

Additional information:

Federal Trade Commission: Complying with COPPA: Frequently Asked Questions

EUROPEAN UNION AND FRANCE

Electronic Commerce Directive

According to this directive, operators are not liable for the illegal activity or information placed on their systems by a user **when they are in no way involved** in the activity or information. Upon obtaining actual knowledge or awareness of its illegality, the operator must act promptly to remove the content or block access to it.

Additional information:

European Commission, Electronic Commerce Directive

AUSTRALIA

Australian Copyright Act

Australian law offers sparse protection to online operators. This means that when user-generated content infringes copyright on your platform, you can be held partially responsible for allowing the breach. You therefore need to implement measures to monitor UGC on your site (e.g. a system that approves UGC before it is posted online) and remove content that fails to respect copyrights.

Additional information:

Australian Copyright Council

Office of the Australian Information Commissioner

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

All stores require developers to classify their apps based on their **overall content**, including UGC and advertisements. Each store has a rating system based on the absence or presence of various criteria (e.g. violence, language level, etc.). Stores also require developers to respect intellectual property rights.

Apple App Store

Apps that allow UGC must develop **methods to filter content, a whistle-blowing mechanism for offensive content** and a way of blocking abusive users. Apps that allow content to be downloaded from third-party sources (e.g. YouTube, Vimeo, etc.) must have obtained explicit permission from said sources.

Additional information

SELF-REGULATION

Since it is an area well regulated by law, user-generated content is not covered by any self-regulatory programs.

OUR RECOMMENDATIONS

- If you invite children to share photos and/or personal videos, make sure you **filter such content before posting it online**. Known as "pre-moderation," this helps you avoid publicly sharing personally identifiable data.
- Obtain adequate rights for user-generated content through your **terms of use**. For example, do you want to own the content or just have a license to use it?
- Place UGC under license: the rights you grant your users to use UGC posted on your platform must not be more extensive than those you obtained from users who shared the content.
- Post a notice to distinguish copyrighted works on your platform. For example, if your terms of use specify that your users remain the owners of content they create, your notice might look like this:

© 2015 [your name] and contributors

- Indicate in your terms of use that users must not post content that breaches intellectual property rights and that you reserve the right to remove any content that constitutes a breach.
- Develop procedures like a content filtering system to prevent having any UGC that infringes intellectual property rights posted on your platform.
- In your terms of use, state the procedure for filing a complaint regarding intellectual property. **Complaints must be processed promptly**:

1. Remove the infringing content.
2. Inform the user who posted the infringing content that the content has been removed, explain why and refer the user to your intellectual property policy.
3. If appropriate under your digital code of conduct, consider imposing a sanction on the offending user.
4. Inform the complainant that the content has been removed.

- Incorporate a mechanism that lets users easily flag offensive UGC.
- Participatory media raise a number of legal issues: for your own protection, **seek professional legal advice**.

Bibliography.

BACKGROUNDER 14. USER AND CONTENT MODERATION

Addresses products that allow users to contribute content and/or interact with each other or the content.

DEFINITION

1.1 What is moderation?

On what basis should moderation be performed?Moderating an interactive platform means screening content submitted by users and/or user interactions **by applying a set of predefined rules to distinguish the acceptable from the unacceptable**. In youth production, moderation covers the following:

- "Inappropriate" speech, behaviour and content (adult users/predators, preventing real-world encounters, violence, drugs, alcohol, weapons, illegal activities, etc.)
- Disrespectful behaviour toward other users (stalking, cyberbullying, inappropriate language, racist or sexist remarks, hate speech, etc.)
- The disclosure of personally identifiable information
- Disruptive behaviour (abuse of reporting mechanisms, spamming, impersonating platform staff, etc.)
- Content that breaches intellectual property rights (e.g. posting a link to illegally download a movie or sharing a photo that does not belong to the user)

1.2 What are the possible approaches to moderation?

There are a number of ways to approach moderation:

- Pre-moderation: when content submitted to a website is placed in a queue to be checked by a moderator before being made public.
- Post-moderation: when submitted content is displayed immediately but replicated in a queue for a moderator to review and remove if inappropriate.
- Automated moderation: deploying various technical tools to process user-generated content (UGC) through a set of defined rules. Often used in chatroom scenarios, these tools include:
    - White lists: predefined words. Users cannot enter their own text.
    - Black lists: users type their own messages which are filtered to remove any inappropriate words before they can be seen by other users.

1.3 How should users who violate the rules of good conduct be handled?

Consequences imposed for breaches of conduct should be **graduated in line with the gravity of the alleged violations**. For example, the user receives a formal warning after the first offence, his account is suspended for 24 hours after the second and so on, right up until the account is closed.

This **educates users** who act in good faith but who, in their inexperience, bypass or transgress certain rules of conduct. It's also a means for moderators to detect suspicious behaviour that could help identify a predator (Backgrounder 21, 1.3).

1.4 Which moderation approach is best?

There is no one universal approach for all platforms. Each approach offers a different level of control over published content and user interactions. Depending on your needs, you can opt for a **combined approach**. When evaluating your requirements, consider the following:

- **Assessing the risk** posed by UGC
- The levels of maturity and autonomy of your **users**
- The **budget** you can allocate to moderation

For more information: How to De-Risk the Creation and Moderation of User-Generated Content

1.5 Flagging inappropriate content/behaviour

Tools that let users **anonymously** denounce inappropriate content and/or behaviour are **essential to ensuring compliance with certain intellectual property laws, including copyright laws**. In general, operators will be absolved of all liability if they act promptly when advised of the presence of infringing content on their platforms.

Inappropriate content or behaviour can be flagged in a number of ways; the important thing is to have a mechanism that's easy to access and use. One way is to have a clickable "Report" icon everywhere content can be shared or users can interact. You must also establish **effective procedures for responding quickly to such alerts.**

REGULATIONS

While moderation **is not required by law**, it is **strongly recommended in youth production for security reasons**. For more information on the regulatory framework governing participatory media, click here.

UNITED STATES

Children's Online Privacy Protection Act (COPPA)

Federal law that applies to products that collect personal information from U.S. children under 13 years of age. COPPA considers photos, videos and audio files containing a child's image or voice to be personal information. If your platform enables content of this kind to be shared, you must:

1. Screen and remove any content (photos, videos or audio tracks) where children can be seen and/or heard before this content goes online; **OR**
2. Obtain verifiable parental consent before allowing children to submit photos, videos and/or audio recordings of themselves.

Under COPPA, certain user interactions — for example, contributing to a forum — do not require verifiable parental consent provided the operator takes reasonable measures (e.g. pre-moderation) to ensure that no personal information is inadvertently disclosed. **Staff who have access to personal information (e.g. moderators)** must be **sufficiently trained** to handle sensitive information of this kind.

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Each app store has a rating system based on the presence or absence of various criteria (violence, language level, nudity, pornography, etc.). This applies to all app content, including user-generated content. Apps that allow UGC should employ **a moderation method to filter content** and have **a whistle-blowing mechanism for inappropriate content** as well as a means of blocking abusive users.

- Apple App Store
- Amazon Appstore
- Google Play

SELF-REGULATION

While no specific self-regulation code applies to content moderation, it is strongly recommended for participatory media.

OUR RECOMMENDATIONS

- Consider your production budget and determine what portion you wish to allocate to moderation, based on your platform's features, keeping in mind that content filtering and moderating can entail significant operating costs.
- Moderation should be based on defined rules. These rules of conduct, expressed in accessible language, should be laid out in your digital code of conduct and/or terms of use.

- Include a clause granting you the right to remove any content that violates your platform's policies.
- Post security reminders in "critical" areas of your platform. For example, in the chatroom, remind children not to disclose personal information like phone numbers.
- If you opt for pre-moderation, erase all content containing personal data: blur faces in photographs, strip metadata from documents and so on.
- Moderators work closely with children. Be sure to select them carefully and train them to manage problem situations as well as work with personal information.
- Make sure your reporting mechanism is easy to find and use. Design it so that users can include the reason for the complaint (e.g. "Why are you reporting this content?" with checkboxes they can tick and/or a text box), since this will speed up processing.
- To prevent the exchange of encrypted data (age, address, etc.), the following are recommended:
    - **Block the numbers keypad**, making it impossible for the user to enter digits (1, 2, etc.).
    - Use a black-list tool to block numbers written out in words (one, two, etc.)
- For products where extra precautions are advisable (e.g. for very young audiences), the use of a white list is recommended.
- Periodically review and update your moderation methods (e.g. black list words).
- Moderating an interactive platform may raise legal issues: for your own protection, **seek professional legal advice**.

Bibliography.

BACKGROUNDER 15. DIGITAL CODE OF CONDUCT

Explains what a digital code of conduct is and what it should contain. The digital code of conduct involves concepts such as netiquette (respectful and appropriate conduct online) and good digital citizenship (safe online behaviour).

DEFINITION

1.1 What is a digital code of conduct?

It's a set of rules **pertaining to the use of participatory media**. A digital code of conduct forms the basis for user and content moderation. It's also a valuable tool for educating your users about computer-mediated communications, in addition to helping keep your platform environment safe and respectful.

1.2 What should a digital code of conduct include?

Common topics include the **sharing of personal information**, **disrespect toward other users**, **inappropriate content** and **disruptive behaviour**(spamming [Backgrounder 11], abuse of the reporting mechanism, etc.). The code of conduct can also serve as a useful reminder of copyright principles to prevent users from inadvertently or deliberately publishing copyrighted works.

Set out in accessible language, a digital code of conduct should list (as exhaustively as possible) **rights and responsibilities**, **expectations** and the**consequences** in the event of an infringement. The code should specify the consequences if the rules are broken — for example, the removal of content or the suspension/closure of a user's account.

1.3 How should the digital code of conduct be displayed?

There is no single recommendation for how or where a digital code of conduct should be displayed. **Its importance will vary greatly depending on the type of platform and degree to which the platform is participatory.** For example, in a social network where users have frequent opportunities to interact, the digital code of conduct may take the form of a contract that users must agree to before they can participate.

REGULATIONS

A digital code of conduct **is not required by law**; however, given that it forms the basis of user and content moderation, you are strongly recommended to include one. For more information on the regulatory framework that applies to participatory media, click here.

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Mobile app stores do not require developers to post a digital code of conduct.

SELF-REGULATION

No self-regulation program specifically advocates having a digital code of conduct.

OUR RECOMMENDATIONS

- Some platforms integrate their digital code of conduct into their terms of use. However, in youth production, you're best off making it a separate document to show your commitment to your users' safety.
- Ensure that parents can access your digital code of conduct at all times.
- If your audience consists of preschoolers, your code must address their parents and be posted in the parents' section.
- If appropriate to your platform, present your digital code of conduct in a playful manner so as to prompt children to put the rules into practice.
- Avoid legal jargon: your code should adopt a familiar tone and be expressed in plain language adapted to your audience's level of maturity. For example, use familiar formulations like "When you come here to play, you don't have the right to . . ."
- A rule must be stated precisely. As needed, consider **using examples to illustrate ideas that are more complex**. A statement like "Watch your privacy! Don't share personal information in the chat room" could be accompanied by a list of what constitutes personal information.
- Consequences should be increased in severity based on type and number of offences: issuing a warning, removing the content, suspending the account for a day, closing the account.
- Make participation contingent on your digital code of conduct: have users check a box to signal their acceptance ("I have read and accept…") before allowing them to access your platform.

1. In order to post on message boards, blogs, guestbooks, send Mail and upload images to the site, you must be a registered user of TeenNick.com. If you have not registered and would like to please Click Here
2. Don't give out, or ask other people for, Personally Identifying Information (or PII). PII is anything that would allow a person to contact you elsewhere or find you in real life, because that can be extremely dangerous. PII includes IM screennames, email addresses, phone numbers, your full name, etc.
3. Don't curse too hard. Mild cursing -- like 'damn', 'hell', 'friggin" or 'he made such an ass of himself"-- is tolerable, if you just cannot help yourself. But the serious, detention-worthy stuff won't fly. And if you manage to say something totally vulgar without using any curse words, or just mask out some letters in a harsh curse word, that's not OK either.
4. Don't post copyrighted material, or pretend you created something when someone else actually made it.
5. No graphic or gratuitous discussions of sex are allowed in message board posts, blogs or Mail. Explicit photos and images are not allowed, and uploading them may result in your account being deactivated.
6. Don't post, submit or send anything that glorifies, encourages, or tells people how to do things that are violent, illegal, or harmful to themselves and/or others.
7. Don't use hate speech in TeenNick.com's community -message boards, guestbooks, blogs and Mail, or upload images containing offensive depictions of people. That includes negative stereotypes, racial epithets (like negative words used to describe a group of people), and bigotry.
8. Don't get into flame wars. We want you to discuss your opinions and express yourself. But don't insult other people on the site or in Mail to get your point across, please.
9. Saying cruel and demeaning things about other people in the TeenNick community or people you know in real life is not OK. Talking trash about a politician or other public figure might be OK, but please be mindful of the other rules which would apply to any such opinions
10. Don't offer or request advice on message boards, guestbooks, Mail or blogs that should really be coming from a professional. That includes the kind of stuff you should be discussing with a guidance counselor, doctor, therapist, police officer, or lawyer.
11. Don't post ads on the message boards, even if it's for something you made yourself like a zine or website. You can write about it in your blog.
12. No chain letters, pyramid schemes, virus warnings or other 'spam' on the message boards.

Source: Teen Nick@ Viacom International Inc.

Bibliography.

BACKGROUNDER 16. EMBEDDED ADVERTISING

Covers products that use embedded ads as a revenue stream.

DEFINITION

1.1 What is online advertising?

"Advertising" can be defined as any form of published commercial message intended to promote goods or services for a business interest.

The online environment offers numerous advertising possibilities, including embedding ads into the editorial content. Some common examples are:

- Advergames: free games whose aim is to promote a given brand through their dissemination and use
- Brand integration: using editorial content to discuss/give visibility to a brand (similar to "branded content" and "product placement")
- Advertisement: banner messages displayed at specific locations on the web page or application. These ads may also appear as pop-up windows, overlays or interstitials as well as between two page views, video views, game sessions or website sections.
- Behavioural advertising : ads selected and displayed based on the navigation data collected from the user.

1.2 What regulations govern advertising?

Consumer protection laws use the concept of "**false advertising**" to refer to ads likely to deceive the consumer through misleading statements or product misrepresentation. Whether or not an ad is misleading is also determined based on the maturity of its target audience.

Advertising practices are voluntarily regulated through **codes set out by the industry** (advertisers, advertising agencies, media organizations). Such self-regulation establishes ethical standards for how the messages are designed; it also creates a system for evaluating ads and handling complaints.

In advertising, the notion of **responsibility** is complex due to the number of stakeholders involved. When a message violates a law or self-regulatory code, who is responsible? The advertiser? The agency? The media platform? The ad network? The answer varies depending on the jurisdiction in question; however, generally speaking, **responsibility is shared**. All stakeholders must therefore remain abreast of the regulatory framework in effect wherever they advertise.

1.3 Advertising aimed at children

Children may lack the cognitive skills, experience and maturity to detect the commercial intent behind an ad. Because of this, advertising aimed at children is often more strictly regulated.

With the exception of Québec (where the law is more stringent and bans commercial advertising targeting children under 13 years of age, barring certain exceptions prescribed by regulation), all of Canada's other provinces, along with the United States, the European Union, France and Australia, use self-regulatory codes to regulate advertising aimed at young audiences. In general, these codes advocate that:

- Ads must not exploit children's inexperience or credulity.
- Ads must not contain visual information or illustrations liable to harm the child emotionally, morally or physically.
- Ads for products whose sale is prohibited to children (e.g. alcohol, lotteries, etc.) should not present these products in a way attractive to children.

REGULATIONS

CANADA

Two realities coexist in Canada: the province of Québec, where the *Consumer Protection Act* prohibits commercial advertising aimed at children under 13 years of age, barring certain exceptions prescribed by regulations; and the rest of Canada, where advertising aimed at children is controlled through industry self-regulation.

1. **The Competition Act**

Federal law that covers false advertising on all media platforms. All companies based in Canada that advertise online are required to comply. In the digital space, the **responsibility** comes down to **the entity that controls the platform's content**. Note that the Act has **no special provisions for children**.

2. **Provincial Consumer Protection laws**

Legislation enacted in each province that prohibits false advertising in all media. Québec also bans commercial advertising aimed at children under 13 years of age, barring certain exceptions prescribed by regulation. Consumer Protection laws in the other provinces have no special provisions for children.

3. **Personal Information Protection and Electronic Documents Act (PIPEDA)**

Federal statute with policies and directives concerning online behaviour advertising.

For more information:

- Competition Bureau: Application of the Competition Act to Representations on the Internet
- Consumer Information: Provincial and Territorial Legislation
- Office of the Privacy Commissioner: Policy Position on Online Behavioural Advertising

*****QUÉBEC*****

Consumer Protection Act

Provincial law that **prohibits commercial advertising to children under 13** years of age on **all media platforms, barring certain exceptions prescribed by regulation**. The ban applies to messages aimed at children in Québec, **including those issued by companies based outside the province**. The Act applies to any stakeholder involved in the advertising process, including all persons who request the ad as well as those who design, distribute, publish or broadcast it.

In determining whether a commercial message is intended for children aged under 13, you need to **consider the following**:

1. a) The nature and intended purpose of the product advertised (is it attractive to children?)
2. b) How the ad is displayed (is the message designed to attract the attention of children?)
3. c) The time and/or place where the ad appears/is broadcast (are children targeted by or exposed to the message? Are they present where or when it is displayed or broadcast?)

The law also provides that it is necessary to take into account the context of the ad's presentation and the general impression it gives.

The law allows you to post ads on your youth platform provided the messages are not intended for children aged under 13. Analyzing how the factors above interact will let you determine whether an advertisement violates Québec's law.

Warning! As discussed in Section 1, **online advertising can take many forms, all of which are subject to the ban**. Your youth platform should not serve as a vehicle for delivering ads to Québec children aged under 13 or for promoting other brands. For example:

- Advergames: games developed around a product "attractive" to children (e.g. a toy, candy) are in violation of the law.
- Contests : when the prize is a product "attractive" to children, be very careful in how you promote the contest.
- Behavioural and contextual advertising : to be avoided insofar as the messages presented are selected based on children's browsing history or inferred preferences.

The law has three **exceptions**, prescribed by regulation, to the prohibition of commercial advertising to children under 13 years of age. Accordingly, under certain specific conditions it may be possible to **advertise in a children's magazine; advertise for a children's entertainment event;** and **advertise in a way designed to target children in store windows and displays as**

well as on containers, packaging and labels. Furthermore, **educational or lifestyle advertising** is permitted under certain conditions.

It should also be noted that under the law, advertisements can still be considered to be directed at children under the age of 13, even when contained in printed matter intended for an older audience (persons aged 13 and over) or a general audience (persons both under and over 13 years of age), and even when broadcast during a program intended for an older audience (persons aged 13 and over) or a general audience (persons both under and over 13 years of age).

For full details, consult the guide for Advertising Directed at Children under 13 Years of Age

UNITED STATES

Federal Trade Commission (FTC) Act

Federal law prohibiting unfair or deceptive advertising in any medium. Under the Act, advertisers are responsible for the content of their ads. Third parties involved in designing or delivering a message (including platform operators) share the task of assessing the message's content and may be held liable for misleading advertising.

The Act has a special provision for advertising aimed at children which states that advertisers must be careful not to misrepresent a product or its performance to children due to their level of development.

For more information, visit the Federal Trade Commission online

Children's Online Privacy Protection Act (COPPA)

Federal law applicable to products that collect personal information from U.S. children under 13 years of age. COPPA holds operators responsible for all personal information collected through their platforms, including data gathered by third parties (e.g. ad networks). When a third party collects information about your users, you must specify this in your privacy policy and obtain verifiable parental consent prior to collection.

For more information on COPPA, see Backgrounders Collection of Personal Information and Online Behavioural Advertising as well as the COPPA guide, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

Advertising Self-Regulatory Council

U.S. organization defining the policies and procedures of various self-regulatory industry programs. The **Children's Advertising Review Unit (CARU)**assesses advertising and promotional materials across all media to meet its mission of:

- Enforcingits guidelineswith nationaladvertisers, i.e. those conducting advertising campaignsacross thecountry (or a substantial part thereof)
- Monitoringonline platformsto ensurecompliance with the **laws** (e. COPPA) **governing the collection of personal information**

The CARU lays out **principles applicable to the online environment**. For example, advertisers who incorporate advertising into youth production content should make this clear, using language that will be easily understood by the intended audience.

For more information, consult the CARU's guidelines

EUROPEAN UNION

Directives 2005/29/EC and 2006/114/EC concerning unfair business-to-consumer commercial practices

Directive 2006/114/EC prohibits misleading advertising, while Directive 2005/29/EC covers business-to-consumer commercial practices. The latter prohibits misleading, aggressive and rogue practices such as deceptive marketing and unfair advertising, listing various **commercial practices considered unfair**. Directive 2005/29/EC also includes a **provision on children** whereby it is unlawful to include "in an advertisement a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them."

Electronic Commerce Directive 2000/31/EC

This directive covers the liability of operators established in the EU for online services (including those funded by advertising), electronic transactions and other online activities, entertainment services (video on demand), marketing, direct advertising and access to internet services. The directive repeatedly underscores the importance of protecting minors.

For full details on the European legal apparatus, visit the European Parliament website

FRANCE

Code de la consommation (Consumer Code) and Code d'éthique (Code of Ethics) of the Autorité de régulation professionnelle de la publicité

In France, the only tool that covers online advertising directed at children is the **Code of Ethics** issued by the French advertising regulation authority, the**Autorité de régulation professionnelle de la publicité (ARPP)**. The code contains a number of pertinent recommendations and applies to **all ads aired in France, regardless of media**. The **Consumer Code** sets forth provisions prohibiting misleading advertising without being specific to children.

To see the code's provisions in full, consult the following document, available on the ARPP website (in French only)

For more information on the French government's position on deceptive marketing practices (in French only): Le portail de l'Économie et des Finances

AUSTRALIA

Australian Consumer Law

Federal law that generally prohibits misleading conduct in the business environment, including advertising. It applies to all companies that do business in Australia. It has **no provision for advertising directed at children**.

For more information, consult the Australian Consumer Law guidelines

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Apple App Store

Apps cannot use push notifications to issue advertising or promotional offers. Apps in the Kids Category may not include behavioural advertising, while any contextual ads presented in the app must be appropriate for kids.

Additional information

Amazon Appstore

Regarding embedded advertising, your use of the user information generated by players' interactions with embedded ads must comply with Amazon's privacy requirements. You cannot use push notifications to issue advertising or promotional offers.

Additional information

SELF-REGULATION

The section below focuses on the **Canadian self-regulatory system**, which covers advertising directed at children **on digital platforms**.

*Self-regulation on digital platforms draws largely on Advertising Standards Canada's *Broadcast Code for Advertising to Children*

Canadian Code of Advertising Standards

Administered by Advertising Standards Canada (ASC), the code aims to foster and maintain public confidence in advertising. It applies to all forms of advertising distributed through Canadian media and contains **guidelines for advertising to children**.

For more information, consult the ASC's Interpretation Guidelines for Advertising to Children

Digital Advertising Alliance of Canada

Canadian self-regulatory program for online behavioural advertising. For more information, see Backgrounder Online Behavioural Advertising.

Additional information:

Canadian Self-Regulatory Principles for Online Behavioural Advertising

Canadian Marketing Association (CMA) Code of Ethics and Standards of Practice

This code lays out the best practices and key principles for ethical marketing in Canada and applies to all CMA member organizations.

It includes a children's section that urges members to exercise judgment when addressing young audiences, based on the notion that, since children are not adults, not all marketing techniques are appropriate for them. For example, interest-based, targeted or behavioural advertising should not be knowingly used on websites intended mainly for children.

For more information, consult the Code, http://www.the-cma.org/regulatory/code-of-ethics

OUR RECOMMENDATIONS

- If you're designing a platform for a television broadcaster, consult the Broadcast Code for Advertising to Children as well as the broadcaster's internal policies in the matter.
- E-commerce platforms must be incorporated into the parents' section, behind a parental gate appropriate to the age of your target audience.
- Avoid using third parties who collect information for the purposes of behavioural advertising.
- If you want to use an ad network, choose a supplier who can provide you with tools to limit and monitor the kinds of messages displayed.

1. Be transparent about your targeted advertising practices: when you collect tracking data, notify users in a clear and comprehensible manner — for example, using a banner or interactive tool.
2. Give users a chance to opt out of behavioural advertising without barring their access to your platform. The withdrawal must take effect immediately and remain valid for future connections.

- As needed, explain your practices with regard to behavioural advertising in your privacy policy. Include a description of the roles of the various parties involved.
- On your app's overview page, provide a clear and simple description of the type of advertising children will view on your platform.
- If your mobile app has embedded advertising, then for security reasons, block features allowing users to directly call a phone number or follow a Web link leading outside the app.
- If your company is based in Canada but your platform is available in other countries, get legal advice to determine whether your advertising practices may entail legal obligations abroad.

FOOD INDUSTRY PLEDGES

A number of pledges have been issued by the food industry in all jurisdictions in response to pressure groups who point to the marketing industry as a determining factor in childhood obesity. This demonstrates the industry's willingness to engage with children's health and welfare.

- Canada: Canadian Children's Food and Beverage Advertising Initiative
- United States: Children's Food and Beverage Advertising Initiative
- Europe: EU Pledge
- France: Guide des bonnes pratiques de communication nutritionnelle (in French only)
- Australia: Responsible Children's Marketing Initiative

- **Québec: **commercial advertising directed at children under 13 years of age is strictly prohibited across Québec, barring certain exceptions prescribed by regulation**. The ban, which also applies to **companies based outside the province**, will affect:
  - The incorporation of an age-based filter system for platforms whose audience includes users older than 13 years of age
  - The decision to host an advertising network on your platform
  - Methods used to promote contests
  - The content of your newsletter and other mailings
  - Any e-commerce platform you choose to set up

Bibliography.

BACKGROUNDER 17. E-COMMERCE PLATFORMS

Addresses products that directly sell tangible or intangible (virtual) goods to users.

DEFINITION

1.1 Online transactions

An e-commerce platform is a means used to sell tangible or intangible products or services directly to users. "Tangible" goods are material items (for example, spin-off products linked to your website); "intangible" goods, which are non-physical, include virtual currency and downloadable media content. Payment is made electronically by credit card, SMS or a prepaid card purchased at a retail outlet. **The information in this backgrounder addresses credit card transactions**.

You must provide the information needed to allow users to make informed buying decisions: a detailed product description, costs (e.g. one-time or periodic payments, shipping fees), delivery terms, returns and so on.

1.2 Security and protection of personal information

Safeguarding personal data is essential to establishing consumer confidence in e-commerce transactions. To process online sales, payment systems require a great deal of consumer information: contact details, credit card information, bank account number, transaction history and personal identification number (PIN). **To protect personal information throughout every stage of the payment process**, it is vital to partner with third parties whose payment solutions meet the highest security standards.

Your platform must have **a digital certificate** attesting that the data transmitted to your website are encrypted to protect against loss, alteration and theft. Certificates can be obtained from the following companies:

- Verisign
- Thawte

1.3 How does data circulate during a transaction?

1. Clients place their items in a "shopping cart," enter their banking information on the transaction form and confirm their purchase.
2. The data on the form is transmitted to a **secure server** that encrypts data.
3. The encrypted data is sent to a **payment processing service** that serves as the gateway between the merchant and the **financial networks**processing the transaction. Payment gateways **link transactions to an ID**, thus anonymizing cardholder data.

4. The merchant receives the ID from the payment processor.

1.4 Processing payments

Various services let you conclude your online sales transactions. While companies like PayPal generally take care of the entire process, other full-solution providers can offer special features adapted to the needs of your platform — for example, processing digital content sales or providing secure payment solutions designed especially for children.

For more information on e-commerce principles, the following Ontario government document covers the topic in detail:

E-commerce: Purchasing and Selling Online

REGULATIONS

Online transactions are subject to consumer protection and e-commerce security measures. What's more, given the nature of the information required to make an online payment, **platform operators as well as any third parties involved in payment processing must comply with legislation covering personal data handling**. For more information, consult Backgrounder Collection of Personal Information.

CANADA

1. **Competition Act**

Federal law governing commercial practices on all media platforms; includes a provision prohibiting deceptive marketing practices. The Act applies to all companies doing business in Canada. It **has no special provisions for children**.

2. **Consumer Protection Act**

Provincial legislation governing commercial practices, including e-commerce.

Additional information:

- Competition Act
- Provincial/territorial legislation

*****QUÉBEC*****

Consumer Protection Act

Québec's *Consumer Protection Act* prohibits commercial advertising directed at children under 13 years of age **on all media platforms, barring certain exceptions prescribed by regulation.** The law applies to messages addressed to children in Québec, **even for companies based outside the province**. If your paid services include in-app purchases, you must be careful about how these are advertised. See Backgrounder Embedded Advertising andBackgrounder Monetization, for more information.

For credit card purchases, the Act also permits chargebacks. If a merchant fails to meet certain requirements — for example, refusing to reimburse the consumer following cancellation of an online purchase — the consumer can make a chargeback request with the credit card company. Note that chargeback claims are subject to a relatively short time limit.

For further information on commercial advertising directed at children

For more details on the chargeback mechanism

UNITED STATES

Federal Trade Commission Act

Federal law stating that advertising should not be misleading or deceptive. This law covers e-commerce and indicates that, to be authorized, all transactions must be based on the cardholder's informed consent.

For more information, see Advertising and Marketing on the Internet: Rules of the Road

EUROPEAN UNION & FRANCE

Directive on Consumer Rights

This Directive covers online sales and has specific provisions imposing obligations on digital content producers. Producers must provide the following information:

- Product description: system requirements and technical restrictions, details on basic features, known limitations (e.g. not PC-compatible), price (including future subscription costs), information on in-app purchases for freemium/free-to-play products
- Sales terms and conditions: withdrawal period, returns and reimbursement, shipping and delivery
- Company details: name and geographical address, contact information (email and phone)

This information should be available on the product description page, sent by email at time of purchase and readily available at all times on the platform. Furthermore, the Directive grants consumers the right to withdraw from the contract (a.k.a. the **right of return**) within 14 days of the transaction. To avoid an excessive number of refund requests, producers can ask consumers

to **waive their right of withdrawal** by checking a box marked "Order with obligation to pay," which serves as express consent.

Directive on Unfair Commercial Practices

This Directive prohibits unfair, misleading and aggressive business-to-consumer practices and sets out a series of practices to be avoided. It also includes a **provision for children** whereby ads must not include "a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them."

Electronic Commerce Directive

This Directive targets operators established in the EU for online services, electronic transactions and other online activities, entertainment services (video on demand), marketing, direct advertising and access to internet services.

The Directive repeatedly underscores **the importance of protecting minors.** For instance, with regard to unfair practices, the Directive states that**mobile app stores must remove any apps that directly prompt children to make in-app purchases**. It also states that companies must provide the consumer with all essential information and that purchases can only be made with the consumer's express consent.

Additional information:

- The Directive on Consumer Rights
- European Parliament, Consumer protection measures

AUSTRALIA

Australian Consumer Law

National law that governs business practices.

Electronic Transactions Act

Law of the Commonwealth that covers specific areas of e-commerce, like the validation of electronic signatures.

Additional information:

Australian Competition and Consumer Commission

Electronic Transactions Act

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Mobile app stores do not allow you to include a direct link to your online store. The only way to sell virtual goods through your app is through in-app purchases. Additional information:

- Apple App Store

- Amazon Appstore
- Google Play

SELF-REGULATION

Canadian Code of Practice for Consumer Protection in Electronic Commerce

The Code establishes good business practice benchmarks for merchants who conduct commercial activities with consumers online. Among its eight key principles are statements to the effect that vendors:

- Cannot hold consumers liable for any charges related to a transaction to which the consumer has not consented
- Must apply effective security mechanisms consistent with current industry standards to protect the integrity and confidentiality of payment and other personal information provided by consumers, as well as ensure that any third parties involved in the payment process do the same
- Must take **all reasonable steps to prevent monetary transactions with children**

To consult the Code

Canadian Marketing Association (CMA) Code of Ethics and Standards of Practice

This code lays out the best practices and key principles for ethical marketing in Canada and applies to all CMA member organizations. It also includes a section dedicated to the question of children that recommends against:

- Knowingly accepting an order from a child without the parent's express consent
- Pressuring children to urge their parents or guardians to purchase a product or service

For more information, consult the Code online

OUR RECOMMENDATIONS

- Make your privacy policy prominently visible and easily accessible.
- Your privacy policy must be **up to date**. It must clearly and concisely lay out your practices regarding the collection and handling of personal information as well as the security measures you have implemented to protect this information.
- Periodically verify your payment processor's personal information handling practices.
- Your e-commerce platform must address parents and be hidden behind a parental gate. For older children, be sure to include a message such as: "You must be accompanied by a parent to make purchases in the online store."
- Install alert systems to detect suspect transactions or accidental purchases — for example, when a high volume of micro-transactions is recorded within a short timeframe.

Bibliography.

BACKGROUNDER 18. MONETIZATION

Looks at different forms of monetization used on youth platforms.

DEFINITION

1.1 Common business models

There's a degree of confusion surrounding the terms used to describe the various monetization models for digital goods, given the often-subtle distinctions between them. Below are the most common pricing strategies.

- **Freemium**: the platform provides a core version free of charge along with the offer of purchasable "premium" content or services (e.g. access to exclusive areas). The term *freemium* — a combination of "free" + "premium" — is generally used to describe this model.
- **Free-to-play (F2P)**: the platform offers a free version along with individual purchasable features that enhance the user experience (e.g. additional tries, the ability to skip levels, etc.). In this model, everyone has access to the same platform; however, the progress of users who do not pay will be generally slower.
- **Premium or paid**: this strategy features no free version; instead, the user must pay an upfront price to access the platform. The product may be purchased through a **one-time payment** or by **subscription** (recurring fees).

1.2 In-app purchases

In-app purchases consist of a **simplified payment process** that links the user's account to a form of credit (credit card/prepaid card). Users can thus purchase virtual goods **without leaving the platform**. Known as "microtransactions," in-app purchases are a **key feature of freemium and F2P products**. For instance, to make a purchase while using an app downloaded from Apple's App Store, the user enters his/her Apple ID, the transaction is charged to the credit card linked to his/her iTunes account and the virtual goods are downloaded instantly.

1.3 Accidental or unauthorized purchases

While adults understand that in-app purchases will be charged to a credit card and paid for in real money, this principle can be far less clear to children. A youngster faced with the choice of waiting a half-hour to obtain one "life" or of buying "diamonds" that provide 10 lives straight away is extremely likely to be tempted by the latter. Children do not necessarily have the **maturity or consumer savvy** to assess **the value of the purchase** or even **grasp that real money is involved**.

There have been all too many cases of children racking up bills worth hundreds of dollars in a matter of minutes through in-app purchases. Although the problem lies in part with app store billing practices, **apps must still reimburse "unauthorized purchases"** at the request of the cardholder — i.e. the parent.

1.4 The child/user and parent/payer dynamic

A youth platform is aimed at both children and parents: each has their own expectations and objectives, but both have a say in the purchase. This mechanism creates substantial challenges in terms of monetization, especially in the digital environment where in the vast majority of cases, the parent is the one providing the payment. Unless they have an iTunes-type prepaid card, children wishing to use a paid app must ask their parents to pay for it with their credit card.

You are responsible for taking reasonable measures to ensure that parents/cardholders provide their express and informed consent for each purchase.

1.5 After-sales services and technical support

For paid services — even low-priced services — user expectations about customer service are usually higher than for freemium or F2P services. Whether for billing inquiries, subscription renewals or installation issues, after-sales support is a vital aspect of product quality. Users should be able to easily reach customer service at all times.

REGULATIONS

Monetization models are subject to **e-commerce and consumer protection laws**. The concept of online payment entails the **collection of personal information.** For more information, consult backgrounders Collection of Personal Information and E-commerce Platforms.

CANADA

1. **Competition Act**

Federal law governing commercial practices on all media platforms; includes a provision prohibiting deceptive marketing practices. The Act applies to all companies doing business in Canada. It has **no special provisions for children**.

2. **Consumer Protection Act**

Provincial legislation governing commercial practices, including e-commerce.

Additional information:

- Competition Bureau, Application of the *Competition Act* to Representations on the Internet
- Provincial/territorial legislation

*****QUEBEC*****

Consumer Protection Act

Québec's *Consumer Protection Act* **prohibits commercial advertising directed at children under 13 years of age on all media platforms, barring certain exceptions prescribed by regulation.** The ban applies to messages addressed to children in Québec, **even for companies based outside the province.**

Additional information:

Office de la protection du consommateur, Advertising Directed at Children under 13 Years of Age

UNITED STATES

Federal Trade Commission Act

Federal law stating that advertising should not be misleading or deceptive. This law covers e-commerce and indicates that, to be authorized, all transactions must be based on the cardholder's informed consent.

For more information, visit the Federal Trade Commission online. Advertising and Marketing on the Internet: Rules of the Road

EUROPEAN UNION & FRANCE

Directive on Consumer Rights

This Directive covers online sales and has specific provisions imposing obligations on virtual goods. Producers must provide the following information:

- Product description: system requirements and technical restrictions, details on basic features, known limitations (e.g. not PC-compatible), price (including future subscription costs), information on in-app purchases
- Terms and conditions: withdrawal period, returns and reimbursement, shipping and delivery
- Company details: name and geographical address, contact information (email and phone)

This information should be available on the product description page; sent by email at time of purchase; and readily available at all times on the platform. Furthermore, the Directive grants consumers the right to withdraw from the contract (a.k.a. the **right of return**) within 14 days of the transaction. To avoid an excessive number of refund requests, producers can ask consumers to **waive their right of withdrawal** by checking a box marked "Order with obligation to pay," which serves as express consent.

EU member states, in association with the *Directive on Consumer Rights*, have drafted a **Common Position on freemium games**:

- Games advertised as "free" must not mislead the consumer as to the real costs entailed.
- Games **must not directly encourage children to either make in-app purchases** or try to convince an adult to make the purchase for them.

- Consumers must be clearly informed about payment arrangements for in-app purchases, and the default setting for payments should not allow purchases to be made without the consumer's express consent.
- Consumers should be clearly provided with the vendor's email address for any queries or complaints.

Unfair Commercial Practices Directive

This Directive prohibits misleading, aggressive and rogue business-to-consumer practices. It states that "[d]escribing a product as 'gratis', 'free', 'without charge' or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item" as a misleading practice. The Directive also presents a series of commercial practices to avoid, including a **provision for children**whereby it is unlawful to include "in an advertisement, a direct exhortation to children to buy advertised products or persuade their parents or other adults to buy advertised products for them."

E-Commerce Directive

This directive targets operators established in the EU for online services, electronic transactions and other online activities, entertainment services (video on demand), marketing, direct advertising and access to internet services.

The directive repeatedly underscores **the importance of protecting minors.** For instance, with regard to unfair practices, the Directive states that **mobile app stores must remove any apps that directly prompt children to make in-app purchases**. It also states that companies must provide the consumer with all essential information and that purchases can only be made with the consumer's express consent.

Additional information:

- Common position on "free" online games (Common position of national authorities within the CPC)
- The Directive on Consumer Rights
- European Parliament, Consumer protection measures

AUSTRALIA

Australian Consumer Law

Federal law that prohibits misleading commercial practices. The Australian Competition and Consumer Commission — the organization responsible for enforcing it — has issued **recommendations for mobile apps with in-app purchases** such as: "App stores [should] develop clear, publicly-available, age-appropriate rating systems which include consideration of in-app purchases and any encouragements to spend money."

Additional information:

Australian Competition and Consumer Commission

Australian Communications Consumer Action Network, App purchases by Australian consumers

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

App stores must obtain parents' express and informed consent before billing for in-app purchases. This entails:

- Features for blocking in-app purchases
- Indicating the presence of in-app purchases in the app description
- Making a password obligatory for each app purchase

Amazon, Apple and Google state that in-app purchases are for the sale of virtual goods only: they cannot be used to sell products or services that will be supplied or used outside of the application.

Apple App Store

- Apps in the **Kids Category** must obtain **parental consent** or use a **parental gate before allowing the user to make a purchase.**
- The In-App Purchase (IAP) system is the only one permitted for the sale of virtual goods in an application: external shopping mechanisms (e.g. a "Buy" link) are inacceptable.
- Automatic subscription renewal is acceptable only for periodical apps (e.g. newspapers, journals, magazines), business apps (ex. Cloud storage services) and media content (video and audio).

Additional information:

- Apple App Store
- Amazon Appstore
- Google Play

SELF-REGULATION

Canadian Code of Practice for Consumer Protection in Electronic Commerce

The Code establishes good business practice benchmarks for merchants who conduct commercial activities with consumers online. Among its eight (8) key principles are statements to the effect that vendors:

- Cannot hold consumers liable for any charges related to a transaction to which the consumer has not consented
- Must take **all reasonable steps to prevent monetary transactions with children**

To consult the Code

Canadian Marketing Association (CMA) Code of Ethics and Standards of Practice

This code lays out the best practices and key principles for ethical marketing in Canada and applies to all CMA member organizations. It includes a section dedicated to the question of children that recommends against:

- Knowingly accepting an order from a child without the parent's express consent
- Pressuring children to urge their parents or guardians to purchase a product or service

For more information, consult the Code online

OUR RECOMMENDATIONS

- In freemium and F2P models, be careful about how you promote purchases. Never directly exhort children to buy virtual goods or subscriptions; instead, provide clear and accurate information as objectively as possible. For example, when the child exhausts her virtual currency, rather than saying, "You're out of diamonds. Buy some diamonds NOW!" (with a clickable "Buy" link), adopt an informative tone: "You have no more diamonds. You can buy more diamonds at the store for real money. Or you can earn some by successfully completing challenges." Either way, ensure that the parent remains responsible for completing or authorizing the transaction by making the necessary arrangements (described below).
- Keep your audience in mind when incorporating in-app purchases into your platform:
    - Avoid game mechanisms that require children to seek help from friends on social networks — for example, "Ask your Facebook friends for some lives!"
    - Avoid formulations that exploit children's inexperience. For instance: "Your rabbit's starving! Quick, get some carrots at the store!" Or: "Buy this new car to boost your popularity right now!"
    - Provide a detailed explanation of the full costs associated with your platform **before** the user downloads, subscribes or makes a payment:
        - The initial cost of the registration, subscription, download or purchase
        - Subsequent and unavoidable costs to continue to use the platform (e.g. a monthly subscription fee of $2.99)
        - Optional extras, e.g. in-app purchases
- Implement parental control tools to prevent purchases without the parent's explicit consent. Place in-app purchases behind a parental gate adapted to your users' age range (e.g. something beyond a child's abilities, like an algebraic equation or touching all four corners of a tablet computer at the same time). Make it possible to disable in-app purchases or place them in a section accessible only to parents.
- Ensure that your communications are as accurate as possible with regard to the suggested transactions:
- In-app purchases
    - Why are they being offered?
    - What's the price range?

    - Is this a recurring fee?
    - How are they presented in the product?
    - What actions are required to authorize/prevent this type of transaction?
    - How is prevention implemented?
    - What is your reimbursement policy in the event of unauthorized purchases?
- Subscriptions
    - How often is new content added?
    - When is the subscription billed?
    - How long is the content available for?
    - Is renewal automatic?
    - How can a subscription be cancelled?
    - Is the content still available after the subscription expires?
- Provide all the information about your platform's specs needed to make an informed purchasing decision:
    - A short product description
    - A reminder of the key points in the terms of use
    - A list of the personal information collected and a link to the privacy policy
    - Customer service contact information
    - Details about the content (e.g. available languages, duration, resolution, regional restrictions, etc.)
    - Hardware/operating system compatibility information
    - The presence of marketing
    - The presence of social features
- Help parents set parental controls. For example, in the parents' section, explain the procedure for changing the device's security settings.
- Customer service contact information should be updated as needed and easily accessible at all times. It's also preferable to include more than one option for reaching your customer service (e.g. a phone number and an email address).

Bibliography.

BACKGROUNDER 19. MAINSTREAM SOCIAL MEDIA

Presents the issues related to integrating mainstream social networks (e.g. Facebook, Instagram, Twitter) into a youth platform.

DEFINITION

1.1 Social media and youth platforms

Integrating social media is a common marketing practice for mainstream products. However, in youth production, this practice becomes problematic.To comply with U.S. legislation on the collection of personal information, most mainstream social networks require users to be 13 years of age or older to open an account. Furthermore, since these platforms are rarely moderated, they **expose children to a number of risks**, including contact with strangers,cyberbullying and inappropriate content. **Incorporating social media into your platform sends out the wrong message**: you invite children to lie about their age (Backgrounder 7, 1.2) to access websites that, inaccessible to users under 13, can expose them to various risks.

You are **responsible for creating a safe environment** that does not encourage your users to lie to gain access to potentially dangerous websites.

REGULATIONS

In general, regulators consider **mainstream social networks inappropriate for children under the age of 13**, since they expose their users to various risks. Children generally **do not have the required maturity** to handle these risks. The U.S. is the only country to provide specific guidance on the integration of mainstream social media into youth products.**UNITED STATESChildren's Online Privacy Protection Act (COPPA)**

Federal law to protect personal information about children collected online. COPPA applies to products that collect personal information from U.S. children under 13 years of age, **including collection by companies based outside the U.S.**

Operators are responsible for ensuring that any third parties who collect information through their platforms comply with COPPA rules. This includes social media plug-ins (such as "Follow us on Twitter" or the Facebook "Like" button), which often employ tracking technologies. Given that **the information collecting practices of mainstream social media constitute a violation of COPPA** if the user is under 13, and considering that the **operators of child-directed websites are strictly liable** for any personal information collected through their platforms, **you shouldn't incorporate social media** if your platform addresses an audience under the age of 13.

Additional information:

Federal Trade Commission: Complying with COPPA: Frequently Asked Questions

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Apple App Store For Kids Category apps, the App Store recommends clearly indicating in the app's intro page whether it contains **social features**, i.e. those that put the child in contact with other users or allow information to be shared through the app (e.g. top scores in a game, social media sharing features, etc.).

Additional information

SELF-REGULATION

None of the main Canadian self-regulatory bodies address the topic of social media on youth platforms.

OUR RECOMMENDATIONS

- If your platform's **target audience** is **exclusively in the "under 13 years of age" category, avoid integrating mainstream social media**.

Source: Justin's World

- Access to social media integrated into a platform aimed at ages 13 and under should be **strictly limited to the parents' section**.
- If you integrate social media into the parents' section, place **an age-appropriate parental gate** to prevent children from accessing the area.
- If your **target audience is partially in the "under 13 years of age" category**, install an **age filter**. This limits access to social media to the part of the site open to ages 13 years and up only.
- If you use an age filter, it's smarter to ask children to **enter their date of birth** (DD/MM/YYYY) **rather than have them tick a box** saying "age 13 and over"/"Aged under 13."

Bibliography.

BACKGROUNDER 20. CYBERBULLYING

Examines the problem of cyberbullying and provides tips on how to prevent or intervene in a situation of online harassment.

DEFINITION

1.1 What is cyberbullying?

It's a situation in which an abuser **voluntarily and repeatedly** violates a victim online with a view to humiliating, threatening or harassing them. On participatory platforms, this can manifest in a number of ways such as:

- Sending unwanted, nasty, threatening or insulting messages
- Targeting someone by inviting others to make fun of them
- Pressuring others to exclude the victim from the community
- Impersonating the victim to issue inappropriate messages that causes others to respond negatively to the victim
- Sharing the victim's content without their consent

1.2 How can you prevent cyberbullying on your platform?

Cyberbullying is essentially prevented through **moderation**. Unacceptable behaviours are set out in the digital code of conduct; your moderation strategy should seek to ensure compliance with the code. You must also be prepared to apply the appropriate sanctions in the event of violations.

Furthermore, you should provide tools that let users notify you if they are bullied on your platform. These include features for blocking users and thus preventing any future contact as well as whistle-blowing mechanisms.

1.3 When cyberbullying is flagged, how should it be handled?

Cyberbullying is a serious issue and reports of bullying must be taken seriously. As a youth platform, you must promote respect for other users and take prompt action in the event of disrespectful behaviour.

Your moderators should establish procedures for responding to reports of bullying based on your digital code of conduct. Consequences that gradually increase in severity ranging from a simple warning to closure of the account must be imposed as needed. Depending on the gravity of the incident, you can also direct the victim to resources offering specialized support.

REGULATIONS

Each country regulates cyberbullying through differing laws based on the actions of the aggressor. As operator, your role is to punish the offender and direct the victim toward resources. Below is a list of anti-cyberbullying organizations by country:

CANADA

- KidsHelpPhone
- CyberTip!ca
- ca

INTERNATIONAL

- The CyberSmile Foundation

UNITED STATES

- Stop Bullying
- Cyberbullying Research Center

FRANCE

- Internet signalement

AUSTRALIA

- Kids Help
- Cyber (smart)
- Lifeline

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Mobile app stores make no specific mention to cyberbullying in their terms of use.

SELF-REGULATION

The question of cyberbullying is covered by existing legislation.

OUR RECOMMENDATIONS

- Ensure that your digital code of conduct encourages civil behaviour and denounces disrespectful acts toward other users. Specify that repeated violations of the code will entail temporary or permanent suspension of the user's account.
- Design your platform in such a way as to give young people a chance to think before acting. For example, use pop-up windows to display messages like "Are you sure you want to share this?"

- Encourage victims to discuss a bullying situation with their parents.
- If you have the parent's email address, you can send them a message outlining the situation and the steps you have taken to manage it. This applies to the parents of both the victim and the aggressor.
- When you intervene with an aggressor, make sure they understand the following: the nature of the misconduct; how this behaviour violates thedigital code of conduct; and the consequences that will ensue if the aggressor repeats the offence. For example:

On our platform, we do not tolerate disrespect toward other users. Your comment "[*insert comment*]" dated January 1, 2011 addressed to User12 fails to comply with our digital code of conduct [*insert link to your code*]. This is your first warning. If you display a similar lack of respect toward a user again, your account will be suspended for three days."

Bibliography.

BACKGROUNDER 21.
SAFEGUARDING CHILDREN FROM PREDATORS

Addresses the subject of predators — users who take advantage of Internet anonymity to make contact with minors — along with preventive and screening measures.

DEFINITION

1.1 What is a "predator"?

Predation wears many faces but one thing is certain: an online predator is an individual who uses the anonymity of a participatory platform to make contact with children.

A predator **exploits the naivety of young people** who, for lack of experience, are less likely to be suspicious. Predator tactics range from posing as a child to gain the victim's trust to revealing themselves as an adult from the start, then seducing their victims by showing them attention, kindness and affection. Predators generally set out to commit some form of **sexual offence**, such as:

- Asking the child to send explicit content (e.g. nude photos of the child)
- Encouraging the child to participate in sexual activities via webcam
- Initiating a sexually oriented conversation via chat
- Inviting the child to meet in person

1.2 How can predation be prevented?

Preventing predators from using your platform essentially hinges on your **moderation strategy**. Your digital code of conduct identifies which behaviours are unacceptable; your moderation strategy then ensures that these rules are enforced.

1.3 How can predators be screened?

Predator screening is primary accomplished through **moderation (monitoring online interactions)** and by processing **complaints received through reporting mechanisms**.

Predators know that most youth platforms are closely moderated. Because of this, they rarely risk any gestures that would be easily detected. Instead, they set out to obtain **information that will let them contact the child outside of your platform** in a less controlled environment. Pay attention to repeated and insistent **requests for personal information** (age, address, city of residence, etc.) or **suggestions to meet up on another platform** (e.g. Facebook or Skype).

Warning! **Violations do not always equal predation**. Children also transgress the rules; doing so is "normal" behaviour to an extent. However, **predators tend to commit the same violation repeatedly**. For example, let's say that after issuing a number of warnings to a user who repeatedly solicits personal information, you close that user's account. If the same email address then opens a new account under a new pseudonym and again commits the same type of violation, this could indicate a predator.

Predators can be very patient when it comes to building a relationship with a child over time that lets them accumulate information bit by bit. While such an approach is more difficult to detect, **data crossing-referencing** can reveal behaviour of this kind.

1.4 What if you think you've identified a predator on your platform?

Believing you've identified a potential predator on your platform **is a serious matter**. Sexual offences against minors are covered by the criminal codes of all Western countries. Accordingly, you have a **moral and legal obligation to report suspicious behaviour towards children**.

Keep the account active to enable an investigation and **gather information about the suspected predator** (username, email address, comments, conversation history, etc.). **Forward the information** to your local police department or a child protection agency, which will assess the case and tell you how to proceed. The section below lists child protection organizations by country.

REGULATIONS

The sexual exploitation of children on the Internet is a **criminal act**. As a youth platform operator, **it is your duty to report suspicious behaviour to the authorities**, such as:

- Your local police force
- National child protection organizations
- International bodies mandated to protect children from online sexual exploitation

Whatever authority you contact, your report will be evaluated and contentious cases referred to the **local law enforcement agency**, which will **take the action needed and tell you how to proceed**. Below is a list of the major organizations by country:

INTERNATIONAL BODIES

- Virtual Task Force
- Inhope

CANADA

- Canadian Centre for Child Protection
- Cybertip!ca

UNITED STATES

- National Center for Missing & Exploited Children

FRANCE

- Internet-signalement

AUSTRALIA

- Australian Federal Police
- Think U Know

MOBILE APPLICATION DISTRIBUTIONS PLATFORMS

Mobile app stores do not specifically address the question of sexual predators in their terms of use.

OUR RECOMMENDATIONS

- It is your responsibility to take steps to prevent predation and protect your audience, which consists of vulnerable users. **User safety must be a priority**. Consequently, you must provide the **financial, human and technical resources needed to support** a **moderation strategy** appropriate to your platform.
- User and content moderation must be adapted to your platform's features as well as its audience:
    - The more opportunities for interaction between users, the greater the vigilance required.
    - Studies show that **the most at-risk youth are not the youngest, but rather tweens and teens**. Take extra precautions with these age groups.
- Choose your moderators with care and train them to recognize the signs that could indicate a predator.
- In high-risk areas (e.g. chatrooms, private messaging, etc.), use a black list to block the input of numbers, thus preventing personal information like addresses or phone numbers from being shared.
- Establish effective procedures for dealing promptly with complaints received through the reporting mechanism.
- If you think you have a predator on your hands, report the situation to a qualified authority or law enforcement agency.

Bibliography.

BIBLIOGRAPHY – IDENTITY AND PERSONAL INFORMATION

WORKS

Caron, A. H., Cohen, R. I. (2013). *Regulating Screens: Issues in Broadcasting and Internet Governance for Children*. Montréal, McGill-Queen's University Press.

Caron, A. H. (2011). Les enfants devant leurs écrans; la réglementation canadienne de la télévision à l'internet, Presses de l'université de Montréal, 176 pages.

GOVERNMENT AND OFFICIAL ORGANIZATION WEBSITES

Advertising Standards Canada, Interpretation Guideline #2– Advertising to Children, http://www.normespub.com/en/Standards/interpretationGuideline2.aspx

Australian Government – Office of the Australian Information Commissioner, Privacy fact sheet 17: Australian Privacy Principles,http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

Australian Government – Office of the Australian Information Commissioner, Privacy fact sheet 4: Online behavioural advertising – know your options,http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-4-online-behavioural-advertising-know-your-options

Australian Government – Office of the Australian Information Commissioner, Privacy law reform, http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform

California Legislative Information, SB-1177 Privacy: Students, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

CEFRIO, Gérer les enjeux et les risques juridiques du Web 2.0, http://www.cefrio.qc.ca/media/uploader/guide_juridique_Web2.pdf

Children's Online Privacy Protection Act, How to comply with the Children's Online Privacy Protection Act, http://www.coppa.org/comply.htm

Commission nationale de l'informatique et des libertés, Entreprise, vos obligations, http://www.cnil.fr/vos-obligations/vos-obligations/

Digital Advertising Alliance of Canada, The Canadian Self-Regulatory Principles for Online Behavioural Advertising, http://youradchoices.ca/wp-content/uploads/2013/08/The-Canadian-Self-Regulatory-Principles-for-Online-Behavioural-Advertising.pdf

Direct Marketing Association, "How to Comply With The Children's Online Privacy Protection Rule (COPPA)," http://www.the-dma.org/privacy/HowtoComplywithCOPPA-PDFVersion.pdf

Direct Marketing Association, Online Behavioural Advertising Compliance Alert & Guidelines for Interest-Based Advertising,http://www.dmaresponsibility.org/privacy/oba.shtml

Europa, Handbook on European data protection law, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

EUR-Lex, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

EUR-Lex, Protection of personal data, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012

Federal Trade Commission, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Federal Trade Commission, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing,https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf

Future of Privacy, Best Practices for Mobile Applications Developers, http://www.futureofprivacy.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf

Government of Alberta, Personal Information Protection, http://servicealberta.ca/pipa/

Government of British Columbia, Personal Information Protection Act, http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Government of Canada – Canadian Radio-television and Telecommunications Commission, Canada's Anti-Spam Legislation, http://www.crtc.gc.ca/eng/casl-lcap.htm

Government of Canada – Canadian Radio-television and Telecommunications Commission, Canada's Anti-Spam Legislation Requirements for Installing Computer Programs, http://www.crtc.gc.ca/eng/info_sht/i2.htm

Government of Canada – Competition Bureau, Ensuring Truth in Advertising: Mass Marketing Fraud, http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02775.html

Government of Canada – Consumer Information, Provincial and Territorial Legislation, http://www.infoconsommation.ca/eic/site/032.nsf/fra/01173.html

Government of Canada – Justice Laws Website, Personal Information Protection and Electronic Documents Act, http://lois-laws.justice.gc.ca/eng/acts/p-8.6/index.html

Government of Canada – Office of the Privacy Commissioner of Canada, Fact Sheet: Web Tracking with Cookies, https://www.priv.gc.ca/resource/fs-fi/02_05_d_49_02_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Getting Accountability Right with a Privacy Management Program,https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp#i

Government of Canada – Office of the Privacy Commissioner of Canada, Guidelines for Online Consent,https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Policy Position on Online Behavioural Advertising,https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Privacy Toolkit: A Guide for Businesses and Organizations,https://www.priv.gc.ca/information/pub/guide_org_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Securing Personal Information: A Self-Assessment Tool for Organizations,https://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1

Government of Canada – Office of the Privacy Commissioner of Canada, Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps,https://www.priv.gc.ca/information/pub/gd_app_201210_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency, https://www.priv.gc.ca/resource/fs-fi/02_05_d_56_tips2_e.asp

Government of Nova Scotia – Department of Health and Wellness, Marketing to Children and Youth: A Public Health Primer, http://novascotia.ca/dhw/healthy-communities/documents/Marketing-to-Children-and-Youth-A-Public-Health-Primer.pdf

Government of Québec, An Act respecting the protection of personal information in the private sector,http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html

Government of Québec – Services Québec, Entreprises: Concurrence et pratiques interdites, http://www2.gouv.qc.ca/entreprises/portail/quebec/gerer?g=gerer&t=o&e=1427036613

Government of Québec, Office de la protection du consommateur: Advertising Directed at Children Under 13 Years of Age,http://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EN_Guide_publicite_moins_de_13_ans_vf.pdf

MediaSmarts, Taking Action – Marketing and Consumerism, http://mediasmarts.ca/marketing-consumerism/parents-taking-action-marketing-and-consumerism

Privacy Matters, FERPA, PPRA And COPPA, http://www.studentprivacymatters.org/ferpa/

REFEDS, Student Information in the USA and EU, https://refeds.org/wp-content/uploads/2015/05/FERPA-DPD-v1-00.pdf

Student Data Principles, http://studentdataprinciples.org/

Student Privacy Pledge, http://studentprivacypledge.org/

U.S. Department of Education, Protecting Student Privacy While Using Online Education Services: Model of Terms and Services,http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf

U.S. Department of Education, Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices,http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf

Your Online Choices, A Guide to Online Behavioural Advertising: About, http://www.youronlinechoices.com/uk/about-behavioural-advertising

COMMERCIAL WEBSITES

Amazon, App Distribution Agreement, https://developer.amazon.com/appsandservices/support/legal/da

Amazon, FAQs Program Overview, https://developer.amazon.com/public/support/faq#

Apple, App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/#terms-conditions

Apple, Apple Answers the FCC's Questions, http://www.apple.com/hotnews/apple-answers-fcc-questions/

Apple, Business & Education Support, https://www.apple.com/ca/support/business-education/vpp/

AssertID, http://www.assertid.com/coppa/

Google Play, Content ratings for apps and games, https://support.google.com/googleplay/android-developer/answer/188189

Google Play, Google Play Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html

Google Play, Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

Google Play, Personal information, https://support.google.com/googleplay/android-developer/answer/4450969

Google Play, Publish Education Apps, https://developer.android.com/distribute/googleplay/edu/start.html

iKeepSafe, COPPA, http://ikeepsafe.org/privacy/coppa/

ARTICLES AND BLOG POSTS

Advertising Age: Why We All Need to Worry About Children's Privacy, http://adage.com/article/privacy-and-regulation/worry-children-s-privacy/296498/

Borden Ladner Gervais, Targeting the Canadian Consumer: An Important Primer on the Advertising and Marketing Laws in Canada,http://www.blg.com/en/NewsAndPublications/Documents/Targeting_the_Canadian_Consumer_-_Dec_2014.pdf

CooleyGo: How Student Privacy and California's SOPIPA May Affect You, https://www.cooleygo.com/how-student-privacy-and-californias-sopipa-may-affect-you/

CooleyGo: US Department of Education's New Data Privacy Guidance: Why it Matters, https://www.cooleygo.com/us-department-education-data-privacy-guidance/

COPPA Attorney: The COPPA Social Media Button Plug-in Conundrum, http://www.coppalawattorney.com/coppa-social-media-button-plug-in/

Davis & Gilbert LLP: FTC issues updated FAQs on amended COPPA rule, http://www.dglaw.com/images_user/newsalerts/Advertising_FTC_Issues_Updated_FAQs_Amended_COPPA.pdf

Droitdu.net: Google adhère au programme canadien Choix de pub, http://droitdu.net/2014/11/google-adhere-enfin-au-programme-canadien-choix-de-pub/

EngageSciences: Undestanding FTC COPPA Compliance: Social Marketing and Brands,

http://www.engagesciences.com/coppa-compliance-smm-brands/

Gamasutra: What Does a COPPA Compliant Game Really Look Like?,

http://gamasutra.com/blogs/RoySmith/20141022/228308/What_Does_a_COPPA_Compliant_Game_Really_Look_Like.php

Infosec Institute: Difference between the privacy laws in the EU and the US, http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/

iubenda: A Guide to COPPA and Mobile Apps,

http://www.iubenda.com/blog/2013/09/24/guide-coppa-mobile-apps/#gating

Kidsscreen: Who's watching the kids?,

http://kidscreen.com/2015/01/21/whos-watching-the-kids/

Law of the Level: Bargaining with Apple: Understanding the iOS Developer Program License Agreement,

http://www.lawofthelevel.com/2015/02/articles/licensing/bargaining-with-apple-understanding-the-ios-developer-program-license-agreement/

New York Times, "Digital Learning Companies Falling Short of Student Privacy Pledge,"

http://bits.blogs.nytimes.com/2015/03/05/digital-learning-companies-falling-short-of-student-privacy-pledge/?module=BlogPost-Title&version=Blog%20Main&contentCollection=Privacy&action=Click&pgtype=Blogs&region=Body&_r=0

New York Times, "Privacy Pitfalls as Education Apps Spread Haphazardly," http://www.nytimes.com/2015/03/12/technology/learning-apps-outstrip-school-oversight-and-student-privacy-is-among-the-risks.html?ref=business

PlayWell, Why is Student Data Privacy So Complicated?, http://playwell-llc.com/student-data-privacy-complicated/

Practical Law: Data protection: Country Q&A tool, http://uk.practicallaw.com/2-502-1510?qaq=W_q1&qaq=W_q2&qaq=W_q3&qaq=W_q5&qaq=W_q9&qaq=W_q13&qaq=W_q17&qaq=W_q18&qaid=6-502-0556&qaid=6-502-1481

PRIVO: What We Know About the Student Digital Privacy Act, https://privo.com/what-we-know-about-the-student-digital-privacy-act/

BIBLIOGRAPHY –
CONTESTS, SURVEYS AND NEWSLETTERS

WORKS

Caron, A. H., Cohen, R. I. (2013). *Regulating Screens: Issues in Broadcasting and Internet Governance for Children*. Montréal, McGill-Queen's University Press.

Caron, A. H. (2011). Les enfants devant leurs écrans; la réglementation canadienne de la télévision à l'internet, Presses de l'université de Montréal, 176 pages.

GOVERNMENT AND OFFICIAL ORGANIZATION WEBSITES

Advertising Standards Canada, Guideline No. 2 – Advertising to Children, http://www.normespub.com/en/Standards/interpretationGuideline2.aspx

Australian Government – Industry ACMA, Key elements of the Spam Act, http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/key-elements-of-the-spam-act-ensuring-you-dont-spam-i-acma

Australian Government – Office of the Australian Information Commissioner, Can I use my customer database to send a customer a Christmas Card?,http://www.oaic.gov.au/privacy/privacy-topics/business-and-small-business/can-i-use-my-customer-database-to-send-a-customer-a-christmas-card

Australian Government – Office of the Australian Information Commissioner, Information Sheet (Private Sector) 26 – 2008: Interaction between the Privacy Act and the Spam Act, http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-26-2008-interaction-between-the-privacy-act-and-the-spam-act

Australian Government, Gaming (gambling) authorities, http://www.australia.gov.au/content/gaming-authorities

Canadian Marketing Association, Code of Ethics and Regulatory Guidelines, http://www.the-cma.org/regulatory/code-and-guidelines

CEFRIO, Gérer les enjeux et les risques juridiques du Web 2.0, http://www.cefrio.qc.ca/media/uploader/guide_juridique_Web2.pdf

Europa, Handbook on European data protection law, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

EUX-LEX, Data protection in the electronic communications sector, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24120

Federal Trade Commission, CAN-SPAM Act: A Compliance Guide for Business, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Government of Canada, Canada's Anti-Spam Legislation, http://combattrelepourriel.gc.ca/eic/site/030.nsf/eng/home

Government of Canada, Canada's Anti-Spam Legislation and Regulations, http://fightspam.gc.ca/eic/site/030.nsf/eng/00285.html

Government of Canada – Competition Bureau, Enforcement Guidelines: Promotional Contests,

http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/20100409_PromotionalContests-e.pdf/$FILE/20100409_PromotionalContests-e.pdf

Government of France – Legifrance, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1),http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005789847&dateTexte=20080724

Government of France – Service-Public, Quelles sont les mentions obligatoires sur un site internet?, http://vosdroits.service-public.fr/professionnels-entreprises/F31228.xhtml

Government of Québec – Office de la protection du consommateur, Advertising Directed at Children Under 13 Years of Age,http://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EN_Guide_publicite_moins_de_13_ans_vf.pdf

Government of Québec – Office de la protection du consommateur, Concours, tirages et faux concours,http://www.opc.gouv.qc.ca/consommateur/sujet/publicite-illegale/tirage/faux-concours/

Government of Québec – Portail entreprises, Concurrence et pratiques interdites, http://www2.gouv.qc.ca/entreprises/portail/quebec/gerer?g=gerer&t=o&e=1427036613

Government of Québec – Portail entreprises, Publicité aux enfants de moins de 13 ans, http://www2.gouv.qc.ca/entreprises/portail/quebec/marketing?lang=fr&g=marketing&sg=&t=o&e=1700555403:4234500320

Government of Québec – Portail entreprises, Tenue de concours publicitaires, http://www2.gouv.qc.ca/entreprises/portail/quebec/gerer?g=gerer&sg=&t=o&e=2179170523:1700555403:1463643004

Government of Québec – Publications du Québec, An Act Respecting Lotteries, Publicity Contests and Amusement

Machines, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/L_6/L6_A.html

Government of Québec – Régie des alcools, des courses et des jeux, Publicity Contest Notice, https://www.racj.gouv.qc.ca/en/formulaires-et-publications/forms/publicity-contests/publicity-contest-notice.html

HabiloMédias, Protéger sa vie privée sur Internet. Les sites commerciaux, http://habilomedias.ca/fiche-conseil/proteger-sa-vie-privee-sur-internet-sites-commerciaux

COMMERCIAL WEBSITES

Amazon, App Distribution Agreement,

https://developer.amazon.com/appsandservices/support/legal/da

Amazon, FAQs Program Overview,

https://developer.amazon.com/public/support/faq#

Apple, App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/#terms-conditions

Apple, Apple Answers the FCC's Questions,

http://www.apple.com/hotnews/apple-answers-fcc-questions/

Google Play, Content ratings for apps and games,

https://support.google.com/googleplay/android-developer/answer/188189

Google Play, Google Play Developer Distribution Agreement,

https://play.google.com/about/developer-distribution-agreement.html

Google Play, Google Play Developer Program Policies,

https://play.google.com/about/developer-content-policy.html

ARTICLES AND BLOG POSTS

Advertising Age, Keep Your Online Sweepstakes and Contests on the Right Side of the Law, http://adage.com/article/guest-columnists/online-sweepstakes-legal/149206/

Avvo, Legal Compliance Guide for Online Contests and Sweepstakes, http://www.avvo.com/legal-guides/ugc/legal-compliance-guide-for-online-contests-and-sweepstakes-1

Bird & Bird, Simplification of French regulatory constraints on sweepstakes and commercial promotions,http://www.twobirds.com/en/news/articles/2015/france/loteries-publicitaires-et-operations-promotionnelles

Borden Ladner Gervais, Targeting the Canadian Consumer: An Important Primer on the Advertising and Marketing Laws in Canada,http://www.blg.com/en/NewsAndPublications/Documents/Targeting_the_Canadian_Consumer_-_Dec_2014.pdf

Communications Lawyer, Liability of Online Publishers for User Generated Content: A European Perspective,http://www.americanbar.org/content/dam/aba/publishing/communications_lawyer/pinto.authcheckdam.pdf

Digital Media Law Project, Terms of Use, http://www.dmlp.org/legal-guide/terms-use

EngageSciences, Understanding FTC COPPA Compliance: Social Marketing and Brands, http://www.engagesciences.com/coppa-compliance-smm-brands/

Guardian, Setting out good terms and conditions for your small business, http://www.theguardian.com/small-business-network/2013/feb/06/terms-and-conditions-small-business

Infosec Institute, Differences between the privacy laws in the EU and the US, http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/

Keller and Heckman LLP, Structuring Online Sweepstakes and Contests: New Challenges for Marketers, https://www.khlaw.com/3155

La formatrice, La loi C-28 au Canada, qu'est-ce c'est?, http://laformatrice.com/actualites/loi-c-28-au-canada-qu-est-ce-cest/

Mondaq, Australia: What You Need To Know About Australian Sweepstakes And Contest Regulations,http://www.mondaq.com/australia/x/260532/Antitrust+Competition/What+You+Need+To+Know+About+Australian+Sweepstakes+And+Contest+Regulations

Out-law, Moderation, liability and terms of use, http://www.out-law.com/page-7841#Unmoderatedsites

Practical Law: Data protection: Country Q&A tool, http://uk.practicallaw.com/2-502-1510?qaq=W_q1&qaq=W_q2&qaq=W_q3&qaq=W_q5&qaq=W_q9&qaq=W_q13&qaq=W_q17&qaq=W_q18&qaid=6-502-0556&qaid=6-502-1481

BIBLIOGRAPHY – USER-GENERATED CONTENT

WORKS

Caron, A. H., Cohen, R. I. (2013). *Regulating Screens: Issues in Broadcasting and Internet Governance for Children*. Montréal, McGill-Queen's University Press.

Caron, A. H. (2011). Les enfants devant leurs écrans; la réglementation canadienne de la télévision à l'internet, Presses de l'université de Montréal, 176 pages.

GOVERNMENT AND OFFICIAL ORGANIZATION WEBSITES

Advertising Standards Canada, Interpretation Guideline #2– Advertising to Children, http://www.normespub.com/en/Standards/interpretationGuideline2.aspx

Australian Copyright Council, http://www.copyright.org.au/acc_prod/ACC/Home/ACC/Home.aspx?hkey=24823bbe-5416-41b0-b9b1-0f5f6672fc31

Canadian Marketing Association, Code of Ethics and Regulatory Guidelines, http://www.the-cma.org/regulatory/code-and-guidelines

CEFRIO, Gérer les enjeux et les risques juridiques du Web 2.0, http://www.cefrio.qc.ca/media/uploader/guide_juridique_Web2.pdf

Europa, Handbook on European data protection law, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

EUX-LEX, Data protection in the electronic communications sector, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24120

Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Guide des droits sur Internet, Les sites de partage de contenu: Comment évaluer ces risques?, http://www.droitsurinternet.ca/section.php?section=261

Government of Canada – Office of the Privacy Commissioner of Canada, Guidelines for Online Consent,https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp

Government of France – Legifrance, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1),http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005789847&dateTexte=20080724

Government of Québec – Office de la protection du consommateur, Advertising Directed at Children Under 13 Years of

Age,http://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EN_Guide_publicite_moins_de_13_ans_vf.pdf

Government of Québec – Publications du Québec, An Act to Establish a Legal Framework for Information Technology,http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1_A.html

HabiloMédias, Propriété intellectuelle: L'utilisation équitable pour l'éducation aux médias, http://habilomedias.ca/litt%C3%A9ratie-num%C3%A9rique-et-%C3%A9ducation-aux-m%C3%A9dias/enjeux-des-m%C3%A9dias/propri%C3%A9t%C3%A9-intellectuelle/lutilisation-%C3%A9quitable-pour-l%C3%A9ducation-aux-m%C3%A9dias

HabiloMédias, Protéger sa vie privée sur Internet. Les sites commerciaux, http://habilomedias.ca/fiche-conseil/proteger-sa-vie-privee-sur-internet-sites-commerciaux

COMMERCIAL WEBSITES

Amazon, App Distribution Agreement, https://developer.amazon.com/appsandservices/support/legal/da

Amazon, FAQs Program Overview, https://developer.amazon.com/public/support/faq#

Apple, App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/#terms-conditions

Apple, Apple Answers the FCC's Questions, http://www.apple.com/hotnews/apple-answers-fcc-questions/

Google Play, Content ratings for apps and games, https://support.google.com/googleplay/android-developer/answer/188189

Google Play, Google Play Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html

Google Play, Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

ARTICLES AND BLOG POSTS

Blakes, Le contenu généré par les utilisateurs, un risque pour les exploitants de sites web,http://www.blakes.com/French/Resources/Bulletins/Pages/Details.aspx?BulletinID=255

Borden Ladner Gervais, Targeting the Canadian Consumer: An Important Primer on the Advertising and Marketing Laws in Canada,http://www.blg.com/en/NewsAndPublications/Documents/Targeting_the_Canadian_Consumer_-_Dec_2014.pdf

Clayton UTZ, Guide to Social Media: Risks and Opportunities for Business, http://www.claytonutz.com/docs/Social_Media_2013.pdf

Cognizant, How to De-Risk the Creation and Moderation of User-Generated Content, http://www.cognizant.com/InsightsWhitepapers/How-to-De-Risk-the-Creation-and-Moderation-of-User-Generated-Content.pdf

Communications Lawyer, Liability of Online Publishers for User Generated Content: A European Perspective,http://www.americanbar.org/content/dam/aba/publishing/communications_lawyer/pinto.authcheckdam.pdf

Davis and Gilbert LPP, FTC Issues Updated FAQs on Amended COPPA Rule,http://www.dglaw.com/images_user/newsalerts/Advertising_FTC_Issues_Updated_FAQs_Amended_COPPA.pdf

E-Moderation, Children being Exposed to Explicit Content in Virtual Worlds, http://www.emoderation.com/children-being-exposed-to-explicit-content-in-virtual-worlds/

E-Moderation, Six Types of Content Moderation you Need to Know About, http://www.emoderation.com/6-types-of-content-moderation-you-need-to-know-about/

EngageSciences, Understanding FTC COPPA Compliance: Social Marketing and Brands, http://www.engagesciences.com/coppa-compliance-smm-brands/

Internet and E-Commerce Law in Canada, User-Generated Content: Recent Developments in Canada and the U.S.,http://www.casselsbrock.com/files/file/docs/UGC%20Paper%20in%20IECLIC%20-%20October%202011%20Glickman%20and%20Fingerhut.pdf

Mondaq, Canada: Risks of User-Generated Content to Website Operators,http://www.mondaq.com/canada/x/117052/Copyright/Risks+of+UserGenerated+Content+to+Website+Operators

Out-law, Moderation, liability and terms of use, http://www.out-law.com/page-7841#Unmoderatedsites

Practical Law: Data protection: Country Q&A tool, http://uk.practicallaw.com/2-502-1510?qaq=W_q1&qaq=W_q2&qaq=W_q3&qaq=W_q5&qaq=W_q9&qaq=W_q13&qaq=W_q17&qaq=W_q18&qaid=6-502-0556&qaid=6-502-1481

BIBLIOGRAPHY – ADVERTISING

WORKS

Caron, A. H., Cohen, R. I. (2013). *Regulating Screens: Issues in Broadcasting and Internet Governance for Children*. Montréal, McGill-Queen's University Press.

Caron, A. H. (2011). Les enfants devant leurs écrans; la réglementation canadienne de la télévision à l'internet, Presses de l'université de Montréal, 176 pages.

GOVERNMENT AND OFFICIAL ORGANIZATION WEBSITES

Advertising Self-Regulatory Council, http://www.asrcreviews.org/

Advertising Standards Canada, Broadcast Code for Advertising to Children,http://www.adstandards.com/en/clearance/childrens/broadcastCodeForAdvertisingToChildren-TheCode.aspx

Advertising Standards Canada, Canadian Children's Food and Beverage Advertising Initiative, http://www.adstandards.com/en/childrensinitiative-old/default.htm

Advertising Standards Canada, Interpretation Guideline #2– Advertising to Children, http://www.normespub.com/en/Standards/interpretationGuideline2.aspx

Advertising Standards Canada (ASC), Association of Canadian Advertisers (ACA), The Canadian Association of Broadcasters (CAB), Concerned Children's Advertisers (CCA), and Institute of Communication and Advertising (ICA), Advertising to Children in Canada A Reference Guide,

www.cab-acr.ca/english/.../advertisingchildren/kids_reference_guide.pdf

Australian Government – Australian Consumer Law, A guide to provisions,http://www.consumerlaw.gov.au/content/the_acl/downloads/A_guide_to_provisions_Nov_2010.pdf

Australian Government – Office of the Australian Information Commissioner, If a business obtains information about its customers in the course of providing them with goods and services, can it use that information for marketing purposes?, http://www.oaic.gov.au/privacy/privacy-topics/business-and-small-business/if-a-business-obtains-information-about-its-customers-in-the-course-of-providing-them-with-goods-and-services-can-it-use-that-information-for-marketi

Australian Government – Office of the Australian Information Commissioner, Privacy fact sheet 17: Australian Privacy Principles,http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

Autorité de régulation professionnelle de la publicité, Enfant, http://www.arpp-pub.org/IMG/pdf/Reco_Enfant.pdf

Canadian Marketing Association, Code of Ethics and Regulatory Guidelines, http://www.the-cma.org/regulatory/code-and-guidelines

CEFRIO, Gérer les enjeux et les risques juridiques du Web 2.0, http://www.cefrio.qc.ca/media/uploader/guide_juridique_Web2.pdf

Children's Advertising Review Unit, Self-Regulatory Program for Children's Advertising: Guidelines, http://www.caru.org/guidelines/guidelines.pdf

Council of Better Business Bureaus, Children's Food and Beverage Advertising Initiative, http://www.bbb.org/council/the-national-partner-program/national-advertising-review-services/childrens-food-and-beverage-advertising-initiative/

Digital Advertising Alliance of Canada, The Canadian Self-Regulatory Principles for Online Behavioural Advertising, http://youradchoices.ca/wp-content/uploads/2013/08/The-Canadian-Self-Regulatory-Principles-for-Online-Behavioural-Advertising.pdf

Europa, Handbook on European data protection law, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

European Parliament, Fact Sheets on the European Union: Audiovisual and media policy, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.13.2.html

EUX-LEX, Data protection in the electronic communications sector, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24120

Federal Trade Commission, Advertising and Marketing on the Internet: Rules of the Road, https://www.ftc.gov/tips-advice/business-center/guidance/advertising-marketing-internet-rules-road#general

Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Federal Trade Commission, Marketing your Mobile App: Get it Right from the Start, https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf

Government of Canada – Competition Bureau, Application of the Competition Act to Representations on the Internet,http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03134.html

Government of Canada – Competition Bureau, False or Misleading Representations and Deceptive Marketing Practices Under the Competition Act,http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03133.html

Government of Canada – Consumer Information, Provincial and Territorial Legislation, http://www.consumerinformation.ca/eic/site/032.nsf/eng/01173.html

Government of Canada – Office of the Privacy Commissioner of Canada, Every Move You Make… Advertisers are tracking your online behaviour,https://www.priv.gc.ca/resource/fs-fi/02_05_d_52_ba_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Guidelines for Online Consent,https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Policy Position on Online Behavioural Advertising,https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp

Government of France – Conseil supérieur de l'audiovisuel, La protection des mineurs sur Internet, http://www.csa.fr/Television/Le-suivi-des-programmes/Jeunesse-et-protection-des-mineurs/La-protection-des-mineurs-sur-internet

Government of France – Le portail de l'Économie et des Finances, Les pratiques commerciales trompeuses,http://www.economie.gouv.fr/dgccrf/Publication/Vie-pratique/Fiches-pratiques/Pratiques-commerciales-trompeuses

Government of Québec – Portail entreprises, Concurrence et pratiques interdites, http://www2.gouv.qc.ca/entreprises/portail/quebec/gerer?g=gerer&t=o&e=1427036613

Government of Québec, Office de la protection du consommateur: Advertising Directed at Children Under 13 Years of Age,http://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EN_Guide_publicite_moins_de_13_ans_vf.pdf

International Chamber of Commerce, Marketing and Advertising: Self-regulation, http://www.iccwbo.org/Advocacy-Codes-and-Rules/Areas-of-work/Marketing-and-Advertising/Self-regulation/

Option Consommateurs, La publicité destinée aux enfants: Identifier la meilleure protection possible, http://www.option-consommateurs.org/documents/principal/fr/File/rapports/pratiques_commerciales/oc_ic_publicite_enfant_200804.pdf

COMMERCIAL WEBSITES

Amazon, App Distribution Agreement, https://developer.amazon.com/appsandservices/support/legal/da

Amazon, FAQs Program Overview, https://developer.amazon.com/public/support/faq#

Apple, App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/#terms-conditions

Apple, Apple Answers the FCC's Questions, http://www.apple.com/hotnews/apple-answers-fcc-questions/

Google Play, Content ratings for apps and games, https://support.google.com/googleplay/android-developer/answer/188189

Google Play, Google Play Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html

Google Play, Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

ARTICLES AND BLOG POSTS

Advertising Age, Better Business Bureaus Revise Ad Code for the First Time Since 1970s, http://adage.com/article/cmo-strategy/business-bureaus-ad-code-revised/297113/

Borden Ladner Gervais, Targeting the Canadian Consumer: An Important Primer on the Advertising and Marketing Laws in Canada,http://www.blg.com/en/NewsAndPublications/Documents/Targeting_the_Canadian_Consumer_-_Dec_2014.pdf

EngageSciences, Understanding FTC COPPA Compliance: Social Marketing and Brands, http://www.engagesciences.com/coppa-compliance-smm-brands/

Davis and Gilbert LPP, FTC Issues Updated FAQs on Amended COPPA Rule,http://www.dglaw.com/images_user/newsalerts/Advertising_FTC_Issues_Updated_FAQs_Amended_COPPA.pdf

Kidsscreen: Who's watching the kids?, http://kidscreen.com/2015/01/21/whos-watching-the-kids/

Practical Law: Data protection: Country Q&A tool, http://uk.practicallaw.com/2-502-1510?qaq=W_q1&qaq=W_q2&qaq=W_q3&qaq=W_q5&qaq=W_q9&qaq=W_q13&qaq=W_q17&qaq=W_q18&qaid=6-502-0556&qaid=6-502-1481

Robert Wood Johnson Foundation, Recommendations for Responsible Food Marketing to Children, http://www.foodpolitics.com/wp-content/uploads/report.pdf

The Brand Protection Blog, Advertising, Websites, and Children's Privacy, http://www.thebrandprotectionblog.com/advertising-websites-and-childrens-privacy/

BIBLIOGRAPHY – SALES AND MONETIZATION

WORKS

Caron, A. H., Cohen, R. I. (2013). *Regulating Screens: Issues in Broadcasting and Internet Governance for Children*. Montréal, McGill-Queen's University Press.

Caron, A. H. (2011). Les enfants devant leurs écrans; la réglementation canadienne de la télévision à l'internet, Presses de l'université de Montréal, 176 pages.

GOVERNMENT AND OFFICIAL ORGANIZATION WEBSITES

Advertising Standards Canada, Interpretation Guideline #2– Advertising to Children, http://www.normespub.com/en/Standards/interpretationGuideline2.aspx

Australian Communications Consumer Action Network, App purchases by Australian consumers,http://accan.org.au/files/App_purchases_by_Australian_consumers.pdf

Australian Government – Australian Competition & Consumer Commission, http://www.accc.gov.au/

Australian Government – Australian Consumer Law, A guide to provisions,http://www.consumerlaw.gov.au/content/the_acl/downloads/A_guide_to_provisions_Nov_2010.pdf

Australian Government – Office of the Australian Information Commissioner, If a business obtains information about its customers in the course of providing them with goods and services, can it use that information for marketing purposes?, http://www.oaic.gov.au/privacy/privacy-topics/business-and-small-business/if-a-business-obtains-information-about-its-customers-in-the-course-of-providing-them-with-goods-and-services-can-it-use-that-information-for-marketi

Australian Government – The Treasury, E-commerce Legislation, http://www.treasury.gov.au/Policy-Topics/Business/Small-Business/Legal-Topics/Multimedia-Aspects/ecommerce/Legislation

Canadian Consumer Handbook, Online Shopping, http://www.consumerhandbook.ca/en/topics/consumer-protection/online-shopping

Canadian Marketing Association, Code of Ethics and Regulatory Guidelines, http://www.the-cma.org/regulatory/code-and-guidelines

CEFRIO, Gérer les enjeux et les risques juridiques du Web 2.0, http://www.cefrio.qc.ca/media/uploader/guide_juridique_Web2.pdf

CMF Trends: The Freemium Model: Faster, Higher, Stronger, http://trends.cmf-fmc.ca/blog/the-freemium-model-faster-higher-stronger/

Europa, Common position of national authorities within the CPC: Online « free » games,http://ec.europa.eu/consumers/enforcement/docs/common_position_on_online_games_en.pdf

Europa, Handbook on European data protection law, http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

Europa, In-app purchases: Joint action by the European Commission and Member States is leading to better protection for consumers in online games,http://europa.eu/rapid/press-release_IP-14-847_en.htm

Europa, The Directive on Consumer Rights, http://ec.europa.eu/consumers/consumer_rights/rights-contracts/directive/index_en.htm

European Parliament, Fact Sheets on the European Union: Consumer protection measures, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.5.2.html

European Parliament, Fact Sheets on the European Union: Audiovisual and media policy, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.13.2.html

EUX-LEX, Data protection in the electronic communications sector, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l24120

EUR-LEX, Directive 2011/83/UE on consumer rights, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0083

Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Federal Trade Commission – Consumer Information, Kids' in-app spending on Android? Parents didn't app-rove, https://www.consumer.ftc.gov/blog/kids-app-spending-android-parents-didnt-app-rove

Federal Trade Commission, Marketing your Mobile App: Get it Right from the Start, https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf

Federal Trade Commission, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing,https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf

Future of Privacy, Best Practices for Mobile Applications Developers, http://www.futureofprivacy.org/wp-content/uploads/Apps-Best-Practices-v-beta.pdf

Government of Alberta, Consumer tips: Internet Shopping, http://www.servicealberta.gov.ab.ca/pdf/tipsheets/Internet_shopping.pdf

Government of Canada – Competition Bureau, Application of the Competition Act to Representations on the Internet,http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03134.html

Government of Canada – Competition Bureau, False or Misleading Representations and Deceptive Marketing Practices Under the Competition Act,http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03133.html

Government of Canada – Consumer Information, Provincial and Territorial Legislation, http://www.consumerinformation.ca/eic/site/032.nsf/eng/01173.html

Government of Canada – Financial Consumer Agency of Canada, Mobile Payments and Consumer Protection in Canada, http://www.fcac-acfc.gc.ca/Eng/resources/researchSurveys/Documents/FCAC_Mobile_Payments_Consumer_Protection_accessible_EN.pdf

Government of Canada – Industry Canada, Office of Consumer Affairs, Canadian Code of Practice for Consumer Protection in Electronic Commerce,http://www.ic.gc.ca/eic/site/cmc-cmc.nsf/vwapj/EcommPrinciples2003_e.pdf/$FILE/EcommPrinciples2003_e.pdf

Government of Canada – Industry Canada, Office of Consumer Affairs, Mobile Commerce — New Experiences, Emerging Consumer Issues,https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02518.html

Government of Canada – Office of the Privacy Commissioner of Canada, Guidelines for Online Consent,https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, Privacy Toolkit: A Guide for Businesses and Organizations,https://www.priv.gc.ca/information/pub/guide_org_e.asp

Government of Canada – Office of the Privacy Commissioner of Canada, The Transformation of the Canadian Payments System: Why Privacy is Essential for Trust and Innovation in the Payments System, https://www.priv.gc.ca/information/research-recherche/sub/sub_psr_1109_e.asp

Government of France – Le portail de l'Économie et des Finances, Les pratiques commerciales trompeuses,http://www.economie.gouv.fr/dgccrf/Publication/Vie-pratique/Fiches-pratiques/Pratiques-commerciales-trompeuses

Government of Ontario, E-commerce: Purchasing and Selling Online, https://dr6j45jk9xcmk.cloudfront.net/documents/435/medi-booklet-e-commerce-accessible-e-final.pdf

Government of Ontario, Integrating mobile with your marketing strategy, https://dr6j45jk9xcmk.cloudfront.net/documents/437/medi-booklet-integrating-mobile-accessible-e-final.pdf

Government of Québec – Portail entreprises, Concurrence et pratiques interdites, http://www2.gouv.qc.ca/entreprises/portail/quebec/gerer?g=gerer&t=o&e=1427036613

Government of Québec, Office de la protection du consommateur: Advertising Directed at Children Under 13 Years of Age,http://www.opc.gouv.qc.ca/fileadmin/media/documents/consommateur/sujet/publicite-pratique-illegale/EN_Guide_publicite_moins_de_13_ans_vf.pdf

HabiloMédias, Fiche-conseils sur la cybersécurité destinée aux consommateurs: Pratiques sûres en matière de commerce électronique,http://habilomedias.ca/sites/mediasmarts/files/pdfs/tipsheet/Fiche-conseilsCybersecuriteConsommateurs-ecommerce.pdf

HabiloMédias, Publicité et consommation: Les enjeux pour les jeunes enfants, http://habilomedias.ca/publicite-consommation/enjeux-jeunes-enfants

Organisation for Economic Co-operation and Development, Guidelines for Consumer Protection in the Context of Electronic Commerce,http://www.oecd.org/sti/consumer/34023811.pdf

U.K. Government – Office of Fair Trading, The OFT's Principles for Online and app-based games,https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf

COMMERCIAL WEBSITES

Amazon, App Distribution Agreement, https://developer.amazon.com/appsandservices/support/legal/da

Amazon, FAQs Program Overview, https://developer.amazon.com/public/support/faq#

Apple, App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/#terms-conditions

Apple, Apple Answers the FCC's Questions, http://www.apple.com/hotnews/apple-answers-fcc-questions/

Bank of Canada, Succeed with e-commerce, https://www.bdc.ca/EN/articles-tools/entrepreneur-toolkit/ebooks/Pages/e-commerce-guide.aspx

Google Play, Content ratings for apps and games, https://support.google.com/googleplay/android-developer/answer/188189

Google Play, Google Play Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html

Google Play, Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

ARTICLES AND BLOG POSTS

Borden Ladner Gervais, Targeting the Canadian Consumer: An Important Primer on the Advertising and Marketing Laws in

Canada,http://www.blg.com/en/NewsAndPublications/Documents/Targeting_the_Canadian_Consumer_-_Dec_2014.pdf

Creditcards.ca, When your child uses your credit card without permission, http://www.creditcards.ca/credit-card-news/child-uses-credit_card-without_permission-1267.php

Davis and Gilbert LPP, FTC Issues Updated FAQs on Amended COPPA Rule,http://www.dglaw.com/images_user/newsalerts/Advertising_FTC_Issues_Updated_FAQs_Amended_COPPA.pdf

Ecommerce Guide, Ecommerce Solutions: 5 Ways to Sell Digital Goods Online, http://www.ecommerce-guide.com/article.php/3794706/Ecommerce-Solutions-5-Ways-to-Sell-Digital-Goods-Online.htm

Ecommerce Platforms, How to Choose the Best Payment Gateway for Your Ecommerce Store, http://ecommerce-platforms.com/ecommerce-selling-advice/choose-payment-gateway-ecommerce-store

EngageSciences, Understanding FTC COPPA Compliance: Social Marketing and Brands, http://www.engagesciences.com/coppa-compliance-smm-brands/

Gamasutra, Monetizing Children, http://www.gamasutra.com/blogs/RaminShokrizade/20130620/194429/Monetizing_Children.php

Gamasutra, The Design of Free-To-Play Games, http://www.gamasutra.com/view/feature/6552/the_design_of_freetoplay_games_.php?print=1

Gamasutra, The Top F2P Monetization Tricks, http://www.gamasutra.com/blogs/RaminShokrizade/20130626/194933/

Guardian, It's time more parents started paying for children's apps, http://www.theguardian.com/technology/2014/jul/11/parents-children-apps-amazon-ftc

iKids, If You Have No Scruples, Your Game Can Male $600,000 a Day, http://kidscreen.com/2013/07/15/if-you-have-no-scruples-your-game-can-make-600000-a-day/

KidsScreen, Parents vs. In-App Purchases, http://kidscreen.com/2012/04/09/parents-vs-in-app-purchases/

Millennial Media, Best Practices For Monetizing Mobile Applications, https://support.mmedia.com/hc/en-us/articles/204610474-Best-Practices-for-Monetizing-Mobile-Applications

Practical Law: Data protection: Country Q&A tool, http://uk.practicallaw.com/2-502-1510?qaq=W_q1&qaq=W_q2&qaq=W_q3&qaq=W_q5&qaq=W_q9&qaq=W_q13&qaq=W_q17&qaq=W_q18&qaid=6-502-0556&qaid=6-502-1481

TaylorWessing, Key Legal Issues for Games Businesses in Europe, http://www.taylorwessing.com/fileadmin/files/docs/TWPlay_Key-legal-issues-for-games-businesses.pdf

BIBLIOGRAPHY – SOCIAL MEDIA, ONLINE COMMUNITIES AND SECURITY

WORKS

Caron, A. H., Cohen, R. I. (2013). *Regulating Screens: Issues in Broadcasting and Internet Governance for Children*. Montréal, McGill-Queen's University Press.

Caron, A. H. (2011). Les enfants devant leurs écrans; la réglementation canadienne de la télévision à l'internet, Presses de l'université de Montréal, 176 pages.

GOVERNMENT AND OFFICIAL ORGANIZATION WEBSITES

Australian Government, Responding to online child sexual grooming: an industry perspective, http://www.aic.gov.au/publications/current%20series/tandi/361-380/tandi379.html

Beyond Borders, Corporate Responsibility, http://www.beyondborders.org/wp/corporate-responsibility/

CEFRIO, Gérer les enjeux et les risques juridiques du Web 2.0, http://www.cefrio.qc.ca/media/uploader/guide_juridique_Web2.pdf

Common Sense Media, What age should my kids be before I let them use Instagram, Facebook, and other social media services?,https://www.commonsensemedia.org/social-media/what-age-should-my-kids-be-before-i-let-them-use-instagram-facebook-and-other-social#

Federal Trade Commission, Complying with COPPA: Frequently Asked Questions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Federal Trade Commission, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing,https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf

Government of Canada – Get Cyber Safe, What are the potential legal consequences of cyberbullying?, http://www.getcybersafe.gc.ca/cnt/cbrbllng/prnts/lgl-cnsqncs-en.aspx

Government of Canada – Royal Canadian Mounted Police, How to Report Child Sexual Exploitation Offences or Luring Related to Children, http://www.rcmp-grc.gc.ca/ncecc-cncee/report-denoncer-eng.htm

HabiloMédias, Cyberintimidation et fiche d'information sur la loi, http://habilomedias.ca/document-accompagnement/cyberintimidation-fiche-information-loi

HabiloMédia, Exploitation sexuelle, http://habilomedias.ca/exploitation-sexuelle/apercu

inHope, http://www.inhope.org/gns/home.aspx

SafeNetwork, Developing online safety policies and procedures for your organisation,http://www.safenetwork.org.uk/help_and_advice/Pages/online_policies.aspx

U.K. Government, Online Abuse and Bullying Prevention Guide for professionals working with young people,https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414118/NSPCC_online_abuse_and_bullying_prevention_guide_3.pdf

COMMERCIAL WEBSITES

Amazon, App Distribution Agreement, https://developer.amazon.com/appsandservices/support/legal/da

Amazon, FAQs Program Overview, https://developer.amazon.com/public/support/faq#

Apple, App Store Review Guidelines, https://developer.apple.com/app-store/review/guidelines/#terms-conditions

Apple, Apple Answers the FCC's Questions, http://www.apple.com/hotnews/apple-answers-fcc-questions/

Google Play, Content ratings for apps and games, https://support.google.com/googleplay/android-developer/answer/188189

Google Play, Google Play Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html

Google Play, Google Play Developer Program Policies, https://play.google.com/about/developer-content-policy.html

ARTICLES AND BLOG POSTS

BBC, Cyberbullies: How best to tackle online abuse?, http://www.bbc.co.uk/news/technology-26121199

Borden Ladner Gervais, Targeting the Canadian Consumer: An Important Primer on the Advertising and Marketing Laws in Canada,http://www.blg.com/en/NewsAndPublications/Documents/Targeting_the_Canadian_Consumer_-_Dec_2014.pdf

COPPA Attorney, The COPPA Social Media Button Plug-in Conundrum, http://www.coppalawattorney.com/coppa-social-media-button-plug-in/#ixzz3XDkFDwvv

EngageSciences, Understanding FTC COPPA Compliance: Social Marketing and Brands, http://www.engagesciences.com/coppa-compliance-smm-brands/

Law360, No Cookie for You: How COPPA Will Affect Your Company, http://www.alston.com/files/docs/How-COPPA-Will-Affect-Your-Company.pdf

Practical Law: Data protection: Country Q&A tool, http://uk.practicallaw.com/2-502-1510?qaq=W_q1&qaq=W_q2&qaq=W_q3&qaq=W_q5&qaq=W_q9&qaq=W_q13&qaq=W_q17&qaq=W_q18&qaid=6-502-0556&qaid=6-502-1481

Remake Learning, Want to stop cyberbullying? Start With Social Media Design, http://remakelearning.org/blog/2014/04/08/want-to-stop-cyberbullying-start-with-social-media-design/