CHILDLIGHT

Global Child Safety Institute

Authors:

Ms Jessica Schidlow
Legal Director, Child USA

Dr Konstantinos Kosmas Gaitis
Research Fellow (Policy & Legal Research), Childlight – Global Child Safety Institute, University of Edinburgh

Dr Mengyao Lu
Research Fellow, Childlight – Global Child Safety Institute, University of Edinburgh

Mr James Stevenson
Technology-Facilitated CSEA Data Specialist, Childlight – Global Child Safety Institute, University of Edinburgh

Professor Deborah Fry
Personal Chair of International Child Protection Research, Childlight – Global Child Safety Institute, University of Edinburgh

Legal challenges in tackling AI-generated child sexual abuse material across the 5 Eyes nations: Who is accountable according to the law?

CANADA

Table of Contents

Abbreviations

AI – Artificial Intelligence

AIDA – Artificial Intelligence and Data Act

C.C.Q. – Civil Code of Québec

CCSM – Continuing Consolidation of the Statutes of Manitoba

CIPO – Canadian Intellectual Property Office

CQLR – Code Québécois Législatif et Réglementaire (Québec Official Compilation of Laws and Regulations)

CSAM – Child Sexual Abuse Material

EU – European Union

ICMEC – International Centre for Missing & Exploited Children

IIMS – Intentional Infliction of Mental Suffering

OECD – Organisation for Economic Co-operation and Development

OPC – Office of the Privacy Commissioner of Canada

PIPEDA – Personal Information Protection and Electronic Documents Act

QC – Quebec

R.S.C. – Revised Statutes of Canada

RSBC – Revised Statutes of British Columbia

RSNL – Revised Statutes of Newfoundland and Labrador

RSS – Revised Statutes of Saskatchewan

S.C.C. – Supreme Court of Canada

Executive Summary

This study is among the first to critically review the regulatory context of the Five Eyes nations (UK, USA, Canada, Australia and New Zealand) on the topic of accountability around child sexual abuse material (CSAM) created via generative Artificial Intelligence (gen-AI). We examined this topic on a national, state and territory level in Australia; on a national level in New Zealand; on a federal and state level in the United States (US); on a federal and provincial level in Canada; and lastly on a reserved and devolved level in Britain. We have identified key strengths, as well as weaknesses of the studied legislative contexts, which we selected due to their democratic political systems, their technologically advanced character, and progressive legislative systems.

In Canada, there is a distinction between federal law and province-based law. The federal Criminal Code lacks specific prohibitions against AI-generated CSAM. Nonetheless, the relevant sections of the Canadian Criminal Code have been interpreted widely by the Supreme Court of Canada to provide coverage for several types of harmful material. However, two exceptions, remain: One for material created only for personal use, and another for works of art that lack intent to exploit children. Canadian federal law criminalises the non-consensual distribution of intimate images. However, whether these provisions apply to AI-generated CSAM is uncertain. Enforcement is the responsibility of provincial agencies, and civil remedies for victims vary widely across provinces, creating a patchwork of protections in which access to relief depends on the victim's location.

Privacy laws in Canada offer some avenues for assistance, but they lack a more tailored character to address the specific harms associated with AI-generated CSAM. Copyright law offers a potential, although complex, avenue for addressing AI-generated CSAM.

Lastly, in Canada, a significant proposed law reform was the Online Harms Act. If passed, this Act would have created a new regulatory framework requiring online platforms to act responsibly to prevent and mitigate the risk of harm to children on their platforms. Under the Act, online platforms would have a duty to implement age-appropriate design features and to make content that sexually victimises a child or re-victimises a survivor inaccessible, including via the use of technology, to prevent CSAM from being uploaded in the first instance. A new Digital Safety Commission would oversee compliance and be charged with the authority to penalise online platforms that fail to act responsibly. Accordingly, the Act would create a legally binding framework for safe and responsible AI development and deployment that could potentially apply to restrict or penalise content that would otherwise be legal, but that poses a substantial risk of sexual exploitation or revictimisation of a child. Prorogation of the Parliament of Canada ended the parliamentary session relevant to this Bill. As a result, all proceedings before Parliament ended, and bills that did not receive Royal Assent have been "entirely terminated" (Lexology, 2025).

Based on these findings, the following recommendations are made for Canada:

Recommendation 1. Amend existing CSAM laws to explicitly cover AI-generated content, even when it includes fictitious children.

Recommendation 2. Amend CSAM laws to regulate the misuse of AI.

Recommendation 3. Establish a legally binding framework for safe and responsible AI development and deployment.

Recommendation 4. Expand legal protections to include control over one's own image.

Introduction

Child sexual exploitation and abuse (CSEA) is considered a violation of children's rights and dignity (Ngo, 2021). A "widespread, worldwide issue of concerning magnitude" that affects both girls and boys (Simon, Luetzow & Conte, 2020: 2). CSEA may entail a series of negative effects for victims, which can impact their physical, mental or psychological health, their emotional wellbeing, social skills and interpersonal relationships, economic status, as well as vulnerability to future victimisation (Fisher et al., 2017). Within this, technology and related platforms or online environments are considered spaces which can be protective, but also pose significant risks to children's safety, increasing their vulnerability to CSEA victimisation (Simon, Luetzow & Conte, 2020). This vulnerability to victimisation is considered to be higher for children than adults (Quayle, 2016).

The rapid development of technology has led to the birth of new, immersive forms of technology, which are usually grouped under the umbrella term "eXtended Reality" (XR) (Huang, 2022). Prominent among these emerging technologies is Artificial Intelligence (AI), defined widely by Bahoo, Cucculelli and Qamar (2023: 1) as "the system's ability to interpret data and leverages computers and machines to enhance humans' decision-making, problem-solving capabilities, and technology-driven innovativeness". As such and following the increasing dissemination of child sexual abuse material (CSAM) noticed across the clear and dark web, AI can prove to be a valuable tool in the efforts against CSEA by allowing the invention of detection intelligence algorithms that will use deep-learning techniques as a method of accurate detection of CSAM online (Lee et al., 2020; Ngo, McKeever & Thorpe, 2023). However, AI can also be misused by offenders to create CSAM with varying levels of realism that can often be hardly distinguishable from real-life material (Internet Watch Foundation, 2023). Irrespective of whether AI-created CSAM involves artificial children or children

modelled after real-life children, there is widespread concern that it can be a pathway to higher levels of CSEA offending that may include the sexual exploitation and abuse of children in real life (Internet Watch Foundation, 2023). As such, it requires a robust and clear legislative response, particularly with regards to accountability over AI-created CSAM. This call comes amidst a hotly contested debate, with some stakeholders promoting notions that CSAM created via generative AI does not hurt real children or that it may also serve to divert potential offenders from sexually exploiting and abusing real children, while others fear that generative AI-created CSAM may be the first step on a pathway towards higher offending in CSEA with real children (Internet Watch Foundation, 2023).

Based on the above, examining the existing legislative context of the Five Eyes countries, which comprise Australia, Canada, New Zealand, the United Kingdom (UK) and the United States of America (USA), becomes crucial in order to assess the readiness of their regulatory frameworks against the phenomena of AI-created CSAM and AI-facilitated child sexual exploitation and abuse. These countries have a long history of association dating back to 1956 (Weaver & Roseth, 2024). A recent study provided a review of the legal challenges that AI-generated CSAM presents in the context of Europe. Similar to the present study, this research looked at legal frameworks concerning both the creation and generation, as well as the distribution of that child sexual abuse material (Parti & Szabo, 2024). The five countries have been selected due to their democratic and open political systems, their high levels of technological advancement and literacy, as well as their progressive and advanced legislative systems, which often serve as the regulatory blueprints for other countries across the globe to model their legislation after. It also assists in forecasting the potential technological developments that have yet to be created or alternatively used in the sexual harm of children. By identifying and helping to shore up any gaps in

legislation now, it will be much easier in the future to address technology-facilitated CSEA (TF-CSEA) through the use of AI. It is especially timely as four of the five included countries are in the process of ratifying or drafting legislation to address online environment safety. The United Kingdom and Australia are in the process of implementing the respective Online Safety Acts, with Canada and the United States currently working on multiple pieces of legislation to address safety online (Ness et al., 2023). The capacity of AI-driven CSAM and child sexual abuse and exploitation will only increase with time as technology continues to develop (Parti & Szabo, 2024). It is important that legislation in countries known for combatting TF-CSEA is prepared for this. As such, it is necessary for this study to review the full breadth of legal coverage for crimes committed against children using any type of AI.

Methodology

Given that XR environments, and primarily AI, constitute a new and evolving field of technology, we anticipate gaps in legislation across the Five Eyes nations on the matter of accountability over AI-generated CSAM. To examine our research hypothesis, we conducted a legislative review of relevant laws and case law across the Five Eyes countries (USA, UK, Canada, Australia, New Zealand).

The review and analysis of the emerging pieces of legislation and caselaw was informed by the "black-letter law" approach (McConville & Chui, 2007), also known as doctrinal legal research method. Using this method, we gathered legal rules found in primary sources, such as statutes, case law, regulations, and proposed bills, and identified underlying themes or systems of application related to each source to develop a descriptive and detailed analysis of the effectiveness of existing laws, identify ambiguities and gaps, and suggest necessary legal reforms. This approach focuses on the letter of the law rather than on the spirit of the law and is therefore taking a "literal approach to reading the law", as Wright (2018: 30) points out. By critically analysing primary and secondary legal sources, the aim of this approach is to restrict the number of possible outcomes, thus succinctly summarising and clarifying what the law instructs in a more systematised and narrower way than socio-legal analyses, which tend to look at the broader societal, political and policy context of legislation (Wright, 2018). The identification of themes in our legislative analysis is guided by our research hypothesis and research questions.

More specifically, we reviewed laws and case law from the Five Eyes countries on the topic of accountability with regards to generative-AI CSEA/CSAM. Legislation and case law was eligible for inclusion, if they focus on any area that intersects with accountability for CSEA/CSAM and particularly with regards to generative AI software; or if they defined concepts that are applicable and useful for

phenomena of AI-generated CSAM (e.g. case law defining the concept of obscenity). There was no defined search period, as any legislation or caselaw that can be applicable on the study topic will be included. All legislative and caselaw sources were in English given that all countries studied are Anglophone nations.

To identify relevant legislations and cases across the five countries, we conducted an initial search of legal websites, such as Lexis Nexis, Practical Law, Google Scholar and Google; utilised official Government sources; and searched on local court and prosecution services' websites.

Regarding Canada, platforms such as Justice Laws Website and CanLII Database were additionally used to retrieve legal sources.

To identify potential law reforms as well as updates on the most recent cases, we conducted internet searches, consulted media sources and obtained discussion papers or reports from the relevant government agency websites. Supplementary materials, including press releases, news articles and policy reports, were identified through standard search engine queries and databases such as the Koons Family Institute/International Centre for Missing & Exploited Children (ICMEC) database and the Organisation for Economic Co-operation and Development (OECD) database.

Lastly, consulting our extensive network of experienced colleagues located in Canada crucially assisted us in locating further legislations or caselaw on the matter that we were not able to obtain via the above methods.

All identified legislations were collated and organised via Excel spreadsheets and then analysed. Traditional methods of selection process did not apply here, given that both the existence and non-existence of relevant legislative provisions or caselaw on the studied topic have equal research value and led to important

conclusions regarding the strengths and weaknesses of said legislation and regulatory frameworks of the 5 studied nations.

Data was extracted using a data extraction tool developed by the research team (https://osf.io/as83r/files/osfstorage/67851f0aaeb11fe8762f3f18). The data extracted included specific details about legislative definitions, provisions regarding accountability and other key findings relevant to the review questions. More specifically, the data extraction tool contained themes such as:

- Definitions: How reserved, devolved, federal, state, and provincial laws define terms such as “pseudo-photographs”, “indecent material”, "child pornography"[1], "obscene material," and related offenses, with a particular focus on computer-generated content.
- Accountability Provisions: Mechanisms by which individuals, platforms, and third parties are held accountable for producing, hosting, or distributing AI-generated CSAM.
- Civil Remedies: Available remedies for victims seeking compensation, particularly where AI CSAM is involved.
- Legislative Gaps: Identification of areas where legislation lacks clarity, such as the legal status of using real CSAM in AI training datasets.

This structured approach ensured a comprehensive review of current legal frameworks while highlighting areas for potential reform to meet the challenges posed by advancements in AI technology. We examined:

- 10 Canadian federal laws
- 2 pending cases of Canadian federal legislation
- 8 Canadian federal cases
- 8 Canadian provincial image-based abuse laws (civil)

[1] Childlight follows the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. The terms ‘child abuse’, ‘child prostitution’, ‘child pornography’ and ‘rape’ are used in legal contexts.

- 3 Canadian provincial privacy laws (civil)
- 7 Canadian provincial tort laws
- 10 Canadian provincial tort law cases

Legislative Review: Canada

The Canadian Criminal Code provides robust federal protections against all forms of child exploitation, including AI-generated CSAM. As in the United States, Canada prohibits both CSAM and obscenity as non-protected speech, criminalising the production, distribution, and possession of such content the primary legal mechanisms for combating AI-generated CSAM. The Criminal Code also includes protections against the non-consensual distribution of intimate images, which may be invoked to combat morphed images and other malicious uses of AI. Federal privacy and copyright laws may also provide some protection to victims. While the federal government has exclusive jurisdiction in criminal law, the provinces control much of civil law and have enacted laws to provide victims with meaningful redress for privacy and other related violations.

The Federal Legal Framework

i. Canadian Criminal Code Offenses

1. Child Pornography

In Canada, the regulation of CSAM is primarily governed at the federal level under the Canadian Criminal Code, which applies uniformly across all provinces and territories. Although the Code does not explicitly address AI-generated content, Section 163.1 of the Code covers access, possession, creation, and distribution of "child pornography", which is defined broadly to include any visual representation, including those made by "electronic or mechanical means" that depicts a "person" who is or is represented as a minor engaging in "sexual activity" or the "dominant characteristic" of which is, "for a sexual purpose", the exhibition of a minor's genitals or anus *(R.S.C., 1985, c. C-46 s. 163.1(a)(1))*. This definition extends beyond visual depictions to include written material, audio recordings, and other representations that advocate or counsel sexual activity

with a minor that would be an offense under the Criminal Code *(R.S.C., 1985, c. C-46 s. 163.1(b)-(d))*.

Punishment usually entails imprisonment with varying duration based on the act committed *(R.S.C., 1985, c. C-46 s. 163.1(2)-(3); R.S.C., 1985, c. C-46, s. 163.1(4), (4.1))*. Aggravating factors, such as intent to profit or involvement of particularly young victims, may result in harsher sentences, with offenders also subject to mandatory registration on the National Sex Offender Registry *(R.S.C., 1985, c. C-46 s. 163.1(4.3))*.

Persons and organisations that provide internet services must also report tips regarding websites that may contain CSAM to the Canadian Centre for Child Protection and law enforcement if they believe a CSAM offense has been committed using their service *(S.C. 2011, c. 4)*. Failure to report can result in fines for repeat violations, and 6 months imprisonment for individuals.

On the matter of application of the "child pornography" statute to AI-generated CSAM relies, the Supreme Court of Canada has said:

> *"The available evidence suggests that explicit sexual materials can be harmful whether or not they depict actual children. Moreover, with the quality of contemporary technology, it can be very difficult to distinguish a 'real' person from a computer creation or composite. Interpreting 'person' in accordance with Parliament's purpose of criminalising possession of material that poses a reasoned risk of harm to children, it seems that it should include visual works of the imagination as well as depictions of actual people. Notwithstanding the fact that 'person' in the charging section and in s. 163.1(1)(b) refers to a flesh-and-blood person, I conclude that 'person' in s. 163.1(1)(a) includes both actual and imaginary human beings." (R. v. Sharpe, 2001)*

That said, the Court carved out two exceptions to the possession provision where regulation could not be justified under the *Charter*: 1) self-created,

privately held works of imagination and 2) lawfully created visual recordings of consensual sexual activity involving the possessor and held for private use (*R. v. Sharpe, 2001,* para.76).[2] These exceptions do not insulate individuals who possess such materials with the intent to distribute them.

The Court emphasised that regulation is constitutionally justifiable if there is a "reasonable risk" of harm to children, categorising harm as per section 163.1 as follows: 1) child sexual abuse and exploitation of children who are used in the production of CSAM and whose images are disseminated over time; 2) normalising deviant sexual behaviour that increases the risk of physical harm to children; 3) fuelling fantasies that incite violence against children; and 4) the use of CSAM to groom children in order to facilitate physical sexual offenses against them (paras. 85-94). As a result, in 2023, a Provincial court in Quebec sentenced a man to over 3 years in prison for using deepfake technology to produce synthetic videos of children being sexually assaulted, making it the first case in the country to address AI-generated CSAM (Serebrin, 2023), evidencing the broad interpretation of "child pornography" laws in the country.

Obscenity

Section 163 of the Criminal Code governs offenses related to the creation and distribution of "obscene" material." *(RSC 1985, c C-46, s 163)*. The core of these prohibitions is found in Section 163(8), which defines "obscene material" as any matter of which the "dominant characteristic" is the "undue exploitation of sex," or a combination of sex and either crime, horror, cruelty, or violence (ibid., s 163(8)). Notably, Section 163(5) removes intent from consideration—if

[2] *See also* R v Barabash, [2015] SCC 29 (holding that any exemptions to the law were only valid if no factual exploitation or abuse of children was involved in creating the materials.).

the material meets the definitional threshold, it constitutes an offense punishable by up to two years imprisonment *(RSC 1985, c C-46, s 169)*.[3]

The potential applicability of these provisions to AI-generated CSAM is guided by the principles set forth by the Supreme Court in *R v. Butler*. In this landmark decision, the Court evaluated whether the legal definition of obscenity infringes on the right of free expression under Section 2(b) of the *Canadian Charter of Rights and Freedoms (R. v. Butler, 1992)*. To qualify as obscene, the exploitation of sex must not only be its dominant focus, but such exploitation must also be "undue." To aid in the Court's analysis, Justice Sopinka articulated three categories of potentially obscene materials:

1. Explicit sex with violence, which almost always meets the threshold of obscenity.
2. Explicit sex without violence but involving degradation or dehumanisation, which qualifies if it poses a substantial risk of harm.
3. Explicit sex without violence, degradation, or dehumanisation, which is generally tolerated unless it involves minors (*R. v. Butler*, p.475).

The Court applied the community standards of tolerance test, evaluating what society deems others should not be exposed to, along with the internal necessities test, which exempts material with legitimate artistic, scientific, or literary value. The Court ultimately upheld Section 163, clarifying that the purpose of the law was not "moral condemnation" but rather "the prevention of harm to society," particularly the influence that degrading sexual material can have on public attitudes toward women and children.

[3] RSC 1985, c C-46, s 169. An obscenity charge is a hybrid offense that can be treated as either a summary offense (minor crimes) or an indictable offense (major crimes), depending on prosecutorial discretion.

Similarly, AI-generated CSAM can blur boundaries around the acceptability of sexualising minors, reinforcing dangerous ideologies that could lead to real-world abuse. As with traditional obscenity laws, the focus of regulation must remain on the harmful influence of such material on societal norms, rather than the presence of real individuals.

The broad language of Section 163 suggests that AI-generated CSAM could fall within its ambit, although Canadian courts have yet to address this issue directly.

Non-consensual Publication of Intimate Images

Section 162.1 of the Criminal Code prohibits the non-consensual publication, distribution, and sale of intimate images, and Section 164.1 empowers courts to order the removal and destruction of such content, including CSAM, voyeuristic recordings, and advertisements for sexual services, whether distributed through print media or via digital platforms *(Criminal Code, RSC, 1985, c. C-46, s 162.1, 164.1)*. To secure a conviction, the prosecution must prove that the defendant knowingly or recklessly distributed the image without the consent of the individual depicted *(s 162.1)*.

Section 162.1(2) defines an "intimate image" as a visual image or recording, created by any means, of a person who is nude, exposing their genitals or breasts, or engaged in sexual activity *(s 162.1(2))*. This definition also requires that, at the time the image was taken, the circumstances gave rise to a reasonable expectation of privacy, and that the person depicted maintains this expectation when the offense occurs *(s 162.1(2)(b)-(c))*. While these provisions explicitly reference photographic, film, or video recordings, their application to deepfake pornography remains open to judicial interpretation. In the context of

AI-generated CSAM, the key legal questions would be whether the content meets the statutory definition of an "intimate image" (likely) and whether the child depicted has a reasonable expectation of privacy regarding the photograph (less likely). As courts begin to interpret these statutes in the context of evolving AI technologies, the ability to criminalise and remove AI-generated CSAM will depend on how concepts like consent, reasonable expectation of privacy, and distribution are applied to synthetic content.

ii. Privacy Legislation

Privacy legislation is critical in addressing the risks posed by AI systems, particularly those employing deepfake technologies. When AI-generated outputs expose personal or sensitive information without consent, it may constitute a privacy violation.

At the federal level, the *Personal Information Protection and Electronic Documents Act (PIPEDA)* establishes guidelines for how private-sector entities must collect, use, and disclose personal information while engaged in commercial activities *(PIPEDA, S.C. 2000, c. 5)*. Provinces such as Alberta, British Columbia, and Quebec have enacted their own private laws that apply to the private sector and are considered substantially similar to the PIPEDA. As a result, organisations operating under these provincial jurisdictions are typically exempt from PIPEDA's requirements concerning intra-provincial activities. [4]

Under the PIPEDA, the collection, use, or disclosure of personal information must be consistent with what a "reasonable person" would consider appropriate

[4] Personal Information Protection Act, SA 2003, c P-6.5 (Alberta); Personal Information Protection Act, SBC 2003, c 63 (British Columbia); An act respecting the protection of personal information in the private sector, c P-39.1 (Quebec); other provinces such as Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have adopted similar legislation governing personal health information.

under the circumstances (Office of the Privacy Commissioner Canada, 2024a). The Office of the Privacy Commissioner of Canada (OPC) (2024a) emphasises that managing personal information in illegal or potentially harmful ways is inherently inappropriate. Sensitive information—such as biometric data (OPC, 2021), details related to an individual's sexual practices or preferences (OPC, 2016), and information that could affect one's reputation (OPC, 2013; OPC, 2016)—requires additional protection due to its potential to cause long-term harm if compromised.

Additionally, in response to emerging risks of AI technologies, both the OPC and provincial privacy regulators, issued the *Principles for Responsible, Trustworthy, and Privacy-Protective Generative AI Technologies (Generative AI Guidance*) (OPC, 2023). This guidance interprets existing privacy laws in relation to generative AI systems and underscores the importance of obtaining explicit consent when utilising personal information to train or deploy these technologies. The guidance discourages the use of data scraping to collect personal information without consent, which is critical given that these datasets frequently include identifiable information (OPC, 2023). Notably, it anticipates the creation of non-consensual deepfakes will be prohibited, though courts have not issued definitive ruling on many AI-related privacy issues (OPC, 2023).

iii. Copyright Law

Advancements in machine learning and data mining have enabled AI systems to generate content that mimics human-created works, raising important questions about authorship and ownership under Canadian copyright law. Traditionally, Canadian law requires a "natural person exercising skill and judgment" to qualify as the creator of a work *(CCH Canadian Ltd. v. Law Society of Upper Canada, 2004, para. 16)*. While individuals may meet this threshold in AI-assisted works, those

issuing simple prompts to generative AI systems like ChatGPT are less likely to qualify.

Liability concerns extend to both primary infringement, which requires access, reproduction, and substantial copying of original works, as well as secondary infringement, which occurs when an individual knows or should have known that a work was infringing material and undertakes an additional act in relation to that work in violation of the Copyright Act (Government of Canada, 2021). In the context of CSAM, users may face secondary liability if they prompt AI systems to create explicit or harmful content and then share it with other users. However, without a clear framework for authorship, it remains difficult to determine whether accountability lies with the user, developer, or the service provider.

The use of data mining techniques to train AI models further complicates the legal landscape. This process involves copying and analysing extensive datasets which often contain copyrighted material to identify patterns and generate predictions (Chen, 2020). In Canada, there are two primary exceptions to copyright infringement that might apply to data mining activities: 1) fair dealing, which allows limited use of copyrighted materials for research; and 2) the technological process exception, which applies to material created automatically during technological operations that are erased after completion *(Copyright Act, R.S.C., 1985, c. C-42, s. 29)*. The application of both exceptions to AI-related data mining activities is unclear under current Canadian law.

These uncertainties in copyright law raise critical issues when applied to the context of AI-generated CSAM. AI systems trained on datasets scraped from the internet—without proper consent or oversight mechanisms in place—could inadvertently produce explicit content featuring the likeness of real children. Liability for such content remains difficult to assign, as it is unclear whether responsibility rests with the developer, user, or the AI system itself. Additionally,

proving infringement becomes more complex when AI-generated outputs resemble existing copyrighted works but are created through automated processes. Courts will likely soon be asked to grapple with these questions regarding liability.

The issue of AI authorship is currently before Canada's Federal Court following a controversial decision by the Canadian Intellectual Property Office (CIPO) to grant a copyright registration for an AI-generated image titled *Suryast*, which combined a photograph of a sunset with Van Gogh's painting *The Starry Night.* If upheld, the registration raises the possibility that developers or users could claim ownership of AI outputs and potentially avoid liability by shifting responsibility for the misuse of their systems to other actors involved in the content's generation and distribution.

Ultimately, the unresolved intersection of authorship and liability demonstrates the need for clearer legal standards.

Provincial Legal Frameworks

Provinces play a relatively narrow role in the regulation of "child pornography" and "obscenity" because criminal law falls exclusively within federal jurisdiction. However, provincial agencies are responsible for enforcing the *Criminal Code* provisions within their jurisdictions. While criminal law is federally governed, civil laws at the provincial level—namely privacy and non-consensual distribution of intimate images laws —provide an important avenue for victims to seek redress.

i. Non-Consensual Distribution of Intimate Images

In Canada, 8 provinces and territories have enacted legislation addressing non-consensual distribution of intimate images. [5] These statutes provide a civil right of action to those who have had intimate images distributed without their consent. Notably, only half of these laws address morphed or deepfake images and thus could apply to AI-generated CSAM.

British Columbia's *Intimate Images Protection Act,* which came into effect on January 29, 2024, was the first to include images that have been "digitally altered" and "AI-generated material," including deepfakes, under its definition of "intimate images" (Government of British Columbia, 2024). Internet intermediaries are not immune from this Act, and the *Act's* Regulation provides for administrative penalties against individuals, intermediaries, and other entities should such entities fail to comply with orders made under the legislation. *(Intimate Images Protection Regulation BC Reg 293/2023, s 9(1)(a))* Financial penalties are incurred and are intended to discourage the dissemination of non-consensual intimate images and deepfakes. Manitoba followed suit in June 2024 by adding "fake intimate images created through use of software, machine learning, and AI" to its existing definition of "intimate images." *(The Intimate Image Protection Amendment Act, S.M. 2024, c. 17, s. 1)*

Nova Scotia's law, the *Intimate Images and Cyber-Safety Act* (2017), is unique, and among the most comprehensive in that it also covers cyberbullying which is defined broadly as "an electronic communication" that is intended or likely to cause harm to another's health or well-being (c. 7, s. 1), expressly including AI-generated materials. Successful plaintiffs can be ordered to receive general, special, aggravated, or punitive damages, and can also demand that the intimate image be removed from the internet. Finally, the law in Prince Edward Island defines "intimate image" broadly and explicitly affirms that one may have a

[5]Those provinces and territories are Alberta, British Columbia, Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Saskatchewan and Prince Edward Island.

reasonable expectation of privacy in an altered image (2020,c.55,s.2; 2020,c.71,s.2).

To date, courts have not heard cases involving AI-generated images under these provincial laws.

ii. Statutory and Common Law Privacy Torts

The right to privacy is protected under common law torts and privacy legislation in Canada. Some provinces and territories including British Columbia, Saskatchewan, Manitoba, Newfoundland and Labrador, and Quebec have passed personal privacy legislation that broadly prohibits violating the privacy of another and that could be used to seek redress for AI-generated CSAM. The remaining provinces and territories do not have personal privacy legislation but victims in those jurisdictions may be able to rely on one or more common law privacy tort theories to seek redress.

Intrusion upon seclusion and public disclosure of private facts are two common law torts that have so far only been recognised in Alberta, Ontario, and Nova Scotia *(Carbone v Burnett, 2019; Jones v Tsige, 2012; Doucette v. Nova Scotia, 2016)*. To succeed on a claim for intrusion upon seclusion the aggrieved must prove a reckless invasion into their private affairs of the kind that a reasonable person would find to be highly offensive and that the intrusion resulted in distress, humiliation, or anguish. Similarly, to establish a claim for public disclosure of private facts the aggrieved must prove publication of an aspect of their private life without consent in a manner that would be highly offensive to a reasonable person in the aggrieved' s position *(Jane Doe 72511 v. N.M., 2018; Racki v Racki, 2021; EV v Shellington, 2021)*. While provincial courts have not yet dealt with the question of whether individuals have a reasonable expectation of privacy in a digitally altered or AI-generated image of themselves, image-based

abuse claims have been successful in Ontario and Alberta *(Jane Doe 72511 v. N.M., 2018; EV v Shellington, 2021)*.

At present, British Columbia, Saskatchewan, and Newfoundland and Labrador have legislation in place that prohibits the unauthorised use of a person's name, likeness, or personality for financial gain. Posting a deepfake image or video on a website that monetises it in some capacity, including by monetising traffic through advertisements, could represent a cause of action. This tort could also potentially be used to put more pressure on host websites to take on a more active role in vetting the material uploaded on their platforms.

Finally, courts in Ontario and British Columbia recognize the common law tort of false light as set forth in the American *Restatement Second of Torts (Yenovkian v Gulian, 2019; Durkin v Marlan, 2022)*.

iii. Intentional Infliction of Mental Suffering and Harassment Torts

Intentional infliction of mental suffering (IIMS) is another common law tort that may be available to victims of image-based abuse. To prove IIMS, you must show that the defendant intentionally–or with reckless disregard as to the potential to cause emotional distress– engaged in flagrant or outrageous conduct causing plaintiff to suffer a visible and provable illness such as anxiety or depression (e.g., *Lu v. Shen, 2020)*. The tort of harassment is similar to a claim for IIMS though the test requires only that the plaintiff suffer emotional distress rather than illness, for which the defendant's conduct was a proximate cause. Since this test is a lower bar than the test for IIMS, harassment may be a viable avenue for legal recourse if subsequent case law upholds this tort. The obvious difficulty

with respect to both types of claims is proving that the creation of AI-generated CSAM was intended to produce harm rather than having been produced for the creator's pleasure.

Regulatory Framework for Developers and Online Service Providers

In April 2023, the Canadian federal government updated its *2020 Directive on Automated Decision-Making*—part of Canada's broader *Policy on Service and Digital*—to address the risks posed by emerging AI technologies (Government of Canada, 2024). The Directive outlines administrative obligations for automated decision-making in the absence of binding AI legislation, emphasising principles such as understanding AI's impact, ensuring transparency, and protecting privacy. It also mandates essential practices, including bias testing and recourse mechanisms to support accountability and fairness. Since then, lawmakers introduced legislation on AI governance that extends beyond public administration to ensure responsible design and deployment across all systems. Two bills in particular, the *Artificial Intelligence and Data Act* and the *Online Harms Act*, received widespread support, but were eventually terminated due to the prorogation of the Canadian Parliament in January 2025.

i. Artificial Intelligence and Data Act

The *Artificial Intelligence and Data Act* ("AIDA") was the federal government's answer to the problem of AI under-regulation. It focused on regulating organisations that develop AI systems. Among these obligations, organisations that develop or make AI systems available for use are required to identify, assess, and mitigate the risk of harm caused by the system. The Act also created a criminal offense for making an AI system available for use knowing or being

reckless as to the fact that it is likely to cause serious physical or psychological harm and where its use actually causes that harm.

The Act would also criminalise the possession or use of personal information in the design, development, operation, or deployment of AI systems when the individual knows, or should know, that the data was obtained— directly or indirectly—through violations of federal or provincial law (s 38). The obligation to implement risk mitigation measures could require developers to, for instance, require organisations to bias their systems against the production of CSAM.

ii. Online Harms Act

On February 26, 2024, Canadian lawmakers introduced the *Online Harms Act*, a landmark bill designed to enhance online safety, protect children, and hold social media companies accountable for content hosted on their platforms *(Bill C-63, 2024)*. The Act was also the first piece of federal legislation to explicitly address deepfakes.

A key focus of the Act was on the protection of children from various forms of harmful online content, including material that sexually victimises a child and "intimate content communicated without consent". The Act defined "intimate content communicated without consent" broadly, to encompass any visual media—such as photographs, films, or videos—that falsely depicts a person, including through deepfake technology, as being nude, exposing their genitalia, or engaging in explicit sexual activity without their consent.

The Act also established the Digital Safety Commission of Canada to enforce compliance, and contribute to the development of regulatory standards, supported by the Digital Safety Ombudsperson.

Finally, the Act would require social media companies to submit digital safety plans, incorporate child protection features into their platforms, and make harmful content inaccessible in Canada.

Overall, and if passed, this Act would have created a new regulatory framework requiring online platforms to act responsibly to prevent and mitigate the risk of harm to children on their platforms. Under the Act, online platforms would have a duty to implement age-appropriate design features and to make content that sexually victimises a child or re-victimises a survivor inaccessible, including via the use of technology, to prevent CSAM from being uploaded in the first instance. A new Digital Safety Commission would oversee compliance and be charged with the authority to penalise online platforms that fail to act responsibly. Accordingly, the Act would create a legally binding framework for safe and responsible AI development and deployment that could potentially apply to restrict or penalise content that would otherwise be legal, but that poses a substantial risk of sexual exploitation or revictimisation of a child.

Prorogation of the Parliament of Canada ended the parliamentary session relevant to this Bill as well as to AIDA. As a result, all proceedings before Parliament ended, and bills that did not receive Royal Assent have been “entirely terminated” (Lexology, 2025).

Conclusion and Recommendations

The Canadian Criminal Code provides robust federal protections against all forms of child exploitation, including AI-generated CSAM. As in the United States, Canada classifies both CSAM and obscenity as prohibited, non-protected speech, making laws that criminalise the production, distribution, and possession of such content the primary legal mechanisms for combating AI-generated CSAM. The Criminal Code also includes protections against the non-consensual distribution of intimate images, which may be invoked to combat morphed images and other malicious uses of AI technologies. However, Canadian courts have read two exceptions to the Code's prohibition on CSAM: material created solely for personal use by the accused and artistic works lacking exploitative intent. Furthermore, the law is unclear regarding non-visual materials, such as AI datasets used to produce CSAM.

Canada still faces challenges in holding tech companies accountable for user-generated content, as Canadian law provides limited means to penalise platforms knowingly hosting or distributing CSAM.

Federal privacy and copyright laws may provide limited protections to victims. Still, privacy laws in Canada often fail to capture the specific harms associated with AI-generated CSAM, while copyright law offers a potential, though complex, avenue for addressing AI-generated CSAM.

In conclusion, while existing CSAM laws in Canada provide a strong foundation of accountability, these statutes were crafted long before generative AI tools gained their foothold online and are clearly insufficient to meaningfully combat the unique dangers posed by these technologies and their outputs. Both countries face significant challenges in prosecuting and regulating AI-generated CSAM due to constitutional constraints, inconsistent and ambiguous statutory

language, and the complexity of enforcing laws in a rapidly evolving technological landscape.

These legal ambiguities underscore the urgent need for a comprehensive regulatory framework that addresses the complexities of AI-generated CSAM. As technology continues to outpace existing laws, the gaps highlighted by cases like *Sharpe* reveal the limitations of traditional statutes in effectively managing the distinct risks associated with synthetic content. To close these gaps and provide clearer guidance for enforcement, lawmakers must consider targeted reforms that not only clarify the status of AI-generated CSAM under "child pornography" and obscenity laws but also address the underlying technological and ethical issues that drive demand for harmful content. The following recommendations propose a series of reforms to modernise existing legal frameworks, ensuring they remain effective against future technological developments:

Recommendation 1: Amend Existing CSAM Laws to Explicitly Cover AI-Generated Content

Current CSAM laws were crafted long before the advent of AI technologies, leaving significant gaps in their applicability to synthetic content such as deepfakes, morphed images, and other AI-generated material. Related provisions in Canada's Criminal Code provide a foundation for criminal liability, but these laws must be updated to explicitly address synthetic CSAM and non-visual depictions.

Federal and provincial laws should also explicitly encompass AI-generated images, moving beyond language focused solely on "computer-generated" imagery. For example, Section 163.1 of Canada's Criminal Code could be revised to cover content created or manipulated using AI, where minors appear to be engaged in explicit conduct, regardless of the involvement of actual children.

Recommendation 2: Amend CSAM Laws to Regulate Model Weights and the Misuse of AI Tools

Reforms must also target unregulated datasets and model weights used to generate synthetic CSAM, which are currently outside the scope of Canadian "child pornography" laws which only cover "visual depictions." To close this loophole, CSAM laws should be amended to explicitly include datasets and model weights within the definition of CSAM and to ban the use of datasets containing CSA, whether in the form of images or audio recordings, for training AI models. This prohibition should require AI developers to verify and document that datasets are free from harmful or exploitative material.

Additionally, CSAM laws should be amended to criminalise the possession and distribution of model weights trained on CSAM. A practical approach would involve classifying AI models trained on illicit datasets as instruments of abuse, similar to laws governing dual-use technologies such as wiretapping devices or software that circumvents copyright protections which serve as a "proximate link" to the crime. The law should also extend to criminalising the creation and distribution of guides or instructions for generating AI-based CSAM.

Moreover, CSAM laws should establish strict liability for AI developers and companies whose models, knowingly or through negligence, contribute to the creation or distribution of CSAM including via the distribution of model weights created with unvetted training data.

Recommendation 3: Establish a Legally Binding Framework for Safe and Responsible AI Development and Deployment

Effective AI governance requires the establishment of a legally binding framework for safe and responsible AI development and deployment. To prioritise child safety, this framework should delineate key operational standards for developers and online service providers. These standards may include designing AI models with built-in safeguards, such as biasing algorithms against generating CSAM and embedding mechanisms to detect language or prompts commonly associated with misuse. High-risk AI models should undergo mandatory pre-release audits and a certification process, similar to protocols in the pharmaceutical and financial sectors, to assess potential risks, including the capacity to generate CSAM, before deployment.

Developers should also be required to increase transparency by disclosing the metadata and datasets used in AI model training. Online service providers, in turn, must publish annual reports detailing their content moderation practices, conduct safety audits following harmful incidents, and face temporary suspension if they fail to mitigate risks effectively. Continuous auditing and moderation of AI-generated content should be mandatory to prevent the circulation of harmful material on these platforms. Measures should include filtering search terms associated with CSAM, and suspending accounts distributing abusive content.

Such a framework would promote accountability and ensure that AI technologies are developed and deployed responsibly, prioritising child safety at every stage.

Recommendation 4: Expand Legal Protections to Include Control Over One's Own Image

Canada should amend existing privacy laws or adopt new legislation that grants individuals the right to control the use of their image and likeness. With the

proliferation of digital technologies and AI-driven media, unauthorised use of a person's likeness has become not only easier but significantly more damaging. Expanding privacy protections to include control over one's image and likeness would allow individuals to prevent misuse, such as the creation and distribution of non-consensual synthetic media or deepfakes. Such protections would support personal and reputational rights, ensuring dignity, autonomy, and control over one's digital identity.

Alternatively, or in addition to privacy laws, several key changes to copyright laws could be adopted to support victim redress in cases of AI-generated CSAM. First, copyright laws could be revised to allow for the transfer of ownership from offenders to victims through plea agreements or civil settlements, granting victims control over unauthorised AI-generated images depicting their likeness. This approach is akin to the government's authority to seize contraband and can inform this novel approach. By granting copyright ownership to victims, they would gain the right to pursue damages, issue takedown requests, and prevent further use of their likeness in exploitative materials.

To strengthen protections against the exploitation of minors, copyright laws could also be amended to grant children inherent ownership over their own image, thereby providing them exclusive control over unauthorised uses, particularly in cases involving AI-generated content, deepfakes, or synthetic media. New language could be added to existing laws as follows: "Notwithstanding any other provision to the contrary, ownership rights in an image shall not extend to photographs or likenesses of a minor, who shall possess an automatic right to control the use of their image." Additionally, provisions related to infringement could be amended to add "any individual who captures or publishes a photograph or likeness of a minor shall be liable for infringement of the minor's image rights. The minor shall be entitled to pursue all remedies available under this title for such infringement." To balance these

protections with practical considerations, the amendment could establish exceptions including for personal or family use, express consent, and incidental capture. This measure would allow children and their guardians to prevent the distribution or misuse of their likeness in harmful ways.

References

Literature Review and Methodology

Bahoo, S., Cucculelli, M., & Qamar, D. (2023). Artificial intelligence and corporate innovation: A review and research agenda. *Technological Forecasting & Social Change*, 188. https://doi.org/10.1016/j.techfore.2022.122264

Fisher, C., Goldsmith, A., Hurcombe, R., & Soares, C. (2017). *The impacts of child sexual abuse: A rapid evidence assessment*. Independent Inquiry Into Child Sexual Abuse. Retrieved from https://www.iicsa.org.uk/reports-recommendations/publications/research/impacts-csa.html

Huang, J, C. (2022). From Building Information Modeling to Extended Reality. In M. Bolpagni, R. Gavina & D. Ribeiro (Eds.), *Industry 4.0 for the Built Environment Methodologies: Technologies and Skills* (pp. 471-494). New York: Springer.

Internet Watch Foundation. (2023). *How AI is being abused to create child sexual abuse imagery*. Retrieved from https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

Lee, H., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*, 34, 1-11. https://doi.org/10.1016/j.fsidi.2020.301022

McConville, M., & Chui, W.H. (2007). Introduction and overview. In M. McConville & W.H. Chui (Eds.), *Research Methods for Law* (pp. 1-17). Edinburgh: Edinburgh University Press.

Ness, S., Riley, C., & Bantourakis, M. (2023, September 23). Digital Governance over online safety is at risk of fragmenting. A multistakeholder approach could prevent that. World Economic Forum. Retrieved from https://www.weforum.org/stories/2023/09/its-time-for-global-alignment-on-digital-governance/

Ngo, N. (2021). Child sexual abuse violence against human dignity of children. *International Journal of Research Studies in Education*, 10(15), 97-108. https://doi.org/10.5861/ijrse.2021.a124

Ngo, N., McKeever, S., & Thorpe, C. (2023). *Determining Child Sexual Abuse Posts based on Artificial Intelligence*. Technological University Dublin. Retrieved from https://arrow.tudublin.ie/scschcomcon/392/

Parti, K., & Szabo, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws*, 13(6), 67. https://doi.org/10.3390/laws13060067

Quayle, E. (2016). *METHOD GUIDE 7: Researching online child sexual exploitation and abuse: Are there links between online and offline vulnerabilities?* Global Kids Online. Retrieved from http://globalkidsonline.net/wp-content/uploads/2016/05/Guide-7-Child-sexual-exploitation-and-abuse-Quayle.pdf

Simon, J., Luetzow, A., & Conte, J.R. (2020). Thirty years of the convention on the rights of the child: Developments in child sexual abuse and exploitation. *Child Abuse & Neglect*, 110, 1-8. https://doi.org/10.1016/j.chiabu.2020.104399

Weaver, J.M., & Røseth, T. (2024). The “Five Eyes” Intelligence Sharing Relationship : A Contemporary Perspective (1st ed. 2024.). London: Springer International Publishing.

Wright, L. (2018). Black-Letter Law. *LawNow Magazine*. https://www.lawnow.org/black-letter-law/

Canada

An Act Respecting the Protection of Personal Information in the Private Sector, c. P-39.1 (Quebec)

Bill C-13, Protecting Canadians from Online Crime Act, 2nd Sess., 41st Parl. (2015)

Bill C-27. (2022). An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act, 1st Sess, 44th Parl

Bill C-63. (2024). Online Harms Act, 1st Sess. 44th Parl

CCH Canadian Ltd. v. Law Society of Upper Canada, [2004] 1 S.C.R. 339

Century 21 Canada Ltd. Partnership v. Rogers Communications Inc., 2011 BCSC 1196

Chen, M. (2020, October 21). *A guide: Text analysis, text analytics & text mining. Towards Data Science*. Retrieved from https://towardsdatascience.com/a-guide-text-analysis-text-analytics-text-mining-f62df7b78747

Civil Code of Québec, CQLR c. CCQ-1991

Copyright Act, R.S.C., 1985, c. C-42, s. 29

Criminal Code, R.S.C., 1985, c. C-46

Durkin v. Marlan, 2022 BCSC 193

EV v. Shellington, 2021 ABQB 739

Government of British Columbia. (2024). *Intimate Images and Consent.* Retrieved from https://www2.gov.bc.ca/gov/content/safety/public-safety/protecting-vulnerable-populations/intimate-images-and-consent

Government of Canada. (2021). *Copyright infringement.* Retrieved from https://ised-isde.canada.ca/site/canadian-intellectual-property-office/en/copyright-infringement

Government of Canada. (2024). *Policy on Service and Digital*. Retrieved from https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32603.

Intimate Images and Cyber-protection Act, S.N.S. 2017, c. 7

Intimate Images Protection Act, R.S.N.L. 2018, c. I-22

Intimate Images Protection Act, R.S.P.E.I. 1988, c. I-9.1

Intimate Images Protection Regulation, B.C. Reg. 293/2023, s. 9(1)(a)

Jane Doe 72511 v. N.M., 2018 ONSC 6607

Lexology. (2025). Prorogation's Digital Impact: Canada's Digital Bills Set to Die on the Order Paper. Lexology. https://www.lexology.com/library/detail.aspx?g=5e9b0d85-d01d-42e9-8a51-f1ad1bce0956&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-

+General+section&utm_campaign=Australian+IHL+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2025-01-21&utm_term

Lu v. Shen, 2020 BCSC 490

Merrifield v. The Attorney General, 2017 ONSC 1333

Office of the Privacy Commissioner of Canada. (2013). *PIPEDA Report of Findings #2013-003: Profiles on PositiveSingles.com dating website turn up on other affiliated dating websites*. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-003/

Office of the Privacy Commissioner of Canada. (2016). *PIPEDA Report of Findings #2016-005: Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner.* Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/.

Office of the Privacy Commissioner of Canada. (2021). *PIPEDA Report of Findings #2021-001: Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner of British Columbia, and the Information of the Privacy Commissioner of Alberta.* Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

Office of the Privacy Commissioner of Canada. (2023). *Principles for responsible, trustworthy and privacy-protective generative AI technologies.* Retrieved from

https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/

Office of the Privacy Commissioner of Canada. (2024a). *PIPEDA fair information principles.* Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.

Office of the Privacy Commissioner of Canada. (2024b). *Pornhub operator failed to obtain meaningful consent before allowing adult content to be posted on its websites.* Retrieved from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/nr-c_240229/

Personal Information Protection Act, S.A. 2003, c. P-6.5 (Alberta)

Personal Information Protection Act, S.B.C. 2003, c. 63 (British Columbia)

Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5

Privacy Act, R.S.B.C. 1996, c. 373

Privacy Act, R.S.N.L. 1990, c. P-22

Privacy Act, R.S.S. 1978, c. P-24

Protecting Victims of Non-Consensual Distribution of Intimate Images Act, R.S.A. 2017, c. P-26.9

R. v. Barabash, [2015] SCC 29

R. v. Butler, 1992 CanLII 124 (SCC), [1992] 1 S.C.R. 452

R. v. Sharpe, [2001] 1 S.C.R. 45, 2001 SCC 2

R. v. Verner, 2017 ONCJ 415

Racki v. Racki, 2021 NSSC 46

Right to Information and Protection of Privacy Act, S.N.B. 2009, c. R-10.6

Serebrin, J. (2023, April 26). Quebec man who created synthetic, AI-generated child pornography sentenced to prison. *The Canadian Press.* Retrieved from https://www.cbc.ca/news/canada/montreal/ai-child-abuse-images-1.6823808.

SOCAN, Re: Sound, CSI, Connect/SOPROQ, Artisti – Tariff for Commercial Radio, 2011-2017 (2016). Retrieved from https://decisions.cb-cda.gc.ca/cb-cda/decisions/en/366778/1/document.do

Statutes of Canada (S.C.), 2011, c. 4

The Intimate Image Protection Act, C.C.S.M., c. 187

The Privacy Act, C.C.S.M., c. P125

Trader v. CarGurus, 2017 ONSC 1841

Yenovkian v. Gulian, 2019 ONSC 7279

More information

Suggested citation: Schidlow, J., Gaitis, K.K., Lu, M., Stevenson, J., & Fry, D. (2025). Legal challenges in tackling AI-generated child sexual abuse material across the 5 Eyes nations: Who is accountable according to the law? Canada. Edinburgh: Childlight – Global Child Safety Institute

Registered study protocol: OSF Registries | Does existing legislation on CSEA/CSAM across the Five Eyes nations and India allow for criminal liability or any other form of accountability with regards to AI-generated CSAM?

Ethics approval: University of Edinburgh, Childlight Research Ethics Sub-Committee (DELOC-KKG-0030424CL)

Advisory committee members: Professor Ben Mathews (School of Law, Queensland University of Technology), Dan Sexton (Chief Technology Officer, Internet Watch Foundation), Michael Skwarek (Manager, Codes and Standards Class 1, Industry Compliance and Enforcement, Australian eSafety Commissioner)

Funding acknowledgement: The research leading to these results has received funding from the Human Dignity Foundation under the core grant provided to Childlight – Global Child Safety Institute under the grant agreement number [INT21-01].