Beyond Copyright

A Roadmap For Canada To Protect Our Faces And Voices From Generative AI

Analysis prepared for OpenMedia by Parinay Gupta | April 2026

Content

Part I: Introduction 1
Part II: Background – Biometrics As Fuel For AI 3
Part III: Legal Vacuum in Canada 6
Part IV: Comparative Jurisdictional Analysis 8
    United States (The Right of Publicity Approach) 8
    European Union (The Data Protection and Transparency Approach) 9
    China (The Strict Personality Rights Approach) 10
    Denmark (The Copyright Approach) 11
Part V: Feasibility, Pros And Cons Of Canadian Copyright Law For Likeness 12
Part VI: Policy Recommendations 15
Part VII: Conclusion & Way Forward 18

Part I: Introduction

The rise of Generative Artificial Intelligence (GenAI) has rapidly transformed the digital media landscape, fundamentally reshaping how personal identity is understood and introducing a new wave of unprecedented challenges. These GenAI models are capable of utilizing advanced machine learning architectures to seamlessly copy or superimpose a person's face onto another person's body and mimic another person's human speech. Such techniques can be performed at a shockingly fast rate where texts, images, audio and videos are produced at an unprecedented scale, with negligible or zero marginal costs to make these forms of media indistinguishable from authentic content.[1]

These "vocal clones" and "deepfakes" are capable of replicating a person's vocal style, cadence, pitch and physical likeness with a degree of realism that makes the artificial output practically indistinguishable from genuine audio or video recordings. Thus, GenAI presents an impressive but dangerous technological leap with its ability to accelerate the creation of fake environments and realities where identities, content and interactions are artificially created.[2]

In 2024, Hollywood actress Scarlett Johansson expressed anger and shock when OpenAI released a voice assistant named "Sky" bearing an uncanny likeness to her own, despite her earlier refusal to license her own voice.[3] Similarly, voice actor Paul Skye Lehrman was dismayed to find his voice cloned without his permission and used in a YouTube video commenting on the geopolitical conflict in Ukraine. These incidents are not isolated anomalies; they represent a fundamental shift in the digital landscape where human identity is increasingly vulnerable to synthetic exploitation and replication.

Amidst this technological boom, an especially notable area of resistance has begun between AI developers, who need massive amounts of data to train their algorithms, and individuals, who have either non-existent or extremely low legal control over their physical as well as biometric identities.[4] AI companies build their foundational GenAI models by methodically scraping the internet for publicly available audio, video recordings and images, effectively harvesting biometric data, such as facial voiceprints, without any authorization or express consent. It is critical to understand that vocal and facial features, unlike abstract data or text, are inherently biometric; meaning they are unchangeable characteristics closely tied to a person's unique identity.[5] When tech companies commodify these characteristics into data designed to train and power AI models, they convert one's personal identity into a tradable asset.[6] This dynamic exposes ordinary individuals and even public figures alike to extreme risks, ranging from financial fraud and reputational damage to non-consensual production of deepfake pornography

[1] Emilio Ferrara, "Synthetic Reality: The Systemic Epistemic Vulnerability of Generative AI" (2026) at 4.
[2] *Ibid* at 3.
[3] Robert Dale, "Soap 'n' AI" (2024) 30 Natural Language Engineering 1155.
[4] Anja Neubauer, Martin Wynn & Robin Bown, "AI, Authorship, Copyright, and Human Originality" (2026) 6 Encyclopedia 1 at 7
[5] Adam Eric Berkowitz & Miriam E Sweeney, "Look Who's Talking: Voice Cloning as Tension Point Between Identity and Data" (2025) at 13
[6] *Ibid* at 13.

and the unauthorized duplication of creative works.[7] Despite the obvious possible harms relating to these existential threats, the existing Canadian legal regime frequently leaves individuals legally defenseless, treating their physical attributes as public property rather than proprietary rights.

The current Canadian regulatory vacuum has been slow to adapt to the coming of GenAI[8] when compared to jurisdictions around the world that are currently adopting very different approaches so as to safeguard human identity against replication powered by machines.[9] To create the roadmap for this Canadian legal reform, this paper conducts a comparative jurisdictional analysis of alternative international frameworks currently struggling to address the AI identity crisis.[10] While global responses remain highly divergent, they provide an essential foundational basis for Canada's path forward.[11]

The United States has chosen to rely on a heavily fragmented, state-level right of publicity, illustrated by Tennessee's recently enacted ELVIS Act,[12] which explicitly protects a person's voice against unauthorized cloning used for commercial purposes. The European Union addresses deepfakes through a robust data transparency and protection lens, utilizing the GDPR[13] and the AI Act[14] to compel platforms to respect biometric privacy and label any generated content.[15] China has implemented targeted, stringent regulations requiring providers to obtain separate, explicit consent before using or modifying an individual's biometric information.[16] Denmark, on the other hand, is considering a proposal for an approach by proposing amendments to its Copyright Act to directly grant individuals intellectual property protection against the unauthorized digital imitation of their physical characteristics.[17]

By critically evaluating the strengths and limitations of these approaches in Tennessee, the EU, China, and Denmark, this paper will demonstrate why expanding Canadian copyright to cover biometric identity offers the most concrete legal remedy against unauthorized exploitation.

---

[7] L Kyi et al, "Governance of Generative AI in Creative Work: Consent, Credit, Compensation, and Beyond" (2025) at 352

[8] Vasileia Karasavva & Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy" (2021) 24:3 Cyberpsychology, Behavior, and Social Networking 203 at 206.

[9] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 23.

[10] Chopra, Sony AL & Chopra, *supra* note 2 at 37.

[11] Endang Prihatin, "Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum" (2025) 10th International Conference on Sustainability 87 at 88.

[12] *Ensuring Likeness Voice and Image Security Act*, Tenn Code Ann § 47-25-1101 (2024) [ELVIS Act].

[13] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [GDPR].

[14] *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, [2024] OJ, L 2024/1689 [AI Act].

[15] Chopra, Sony AL & Chopra, *supra* note 2 at 30-33.

[16] Hui Xu et al, "China's New AI Regulations" (16 August 2023) Latham & Watkins Privacy & Cyber Practice Number 3110 at 4.

[17] Sofia Karttunen, "The Danish approach to copyright and deepfakes: A model for the EU?" (2026) European Parliamentary Research Service PE 782.611 at 1.

Protecting our faces and voices through copyright will firmly establish that an individual's physical persona is an inviolable, protected asset in the generative AI era.[18]

Part II: Background – Biometrics As Fuel For AI

GenAI models have unprecedented capabilities to create realistic media, but these systems require immense volumes of raw data to function.[19] At the core of this vast data supply chain are human biometrics.[20] Biometric data is technically and legally defined as personal data resulting from specific processing relating to the physical, physiological, or behavioural characteristics of a natural person.[21] In order to understand the fuel that powers GenAI, it is crucial to distinguish between the two main categories of biometrics that are being systematically generated and scraped: physiological biometrics and behavioural biometrics.[22]

Physiological biometrics refer to the unalterable, inherent physical features that uniquely identify a human being. This category includes highly specific physical traits such as fingerprints, facial geometry, DNA, eye irises and palm prints.[23] GenAI models utilize scraped personal photos and videos to learn these unique facial geometries, allowing the algorithms to accurately generate, replace, or edit biometric features to create highly convincing visual media.[24] Conversely, behavioural biometrics include the dynamic characteristics relating to how a person acts, moves, or speaks such as distinctive movement patterns like "gait" and voice. Voice is a highly complex behavioural biometric characterized by both physiological attributes i.e. audible texture and timbre and behavioural speech patterns i.e. pitch, cadence, rhythm and meter.[25] GenAI audio models are capable of analyzing and decoding these attributes to perfectly clone an individual's unique vocal signature, creating artificial speech that flawlessly mimics the original speaker.[26]

Developing and refining these highly sophisticated GenAI models depends almost entirely on mass data scraping from the public. To build detailed, advanced foundational models, tech companies and AI developers deploy automated bots and web scrapers to systematically browse, index, and download vast repositories of information from the internet, including video hosting sites, public databases and most dangerously, from social media platforms. This unrestrained data extraction results in the continuous harvesting of billions of personal photos and vocal samples. For example, companies have notoriously built massive databases

---

[18] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 89-91.
[19] Bao Kham Chau & George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity" (2024) at 5.
[20] Tanusree Sharma, Yihao Zhou & Visar Berisha, "PRAC3 (Privacy, Reputation, Accountability, Consent, Credit, Compensation): Long Tailed Risks of Voice Actors in AI Data-Economy" (2025) at 2.
[21] Mais Qandeel, "Facial recognition technology: regulations, rights and the rule of law" (2024) 7 Frontiers in Big Data 1 at 4-5.
[22] Adam Eric Berkowitz & Miriam E Sweeney, "Look Who's Talking: Voice Cloning as Tension Point Between Identity and Data" (2025) 38:131 Philosophy & Technology 1 at 11.
[23] Qandeel, *supra* note 3 at 5.
[24] Lambert Hogenhout & Rinzin Wangmo, "Protecting Persona Biometric Data: The Case of Facial Privacy" (2025) at 2.
[25] Berkowitz & Sweeney, *supra* note 4 at 11.
[26] Berkowitz & Sweeney, *supra* note 4 at 1-2.

containing billions of scraped facial images to train deepfake algorithms and facial recognition.[27] Similarly, foundational audio models require massive datasets of voice recordings, often scaling up to tens of thousands of hours of audio from thousands of different speakers, frequently utilizing publicly available audiobooks, podcasts and online media.[28]

Crucially, current GenAI models use this mass data scraping from the public without their express permission or knowledge.[29] While AI developers frequently justify these practices by claiming the training data is "publicly available," public accessibility does not ethically or legally equate to explicit consent or authorization for biometric cloning and commercial AI training.[30] Extraction of this data, without any form of consent, effectively transforms intrinsic, immutable human characteristics into commodified, tradable assets. Through the logic of surveillance capitalism, human faces and voices are reduced to raw data points, stripping individuals of their agency over their own digital and physical identities.[31]

The consequences of this unregulated AI scraping are vast, creating an environment where biometric cloning leads to severe societal and individual harms.[32] The primary output of this harvested biometric data is the creation of "deepfakes", AI-generated or manipulated audio and visual content that perfectly resembles existing persons and falsely appears to be authentic.[33] These deepfakes pose profound threats across multiple domains by utilizing advanced deep learning architectures including generative adversarial networks (GANs), diffusion models, and transformer-based systems.[34]

First, biometric cloning has become a powerful tool for non-political disinformation.[35] Even outside of electoral politics, deepfakes are increasingly utilized to spread hoaxes, defame individuals, and attribute inflammatory or false statements to innocent people.[36] By manufacturing coherent but entirely artificial realities, malicious actors can manipulate public perception, facilitate targeted cyberbullying, and inflict severe reputational damage on public figures and private citizens alike.[37]

Second, the cloning and weaponization of behavioural biometrics, particularly voice prints, has led to a surge in sophisticated financial fraud.[38] Audio deepfakes are incredibly malignant

[27] Hogenhout & Wangmo, *supra* note 7 at 2.
[28] Chau & He, *supra* note 1 at 5.
[29] Lambert Hogenhout & Rinzin Wangmo, "Protecting Persona Biometric Data: The Case of Facial Privacy" (2025) at 4.
[30] Tanusree Sharma, Yihao Zhou & Visar Berisha, "PRAC3 (Privacy, Reputation, Accountability, Consent, Credit, Compensation): Long Tailed Risks of Voice Actors in AI Data-Economy" (2025) at 4.
[31] Hogenhout & Wangmo, *supra* note 1 at 1.
[32] Trishana Ramluckan, "Deepfakes: The Legal Implications" (2023) at 3-5.
[33] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 4-5.
[34] Vasileia Karasavva & Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy" (2021) 24:3 Cyberpsychology, Behavior, and Social Networking 203 at 203.
[35] Emilio Ferrara, "The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth" (2025) at 9-13.
[36] Ramluckan, *supra* note 5 at 1.
[37] Ferrara, *supra* note 8 at 1-2.
[38] Bao Kham Chau & George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity" (2024) at 3.

because they lack the visual cues that might otherwise betray a forgery.[39] Cybercriminals use voice cloning technology to bypass security measures and execute highly convincing impersonation scams.[40] In a notable corporate example, fraudsters used AI audio cloning to mimic the voice of a UK energy firm's parent company CEO, successfully tricking a subordinate into transferring funds to a fraudulent Hungarian supplier account.[41] On a consumer level, scammers frequently clone the voices of children or relatives to extort families, tricking victims into believing their loved ones have been kidnapped or are in immediate physical or financial peril.[42]

Third, unregulated facial scraping has radically transformed the realm of digital pornography.[43] While AI tools can technically be used to produce consensual pornography, such as adult film artists willingly licensing their likenesses for AI-based generation, the overwhelming and devastating consequence of this technology is its weaponization for non-consensual image-based sexual abuse.[44]. Utilizing widely accessible software, perpetrators map the scraped facial geometries of non-consenting individuals onto the bodies of adult film actors. This tech-facilitated sexual violence targets ordinary citizens and celebrities, causing severe psychological distress, anxiety, depression, and trauma, while victims are left with few effective avenues for content removal as well as legal recourse.[45]

Ultimately, the unchecked generation of synthetic biometrics leads to a complete erosion of trust in digital media.[46] As deepfakes become increasingly sophisticated and indistinguishable from authentic recordings, Canada faces an increasingly worrying scenario where verifying the truth becomes a laborious and costly burden on the relevant institutions. This environment of pervasive digital deception undermines trust in traditional evidence, journalism, and scientific facts. When reality itself can be effortlessly manufactured and manipulated at zero marginal cost,[47] populations may suffer from "reality fatigue," where the confusion between real and AI leads to a cynical societal default setting where even genuine, authentic evidence is routinely dismissed or doubted as fake.[48]

---

[39] Chau & He, *supra* note 11 at 1.
[40] Sharma, Zhou & Berisha, *supra* note 2 at 3.
[41] Chau & He, *supra* note 11 at 1.
[42] Adam Eric Berkowitz & Miriam E Sweeney, "Look Who's Talking: Voice Cloning as Tension Point Between Identity and Data" (2025) 38:131 Philosophy & Technology 1 at 2.
[43] Vasileia Karasavva & Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy" (2021) 24:3 Cyberpsychology, Behavior, and Social Networking 203 at 203.
[44] Karasavva & Noorbhai, *supra* note 1 at 204.
[45] Karasavva & Noorbhai, *supra* note 1 at 204.
[46] Emilio Ferrara, "The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth" (2025) at 5.
[47] Ferrara, *supra* note 8 at 3-4.
[48] Ferrara, *supra* note 8 at 7.

Part III: Legal Vacuum in Canada

Canada currently lacks a standalone, statutory right to personality at the federal level, forcing victims of unauthorized exploitation to rely almost exclusively on the common law tort of misappropriation of personality. This tort was established and refined in landmark cases such as Krouse v. Chrysler Canada Ltd.[49] and Athans v. Canadian Adventure Camps Ltd.[50] To successfully litigate under this tort, a plaintiff must prove that their identity was clearly utilized by the defendant, that this use was explicitly for the purpose of promoting or advertising a sale, and that the defendant achieved unjust enrichment or a commercial gain at the expense of the plaintiff.[51]

This strict legal requirement to prove 'commercial gain' renders the misappropriation of personality tort critically ineffective against the unique mechanisms of Generative AI. First, the tort is practically useless against the foundational step of GenAI development: internal algorithmic training. When tech companies systematically scrape billions of images and vocal samples from the internet to train their AI models, this mass data ingestion happens entirely behind closed doors. Because the AI developers are not directly using a specific individual's face or voice in a public-facing advertisement to sell a product, the commercial gain is highly abstracted across the entire software infrastructure. Consequently, victims of biometric scraping cannot easily satisfy the "sales versus subject" distinction required by Canadian courts to prove misappropriation.[52]

Furthermore, the commercial gain requirement leaves victims entirely defenseless against deepfakes of a non-commercial nature. Deepfake technology is frequently weaponized to create highly realistic but entirely fabricated content designed to harass, intimidate, or degrade individuals.[53] For example, malicious actors routinely use deepfakes to create content wherein a non-consenting person's face is placed onto an adult film actor's body to create non-consensual pornography.[54] These explicit videos are often distributed on unregulated forums or social media platforms out of malice, revenge, or for personal amusement, rather than for direct financial profit. Without a clear commercial transaction to point to, victims of deepfake pornography cannot pursue a misappropriation claim.[55]

Instead, they are forced to navigate a maze of inadequate legal alternatives, such as pursuing claims for the tort of harassment or intentional infliction of mental suffering.[56] However, prosecuting a mental suffering claim requires proving that the perpetrator purposefully calculated to cause harm and that the victim suffered a visible, provable mental illness. This is an exceptionally high burden of proof that completely fails to address the fundamental theft of

---

[49] *Krouse v Chrysler Canada Ltd*, (1973) 1 OR (2d) 225 (CA).
[50] *Athans v Canadian Adventure Camps Ltd*, (1977) 17 OR (2d) 425 (Ont HC); David Collins, "Age of the Living Dead: Personality Rights of Deceased Celebrities" (2001) 39:4 Alta L Rev 914 at 921-922.
[51] Collins, *supra* note 1 at 922.
[52] Collins, *supra* note 1 at 924.
[53] Trishana Ramluckan, "Deepfakes: The Legal Implications" (2023) at 1.
[54] Vasileia Karasavva & Aalia Noorbhai, "The Real Threat of Deepfake Pornography: A Review of Canadian Policy" (2021) 24:3 Cyberpsychology, Behavior, and Social Networking 203 at 203.
[55] Karasavva & Noorbhai, *supra* note 5 at 205.
[56] Karasavva & Noorbhai, *supra* note 5 at 205.

the victim's biometric identity. Similarly, while the harassment tort possesses a slightly lower threshold, requiring severe emotional distress and gross disregard for potential harm, it still does not provide a direct, exclusive remedy for the unlawful appropriation of one's identity.[57]

The Canadian Copyright Act is similarly ill-equipped to provide remedies for victims of biometric cloning. In its current state, the Copyright Act exclusively protects "human-authored works" and relies on the fundamental premise that a protected creation must be the original product of a human's intellectual judgment and skill. This human-centric framework suffers from a clear legal ambiguity regarding whether intrinsic human characteristics, such as a unique gait, a vocal signature, or a human face, can ever be classified as an original creation.

Even if an AI developer scrapes a copyrighted photograph or audio recording of an individual, Canadian copyright law dictates that the economic and moral rights to that media typically vest with the creator of the work, such as the photographer or the record producer.[58] The rights do not automatically vest with the human subject depicted within the media. This legal reality leaves individuals entirely alienated when their images are scraped to train deepfakes, as copyright protects the work and not the persona.

What complicates the situation further is that a deepfake is merely an algorithmically generated output; it can never be deemed to be an exact, direct copy of a single, specific photograph. Given that the originality threshold for copyright can be relatively low, there is an alarming legal risk that the perpetrator who generates the deepfake could theoretically attempt to claim copyright authorship over the artificially generated output.[59] There is a very real slippery slope where by inputting specific prompts into the AI, the author of the deepfake can argue that they have exercised sufficient judgment and skill to author a new work, leaving the actual victim legally defenseless. Consequently, AI tools can extract the essence of a person's vocal style or physical likeness to generate new works without authorization, simultaneously infringing on personal identity while offering the victim no direct recourse over their own biometrics.

This doctrinal inadequacy is severely compounded by the current political landscape in Canada. The continued stalling and effective death of Bill C-27, which included the highly anticipated Artificial Intelligence and Data Act (AIDA), has left Canada in a prolonged state of legal limbo.[60] Without the passage of AIDA, the Canadian government has failed to establish a dedicated, statutory framework that imposes binding, enforceable obligations on AI developers. Consequently, tech companies operating in Canada are not bound by strict federal mandates demanding ethical training, data sourcing, algorithmic transparency or the implementation of proactive technological safeguards against biometric cloning. This regulatory vacuum allows AI developers to continue scraping and deploying biometric data with minimal federal oversight.

In the absence of a modernized AI statute or a standalone property right to personality, the regulation of biometric data collection, at least in the private sector, defaults to the Personal Information Protection and Electronic Documents Act (PIPEDA). Under PIPEDA, the Office of

[57] Karasavva & Noorbhai, *supra* note 5 at 205.
[58] Collins, *supra* note 1 at 923.
[59] Karasavva & Noorbhai, *supra* note 5 at 205.
[60] Ana Brandusescu & Renée E Sieber, "Missed opportunities in AI regulation: lessons from Canada's AI and data act" (2025) 7 Data & Policy e40.

the Privacy Commissioner of Canada (OPC) explicitly categorizes biometric data, such as facial features and voiceprints, as highly sensitive personal information.[61] Businesses seeking to collect or process this data must satisfy a rigorous four-part test demonstrating a legitimate need, effectiveness, minimal intrusiveness, and proportionality.[62] Furthermore, PIPEDA strictly mandates express, informed consent for the processing of biometrics, emphasizing strict data minimization and requiring the prompt destruction of records once their original purpose is fulfilled.

However, while PIPEDA serves as a vital shield against corporate data misuse, it suffers from a critical limitation: privacy law prevents the unlawful processing of data, but it does not grant individuals positive ownership over their likeness. Privacy frameworks are fundamentally designed to protect personal dignity and informational autonomy; they allow individuals to demand the deletion of their data or to halt unauthorized corporate tracking. They do not, however, confer an intellectual property right or a commercial property right that allows an individual to actively control, license, or monetize their physical identity.

Even at the provincial level, where jurisdictions like British Columbia, Manitoba, Saskatchewan, Newfoundland and Labrador, have enacted statutory Privacy Acts that prohibit the unauthorized use of a person's likeness or voice, the protection is still largely restricted to trade purposes and advertising.[63] These privacy-based mechanisms are ultimately reactive tools intended to stop data breaches, falling drastically short of providing Canadians with a proactive, exclusive legal roadmap to protect their faces and voices from systemic exploitation in the GenAI era.

Part IV: Comparative Jurisdictional Analysis

United States (The Right of Publicity Approach)

The United States confronts the unauthorized digital cloning of faces and voices primarily through the "right of publicity," a legal doctrine rooted in property and privacy rights that protects individuals against the unauthorized commercial use of their identity.[64] However, the American approach is highly fragmented, as there is currently no unified federal right of publicity. Instead, the right is governed by a patchwork of state-level statutes and common law precedents, resulting in significant jurisdictional variations regarding what attributes are protected, whether the right extends post-mortem, and what constitutes commercial exploitation.[65] For instance, while some states protect only a person's name and image, others have broadened their scope to include voice, signature, and overall likeness.[66]

A foundational pillar in the American legal landscape for protecting vocal likeness against imitation is the landmark 1988 case, Midler v. Ford Motor Co.[67] In this case, Ford Motor

[61] "Facial Privacy" (2025) at 6.
[62] "Facial Privacy", *supra* note 12 at 6.
[63] Collins, *supra* note 1 at 926.
[64] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 44.
[65] "The Post-Mortem Right of Publicity" (2021) at 17.
[66] Ibid at 1
[67] *Midler v Ford Motor Co*, 849 F2d 460 (9th Cir 1988); Chopra, Sony AL & Chopra, *supra* note 1 at 40.

Company's advertising agency hired a former backup singer of Bette Midler to deliberately imitate Midler's distinctive vocal style for a television commercial after Midler herself declined to participate. At the time, California's statutory publicity right did not explicitly cover voice, forcing the claim to proceed under California's broader common law right of publicity. The United States Court of Appeals for the Ninth Circuit ruled in Midler's favour, famously declaring that "a voice is as distinctive and personal as a face" and that "to impersonate her voice is to pirate her identity". The court established the precedent that deliberately imitating a distinctive voice to sell a product without consent constitutes an actionable misappropriation of identity and a violation of the common law right of publicity. This case remains highly relevant in the age of GenAI, providing the legal foundation to argue that if analogue vocal imitation was illegal in 1988, highly advanced AI-generated voice cloning should trigger the exact same liability today.[68]

As generative AI technologies have accelerated, individual states have begun modernizing their publicity laws to explicitly address digital cloning. A prominent example is the state of Tennessee, which enacted the Ensuring Likeness, Voice, and Image Security (ELVIS) Act in July 2024. The ELVIS Act explicitly adds a person's voice, whether actual or simulated, to the list of property rights protected under Tennessee's publicity rights framework,[69] ensuring that the unauthorized impersonation of someone's voice through AI for commercial purposes provides a clear statutory cause of action.

Simultaneously, recognizing the limitations of a fragmented state-by-state system, lawmakers in the U.S. Congress proposed the No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act[70] (No FAKES Act). This proposed federal legislation aims to establish a uniform, national property right in one's voice and likeness, making it unlawful to produce or distribute AI-generated replicas of real persons without their explicit consent. However, it remains to be seen how this approach tackles inherent doctrinal friction with the First Amendment given the existence of strong free speech protections, that may hold AI-generated likenesses for satire, parodies or non-commercial uses as constitutionally protected, limiting the ability of individuals to control non-commercial deepfakes.

European Union (The Data Protection and Transparency Approach)

In contrast to the United States, the European Union does not recognize a unified "right of publicity" or an economic property right over one's persona.[71] Instead, the EU addresses the threat of generative AI and deepfakes through a robust, rights-based framework grounded in fundamental privacy, data protection, and consumer safety regulations. The cornerstone of this approach is the General Data Protection Regulation (GDPR), which strictly treats facial images and voice recordings as personal data.[72] When this data is processed to uniquely identify a natural person, it is elevated to the status of highly sensitive biometric data.[73]

---

[68] Chopra, Sony AL & Chopra, *supra* note 1 at 41.
[69] Chopra, Sony AL & Chopra, *supra* note 1 at 44.
[70] *No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act of 2024*, HR 6943, 118th Cong (2024) [No AI FRAUD Act].
[71] Chopra, Sony AL & Chopra, *supra* note 1 at 32.
[72] Ibid.
[73] Mais Qandeel, "Facial recognition technology: regulations, rights and the rule of law" (2024) 7 Frontiers in Big Data 1 at 3.

Under the GDPR, using someone's voice recording or facial image to train an AI model or generate a deepfake requires a clear, lawful basis, such as explicit, informed consent from the data subject. Implied consent or the mere fact that an image is publicly available on the internet does not exempt AI developers from these strict privacy requirements. If an AI firm clones a European citizen's face or voice without this lawful basis, it faces severe regulatory fines and civil claims for unlawful processing. Furthermore, the GDPR grants powerful remedies to individuals, such as the 'right to be forgotten' i.e. 'right to erasure',[74] allowing victims to demand the immediate deletion of unauthorized biometric templates or deepfake pornography from the platforms hosting them.

The EU has further fortified its defenses against biometric cloning by finalizing the sweeping Artificial Intelligence Act (AI Act). Rather than outright banning all deepfakes, the EU AI Act mandates stringent transparency and disclosure obligations to prevent societal deception and fraud.[75] Article 50 of the AI Act specifically targets AI-generated content that impersonates real people, requiring that any AI system capable of generating deepfake audio, images, or video must clearly disclose that the outputs are synthetically created.[76] AI providers and deployers must embed automated watermarks, metadata tags, or clear visual notices indicating that the content is machine-generated, thereby ensuring that viewers can instantly identify a deepfake.

Complementing the GDPR and the AI Act is the Digital Services Act (DSA),[77] which shifts the burden of enforcement onto online intermediaries. The DSA mandates that host platforms exercise increased diligence and implement mechanisms to swiftly remove or disable access to illegal content upon receiving a substantiated notification.[78] This compliance-based approach ensures that if illegal deepfake content, such as non-consensual deepfake pornography or AI impersonation scams, is flagged, the platforms themselves are legally obligated to take it down rapidly or face significant penalties.

China (The Strict Personality Rights Approach)

China has proactively established one of the most stringent and targeted regulatory frameworks in the world to govern generative AI and mitigate the risks of synthetic media. The Chinese approach relies heavily on state-mandated algorithmic transparency and the strict enforcement of personality rights through dedicated administrative provisions.

China has implemented the Provisions on the Administration of Deep Synthesis Internet Information Services.[79] These provisions place comprehensive obligations on service providers,

---

[74] Gabriele Hooffacker, *Online journalism* (Wiesbaden: Springer Fachmedien, 2022) at 160; EU, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1, art. 17.
[75] Chopra, Sony AL & Chopra, *supra* note 1 at 32-33.
[76] Chopra, Sony AL & Chopra, *supra* note 1 at 42.
[77] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, [2022] OJ, L 277/1 [DSA].
[78] Chopra, Sony AL & Chopra, *supra* note 1 at 43.
[79] *Hulianwang Xinxi Fuwu Shendu Hecheng Guanli Guiding* [Provisions on the Administration of Deep Synthesis Internet Information Services], Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security, 25 November 2022 (entered into force 10 January 2023) [Deep

technical supporters, and users involved in creating deepfakes. A critical component of this regulation is the explicit protection of biometric data. Under Article 14 of the Deep Synthesis Regulation, any deep synthesis service provider or technical supporter that edits biometric information, specifically including faces and voices, must directly notify the targeted individuals and obtain their separate, explicit consent before generating the synthetic output.[80] This mandates a highly protective, proactive barrier against the unauthorized digital cloning of any individual's physical characteristics. Additionally, the regulation requires that deep synthetic content that could confuse or mislead the public, such as voice simulations or face manipulations, be explicitly labeled in a reasonable and visible manner.[81]

Furthermore, China expanded its regulatory oversight by promulgating the Interim Measures for the Management of Generative Artificial Intelligence Services.[82] Article 7 of the Generative AI Regulation imposes highly onerous obligations on AI providers regarding the sourcing of their training data. AI developers must ensure that the data and basic models originate from lawful sources and do not infringe upon the intellectual property rights of third parties. Critically, if the training data involves personal information, developers are legally required to obtain the data subject's explicit consent[83] or satisfy other strict legal conditions. These proactive data management rules place the burden of proof heavily on AI developers to maintain ethical, non-infringing data pipelines, actively preventing the mass, unconsented scraping of human voices and faces from the internet for algorithmic training.

Denmark (The Copyright Approach)

Denmark is currently pioneering a groundbreaking legislative model that completely reimagines how the law can protect digital identity from generative AI.[84] The Danish government has proposed a groundbreaking amendment to the Danish Copyright Act, by proposing Section 73a, that explicitly recognizes an individual's physical characteristics, including their face, voice, and bodily gestures, as intellectual property protected under copyright law.[85]

This approach marks a radical conceptual shift.[86] Traditionally, copyright law protects original creative expressions of the human intellect, while physical traits are considered biological facts relegated to privacy or personality rights.[87] However, the Danish proposal treats a person's core

---

Synthesis Provisions]; Hui Xu et al, "China's New AI Regulations" (16 August 2023), Latham & Watkins Privacy & Cyber Practice Number 3110 at 1.

[80] Xu et al, *supra* note 23 at 4.

[81] Xu et al, *supra* note 23 at 6.

[82] *Shengchengshi Rengong Zhineng Fuwu Guanli Zanxing Banfa* [Interim Measures for the Management of Generative Artificial Intelligence Services], Cyberspace Administration of China et al, 10 July 2023 (entered into force 15 August 2023) [Generative AI Measures].

[83] Xu et al, *supra* note 23 at 3.

[84] Sofia Karttunen, "The Danish approach to copyright and deepfakes: A model for the EU?" (2026) European Parliamentary Research Service PE 782.611 at 1.

[85] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 3.

[86] Endang Prihatin, "Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum" (2025) 10th International Conference on Sustainability 87 at 90.

[87] Melian Pérez & Herrerías Castro, *supra* note 2 at 4.

physical identity as a copyrightable object to combat the specific mechanics of deepfake technology.[88] Under Section 73a, any individual, regardless of whether they are a famous celebrity or an ordinary citizen, can seek intellectual property protection against the unauthorized public sharing of realistic, digitally generated imitations of their physical traits.[89] The law strictly prohibits the publication of such realistic deepfakes without the individual's express consent, empowering victims with a specific legal claim and remedy to force the immediate takedown of unauthorized digital imitations from online platforms.[90]

In order to balance this new right with freedom of expression, the Danish proposal includes specific exceptions: deepfakes created for imitation, caricature, satire, parody or social commentary are allowed, provided they do not constitute defamation, spread misleading disinformation or cause serious harm to the depicted individual.[91]

A uniquely powerful enforcement mechanism embedded within this proposed copyright approach is the establishment of a robust post-mortem right. The amendment guarantees that the protection of an individual's digital identity continues for 50 years after their death.[92] This post-mortem right grants the deceased's heirs the affirmative legal authority to control the digital use of the individual's voice and image posthumously, filling a critical gap that exists in several privacy-based frameworks where rights usually lapse upon death.[93] Furthermore, the burden of proof under this framework is reversed; the party distributing the digital content must actively demonstrate that they obtained valid consent from the depicted individual, significantly strengthening the legal position of deepfake victims. Ultimately, Denmark's copyright approach effectively merges personal dignity with intellectual property enforcement, offering a proactive and highly enforceable legal shield against biometric cloning.[94]

Part V: Feasibility, Pros And Cons Of Canadian Copyright Law For Likeness

As demonstrated by the legal vacuum currently existing in Canada, victims of unauthorized biometric cloning lack a proactive, proprietary mechanism to protect their facial and vocal identities. One of the most provocative and viable proposals could be the expansion of the Canadian Copyright Act to explicitly cover physical characteristics. This model is directly inspired by Denmark's groundbreaking legislative proposal, which seeks to amend its national copyright rules to grant individuals explicit intellectual property protection against the unauthorized sharing of realistic, digitally generated imitations of their faces, voices, and bodies.[95] While treating likeness as a copyrightable object offers powerful, ready-made

[88] Prihatin, *supra* note 3 at 90.
[89] Melian Pérez & Herrerías Castro, *supra* note 2 at 3.
[90] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 33.
[91] Prihatin, *supra* note 3 at 90.
[92] Karttunen, *supra* note 1 at 1.
[93] Prihatin, *supra* note 3 at 90.
[94] Prihatin, *supra* note 3 at 91.
[95] Sofia Karttunen, "The Danish approach to copyright and deepfakes: A model for the EU?" (2026) European Parliamentary Research Service PE 782.611 at 1.

enforcement mechanisms, it also introduces profound doctrinal friction, risking the hyper-commodification of human dignity and threatening severe chilling effects on freedom of expression.

The primary appeal and feasibility of the Copyright approach lie in its ability to take advantage of existing, robust legal architectures both internationally and domestically. Copyright law is already an established, highly operationalized framework with well-defined enforcement mechanisms, statutory damages, and international recognition through treaties such as the Berne Convention.[96] By categorizing facial and vocal likenesses as copyrightable objects, Canada could theoretically bypass the need to construct an entirely new, untested sui generis personality rights regime from the ground up.

Under a framework modeled after the proposed Danish Copyright Act amendment (Section 73a), individuals would be granted a specific, actionable intellectual property right to demand the immediate removal of AI-generated imitations posted without their explicit consent.[97] A major advantage of this approach is its seamless integration with modern intermediary liability frameworks. For instance, in the European context, Denmark's proposed copyright amendments are designed to be enforced through the EU Digital Services Act (DSA).[98] The DSA mandates that host platforms swiftly disable or remove access to illegal, copyright-infringing content upon receiving a substantiated notification, effectively shifting the burden of enforcement onto online intermediaries.[99]

If Canada were to adopt this copyright approach, it could similarly empower victims of deepfake pornography and vocal cloning to issue rapid takedown notices under equivalent domestic notice-and-takedown regimes. This would provide a vital, immediate remedy for victims who currently struggle to remove viral deepfakes from the internet. Furthermore, the copyright model dramatically alters the burden of proof. Under the Danish proposal, the party distributing the digital content must actively demonstrate that they obtained valid consent from the depicted individual.[100] For a Canadian plaintiff, this would remove the onerous common law requirement of proving 'unjust enrichment' or 'commercial gain' required by the conventional tort of misappropriation of personality, offering a strict liability standard against unauthorized biometric replication. Finally, embedding likeness within copyright law provides clear parameters for post-mortem rights, guaranteeing that the protection of a digital identity continues for a set statutory period, such as Denmark's proposed timeline of 50 years, after the individual's death, granting heirs the legal authority to supervise posthumous deepfakes.[101]

---

[96] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 5.
[97] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 33.
[98] Karttunen, *supra* note 1 at 1.
[99] Chopra, Sony AL & Chopra, *supra* note 3 at 45.
[100] Endang Prihatin, "Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum" (2025) 10th International Conference on Sustainability 87 at 90.
[101] Karttunen, *supra* note 1 at 1.

Despite its pragmatic enforcement advantages, expanding Canadian copyright law to protect human faces and voices introduces severe conceptual and doctrinal flaws.[102] It can be argued that the historical and philosophical purpose of copyright law is rooted in utilitarian theory whereby it is designed to provide economic incentives to encourage human creativity and the production of new cultural works.[103] Conversely, personality rights, such as the right to one's image and voice, are grounded in the principle of human dignity and exist to safeguard the individual's innermost, existential sphere.[104]

This level of disconnect exposes a structural incompatibility between the subject matter of copyright and the reality of biological traits. The Berne Convention and Canadian copyright law dictate that protection is reserved for "original expressions of human intellect".[105] Originality intrinsically requires a degree of conscious choice, intellectual effort, and creative freedom. A person's face, vocal geometry, or physical gait are inherent qualities of nature and human biology; they are not the result of free, intellectual skill and judgement or an 'authored' expression and attempting to protect a person's intrinsic physical identity under a regime designed for intellectual creations could distort the fundamental object of copyright and neglect its core principles focusing on the act of human creation.

Moreover, treating likeness as copyrightable property threatens to produce severe chilling effects on freedom of expression.[106] In a democratic society, the right to free expression must and should be regularly balanced against the rights of the individual.[107] However, the exceptions and limitations within copyright law differ drastically from the balancing tests utilized in civil privacy or constitutional frameworks.

In intellectual property law, exceptions to the creator's monopoly, such as fair dealing in Canada, are generally strict and must comply with international standards like the Berne Convention's 'three-step test'.[108] This test demands that any limitation must apply only in certain special cases, must not conflict with the normal exploitation of the work, and must not unreasonably prejudice the legitimate interests of the author. In contrast, restrictions on personality rights and image rights are traditionally evaluated through a flexible constitutional balancing test, weighing the right to privacy against freedom of expression and the public's right to information. This balancing considers factors such as the public interest of the debate, the prominence of the public figure, and the form and consequences of the publication.[109]

There is a dangerous slippery slope involved where if Canada were to strictly apply copyright law to human faces and voices, it could result in extreme corporate overreach. Politicians, celebrities, and their respective estates or representative managing agencies could wield

[102] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 3.
[103] Melian Pérez & Herrerías Castro, *supra* note 1 at 5-6.
[104] Melian Pérez & Herrerías Castro, *supra* note 1 at 6.
[105] Melian Pérez & Herrerías Castro, *supra* note 1 at 4.
[106] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 31.
[107] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 5.
[108] Melian Pérez & Herrerías Castro, *supra* note 2 at 4-5.
[109] Melian Pérez & Herrerías Castro, *supra* note 2 at 5.

copyright infringement claims as a weapon to suppress critical or unflattering digital media.[110] While the Danish proposal attempts to carve out specific exceptions for deepfakes created for social commentary, caricature, parody, imitation and/or satire,[111] detractors rightly note that imposing a property-like monopoly over human likeness inherently jeopardizes legitimate free speech. Overly broad property rights in a person's digital identity could heavily curtail investigative journalism, documentary-style filmmaking and political satire, all of which rely on the ability to freely reference and depict real individuals without navigating the rigid, permission-based hurdles of copyright clearance.[112]

It is important to remember that while the copyright approach offers a tantalizingly swift mechanism to force the removal of deepfakes via established digital takedown legal regimes,[113] it relies on a flawed legal fiction. Forcing biological reality into an intellectual property framework designed for economic incentivization may risk ignoring the dignity-based harms inflicted by GenAI biometric cloning and may risk sacrificing vital Charter based protections[114] in favour of highly commercialized identity rights.[115]

Part VI: Policy Recommendations

Canada currently suffers from a significant regulatory vacuum; the common law tort of misappropriation of personality relies on an archaic 'commercial gain' threshold,[116] and the Canadian Copyright Act does not currently classify biological facts like facial geometry or vocal signatures as original works of authorship.[117] To protect Canadians from the devastating impacts of deepfake pornography, financial fraud, and disinformation, this paper outlines a comprehensive, forward-looking legislative roadmap based on the principle of ius constituendum i.e. the ideal law to be established in the future.[118]

When evaluating the most viable legislative pathway for Canada to protect biometric identity, lawmakers must choose between creating a fragmented, province-by-province right of publicity (as seen in the United States, such as Tennessee's ELVIS Act) or adapting existing federal intellectual property regimes.[119] Based on a comparative legal analysis, this paper strongly

---

[110] Chopra, Sony AL & Chopra, *supra* note 1 at 31.
[111] Endang Prihatin, "Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum" (2025) 10th International Conference on Sustainability 87 at 90.
[112] Chopra, Sony AL & Chopra, *supra* note 1 at 31.
[113] Sofia Karttunen, "The Danish approach to copyright and deepfakes: A model for the EU?" (2026) European Parliamentary Research Service PE 782.611 at 1.
[114] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [Charter].
[115] Melian Pérez & Herrerías Castro, *supra* note 2 at 6-7.
[116] David Collins, "Age of the Living Dead: Personality Rights of Deceased Celebrities" (2001) 39:4 Alta L Rev 914 at 922.
[117] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 28.
[118] Endang Prihatin, "Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum" (2025) 10th International Conference on Sustainability 87 at 88.
[119] Chopra, Sony AL & Chopra, *supra* note 2 at 30-31.

recommends that Canada adopt the groundbreaking approach currently being pioneered by Denmark: a radical expansion of copyright law to explicitly protect human likeness.[120]

Under this proposal, any individual can seek copyright protection against the unauthorized public sharing of realistic, digitally generated imitations of their physical characteristics.[121] While critics can rightfully argue that this approach suffers from a teleological mismatch, asserting that copyright is meant to incentivize human intellectual creation rather than protect innate biological traits,[122] the Danish model correctly recognizes that in the GenAI era, human identity is systematically digitized, remixed, and exploited precisely like traditional creative works.[123]

In the age where GenAI is rapidly advancing on an almost daily basis, taking inspiration from the Denmark model still remains the most robust and immediate pathway for Canada because it leverages pre-existing, highly operationalized intellectual property enforcement mechanisms.[124] By classifying unauthorized deepfakes as copyright infringement, victims bypass the onerous burden of proving 'commercial gain' required by the Canadian misappropriation of personality tort.[125] The copyright approach effectively reverses the burden of proof, legally requiring the party distributing the digital content to actively demonstrate that they obtained valid, explicit consent from the depicted individual.[126] Furthermore, following the Danish blueprint, Canada should implement a 50-year post-mortem right for digital likeness.[127] This guarantees that the protection of a digital identity continues for half a century after an individual's death, granting their heirs the affirmative legal authority to control posthumous exploitation and protect the dignity of the deceased.[128]

However, the copyright approach is only one leg that a new Canadian legal approach will have to stand on. It must also proactively cut off the supply chain of unauthorized synthetic media, for which it must enact stringent legal mechanisms governing how AI training data is collected.[129] Currently, foundational AI models rely on untargeted web scraping, indiscriminately harvesting billions of vocal samples and personal images under the flawed assumption that public availability equates to ethical or legal authorization.[130] Canadian policy should align with the demands of the creative and the public workforce by integrating a version of the PRAC³ framework, Privacy, Reputation, Accountability, Consent, Credit, and Compensation, into federal privacy and data protection mandates. This framework highlights how the non-consensual training of AI models amplifies privacy risks and strips individuals of control over their biometric identifiers and creative labor.[131] Consequently, Canada must reform the Personal Information

[120] Sofia Karttunen, "The Danish approach to copyright and deepfakes: A model for the EU?" (2026) European Parliamentary Research Service PE 782.611 at 1.
[121] Melian Pérez & Herrerías Castro, *supra* note 6 at 3.
[122] Melian Pérez & Herrerías Castro, *supra* note 6 at 5-6.
[123] Prihatin, *supra* note 3 at 89.
[124] Karttunen, *supra* note 5 at 1.
[125] Collins, *supra* note 1 at 924.
[126] Prihatin, *supra* note 3 at 90.
[127] Melian Pérez & Herrerías Castro, *supra* note 6 at 4.
[128] Prihatin, *supra* note 3 at 90.
[129] Bao Kham Chau & George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity" (2024) at 4.
[130] Tanusree Sharma, Yihao Zhou & Visar Berisha, "PRAC3 (Privacy, Reputation, Accountability, Consent, Credit, Compensation): Long Tailed Risks of Voice Actors in AI Data-Economy" (2025) at 2.
[131] Sharma, Zhou & Berisha, *supra* note 2 at 1.

Protection and Electronic Documents Act (PIPEDA) to explicitly prohibit the untargeted scraping of facial and vocal data for commercial AI training or surveillance purposes.[132]

Crucially, the law must ban the use of "implied consent" for biometric data processing.[133] Given how biometric identifiers like voiceprints and facial geometry are immutable and uniquely sensitive,[134] AI developers must be legally mandated to use a code-based architectural 'privacy-by-design' model to secure granular, explicit, and actively affirmed 'opt-in' consent directly from the data subjects before their likeness can be ingested into any training dataset. Furthermore, Canada should provide citizens with an absolute right to erasure, allowing them to withdraw their consent at any time and demand the permanent deletion of their biometric templates from AI algorithms.[135]

A major flaw in current international frameworks, including the EU AI Act and various American legislative proposals, is their disproportionate focus on penalizing the end-users who generate illicit deepfakes, while virtually ignoring the structural mechanics of the GenAI supply chain.[136] The hardware, compute power, and underlying foundation models required to process data and generate hyper-realistic synthetic media are exclusively owned by a highly concentrated handful of massive tech companies, such as OpenAI, Microsoft, and Google. These entities lease access to their models to downstream users via Application Programming Interfaces (APIs), operating under a Software as a Service (SaaS) framework.[137]

Canada must recognize these entities as the "landlords of creativity" and place them at the center of the liability analysis. Given that these landlords own the critical infrastructure and have the technical capacity to implement systemic guardrails, they can be viewed as the 'cheapest cost avoiders'.[138] Canadian law should impose a default liability regime holding these infrastructure providers responsible for illicit synthetic media generated using their platforms.[139] These landlords of creativity must be legally required to strictly limit the generation capacities provided to unidentified or unregistered customers, restricting anonymous users to heavily "red-teamed" functionalities to prevent malicious mass-generation.[140] These landlords must also maintain a persistent, secure audit trail for registered users, logging the exact prompts and user inputs that lead to specific generated outputs. By linking generative outputs to user attribution, authorities can definitively trace malicious deepfakes back to the offending tenant, bridging the accountability gap while absolving the compliant landlord of direct liability.[141]

Canadian NGOs and policy think-tanks need to lead the charge by arguing that Canada is perfectly positioned to pioneer a world-leading 'hybrid model' that synergizes the strongest elements of the European Union's transparency approach with the aggressive enforcement

[132] Lambert Hogenhout & Rinzin Wangmo, "Protecting Persona Biometric Data: The Case of Facial Privacy" (2025) at 12.
[133] Hogenhout & Wangmo, *supra* note 5 at 11.
[134] Hogenhout & Wangmo, *supra* note 5 at 4.
[135] Hogenhout & Wangmo, *supra* note 5 at 11.
[136] Bao Kham Chau & George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity" (2024) at 6.
[137] Chau & He, *supra* note 1 at 2.
[138] Chau & He, *supra* note 1 at 3.
[139] Chau & He, *supra* note 1 at 24.
[140] Chau & He, *supra* note 1 at 21.
[141] Chau & He, *supra* note 1 at 23.

teeth of the Danish copyright model.[142] There should be a push for the adoption of the rigorous transparency requirements found in Article 52 of the EU AI Act.[143] This would legally mandate that all AI systems capable of generating deepfake video or audio insert standardized technological measures, such as content origin metadata, open-source digital watermarking and clear visual disclosures.[144] Canadian NGOs and policy think-tanks can argue that this EU-style transparency is vital for consumer protection, ensuring that artificially synthesized financial fraud and political disinformation are instantly recognizable to the Canadian public.[145] They must forcefully argue that transparency alone is insufficient for victims of reputational harassment or deepfake pornography, who require immediate content removal.[146] Therefore, they should demand the Canada-specific recreation of the proposed Danish Section 73a, granting individuals copyright ownership over their digital likeness,[147] combined with the intermediary liability mechanisms of the EU's Digital Services Act (DSA).[148] Under this hybrid framework, once a Canadian victim issues a copyright takedown notice for an unauthorized deepfake, the online host platforms and Internet Service Providers are legally compelled by Canada-specific DSA-style rules to expeditiously remove the illegal content or face severe statutory damages.[149]

To pre-empt criticisms regarding freedom of expression, Canadian NGOs and policy think-tanks can emphasize that this hybrid model carefully balances human dignity with Canadian Charter-protected rights.[150] By incorporating specific, clearly defined exceptions for imitation, caricature, parody, social commentary and satire; provided they do not constitute defamation or misleading disinformation, this framework ensures that artistic and political speech remains protected.[151] Ultimately, by lobbying for this synthesized EU-Danish approach alongside strict liability for AI landlords and mandatory opt-in consent for data scraping,[152] Canadian NGOs and policy think-tanks can help Canada construct an impenetrable legal future to protect the faces and voices of its citizens in the GenAI era.

Part VII: Conclusion & Way Forward

As GenAI as a technology proliferates at an unprecedented scale and with negligible marginal cost, society is no longer merely facing a unique threat of isolated 'deepfakes';[153] it is

---

[142] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 43.
[143] Chopra, Sony AL & Chopra, *supra* note 2 at 42.
[144] Anja Neubauer, Martin Wynn & Robin Bown, "AI, Authorship, Copyright, and Human Originality" (2026) 6 Encyclopedia 1 at 13.
[145] Chopra, Sony AL & Chopra, *supra* note 2 at 42.
[146] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, "Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes" (2026) 44 IDP Rev Internet Derecho y Política 1 at 10.
[147] Melian Pérez & Herrerías Castro, *supra* note 6 at 3.
[148] Sofia Karttunen, "The Danish approach to copyright and deepfakes: A model for the EU?" (2026) European Parliamentary Research Service PE 782.611 at 1.
[149] Karttunen, *supra* note 8 at 1.
[150] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [Charter]; Melian Pérez & Herrerías Castro, *supra* note 6 at 8.
[151] Prihatin, *supra* note 1 at 90.
[152] Lambert Hogenhout & Rinzin Wangmo, "Protecting Persona Biometric Data: The Case of Facial Privacy" (2025) at 12.
[153] Ferrara, *supra* note 1 at 1.

confronting the emergence of ‘synthetic realities’ where identity, social interaction as well as media content are entirely manufactured and mutually reinforcing. In this new technological eon, the unregulated cloning of biometric identifiers poses an existential threat to both epistemic security and personal dignity.[154]

This paper has demonstrated that the current Canadian legal framework is critically failing to protect citizens from the unauthorized exploitation of their biometric identities.[155] Canadians are presently trapped in a regulatory vacuum, forced to rely on obsolete legal tools that were never designed for the GenAI era. The common law tort of misappropriation of personality is fundamentally inadequate because it strictly requires victims to prove that the perpetrator achieved ‘unjust enrichment’ or a ‘commercial gain.’[156] This high threshold renders the tort practically useless against the most insidious forms of digital exploitation, such as non-consensual deepfake pornography, political disinformation, and systemic algorithmic training, none of which easily satisfy the requirement of demonstrating a direct, provable financial transaction.

Furthermore, the Canadian Copyright Act offers no sanctuary for victims of biometric cloning.[157] Rooted in the utilitarian requirement of human authorship, traditional copyright law exclusively protects original expressions of the human intellect, not innate biological facts such as facial geometry or vocal signatures.[158] When AI developers indiscriminately scrape publicly available images and audio to train their models, copyright law protects the original creator of the media (such as the photographer), leaving the actual human subject completely disenfranchised.[159] Coupled with a stalled federal AI regulatory agenda and privacy laws (like PIPEDA) that only provide reactive shields against data misuse rather than affirmative ownership rights, Canadians currently possess no proprietary control over their own digital likenesses.[160]

To bridge this hazardous gap, Canada must adopt a proactive, rights-based legislative roadmap grounded in the principle of ius constituendum, the ideal law to be established in the future.[161] As established through the comparative jurisdictional analysis, the most robust and immediate pathway for Canada is to pioneer a hybrid regulatory model that synergizes the aggressive enforcement mechanisms of Denmark’s proposed copyright expansion[162] with the stringent

---

[154] Ferrara, *supra* note 1 at 13.
[155] Vasileia Karasavva & Aalia Noorbhai, “The Real Threat of Deepfake Pornography: A Review of Canadian Policy” (2021) 24:3 Cyberpsychology, Behavior, and Social Networking 203 at 204.
[156] David Collins, “Age of the Living Dead: Personality Rights of Deceased Celebrities” (2001) 39:4 Alta L Rev 914 at 922.
[157] Karasavva & Noorbhai, *supra* note 5 at 206.
[158] Gabriel Ernesto Melian Pérez & Laura Herrerías Castro, “Copyright or personality rights? A critical analysis of Denmark’s approach to deepfakes” (2026) 44 IDP Rev Internet Derecho y Política 1 at 4.
[159] Collins, *supra* note 7 at 923.
[160] Lambert Hogenhout & Rinzin Wangmo, “Protecting Persona Biometric Data: The Case of Facial Privacy” (2025) at 6-7.
[161] Endang Prihatin, “Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum” (2025) 10th International Conference on Sustainability 87 at 88.
[162] Sofia Karttunen, “The Danish approach to copyright and deepfakes: A model for the EU?” (2026) European Parliamentary Research Service PE 782.611 at 1.

transparency mandates of the European Union.[163] By amending the Copyright Act to explicitly recognize an individual's face and voice as protected intellectual property, Canada can empower its citizens with an absolute legal right to demand the swift removal of unauthorized digital imitations from online platforms.[164]

Crucially, this modernized framework must address the root of the problem by regulating the entire generative AI supply chain.[165] Canada must abandon the flawed premise of 'implied consent' for publicly available data and mandate explicit, granular opt-in consent for any biometric data scraped for AI training.[166] Furthermore, liability must be shifted away from exclusively targeting anonymous end-users and firmly placed onto the "landlords of creativity", the highly concentrated foundational infrastructure providers who supply the computational power and models that make deepfakes possible.[167] By legally obligating these entities to maintain secure audit trails and restrict the generation capacities of unverified users, Canada can proactively cut off the proliferation of illicit artificially generated media at its source.[168]

We stand at a critical juncture in the digital age where GenAI has created an environment that allows a person's voice or face to be treated as a cheap and abundant asset, severely corroding the routine verification workflows upon which modern society relies.[169] This is not merely an issue of intellectual property; it is a profound societal crisis. The unrestricted multiplication of synthetic media actively erodes shared epistemic ground, paving the way for a devastating GenAI Paradox where society rationally discounts all digital evidence, effectively raising the cost of truth for everyday life and democratic institutions.[170]

The Canadian government can no longer afford to take a reactive, wait-and-see approach.[171] There is an absolute urgency to establish modern, statutory protections for human likeness before artificially generated media fully destabilizes individual autonomy and public trust. Lawmakers must act decisively to implement copyright protections for biometric identity, mandate ethical AI training practices, and hold digital landlords accountable. Failure to do so will result in the irreversible commodification of the individual self, leaving citizens defenseless in a synthetic reality where their unique voices and faces are no longer owned by them.[172]

---

[163] Pooja Chopra, Reeta Sony AL & Shruti Chopra, "Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective" (2025) 6:3 Legal Issues Digit Age 23 at 42.
[164] Karttunen, *supra* note 14 at 1.
[165] Bao Kham Chau & George He, "Audio Deepfakes and the Regulation of the Landlords of Creativity" (2024) at 6.
[166] Lambert Hogenhout & Rinzin Wangmo, "Protecting Persona Biometric Data: The Case of Facial Privacy" (2025) at 11.
[167] Chau & He, *supra* note 1 at 2-3.
[168] Chau & He, *supra* note 1 at 21-23.
[169] Emilio Ferrara, "The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth" (2025 at 4 & 13.
[170] Ferrara, *supra* note 6 at 13.
[171] Endang Prihatin, "Legal Protection of Face and Voice as Copyrightable Objects in the Era of Deepfake Technology: A Comparative Analysis between Denmark and Indonesia from the Perspective of Ius Constituendum" (2025) 10th International Conference on Sustainability 87 at 93-94.
[172] Hogenhout & Wangmo, *supra* note 2 at 14.