
# WHAT CAN AND SHOULD THE LAW DO ABOUT 'DEEPFAKE': AN UPDATE

*Posted on December 5, 2018*

**Categories:** Insights, Publications

Introduction

In March 2018, we published an article titled "What Can the Law Do About 'Deepfake'?", discussing the proliferation of deepfake videos and several causes of action that may be taken against those who create and propagate deepfake material on the internet. Some of these causes of action included those related to copyright infringement, defamation, violation of privacy, and appropriation of personality. We since spoke before a Standing Committee of Parliament about this topic on October 16, 2018, particularly in light of attacks against democratic institutions and societies through "fake news".

This update, largely a summary of our opening comments to the Standing Committee, looks at several additional causes of action and discusses how we (holistically, not just the courts or the government, but as individuals) can limit the deleterious social consequences of deepfake videos. While, certainly, deepfake videos can play a role in social manipulation, it is ultimately better information and better education that will strengthen societal resistance to improper influence through technologies like deepfakes.

**Legal Recourse: Additional Causes of Action**

In addition to the causes of action previously discussed, there are several torts that are not, at least yet, recognized in Canada, that may be used against the creators of deepfakes. Accordingly, there is room for our courts to expand common law torts and for governments to codify new ones—in fact, it is our view that governments have and should use their ability to create law addressing threats posed by ever-evolving technology. These additional causes of action may also be used to combat deepfake videos in the election context. Below is a summary of some of such causes of action:

***Canada Elections Act***

In 2014, Parliament introduced a provision into the *Canada Elections Act,* SC 2000, c 9 directed at the impersonation of certain kinds of people involved in the election process. Under section 480.1, every person is guilty of an offence who, with intent to mislead, falsely represents themselves to be, or causes anyone to falsely

represent themselves to be:

1. the Chief Electoral Officer, a member of the Chief Electoral Officer's staff or a person who is authorized to act on the Chief Electoral Officer's behalf;
2. an election officer or a person who is authorized to act on an election officer's behalf;
3. a person who is authorized to act on behalf of the Office of the Chief Electoral Officer;
4. a person who is authorized to act on behalf of a registered party or a registered association; or
5. a candidate or a person who is authorized to act on a candidate's behalf.[1]

Deepfake videos could very well fall within the scope of this section if the subject of the video is within a class of persons enumerated above; however, this provision is not specifically targeted at addressing such problems (such as the use of deepfakes, social media bots or computer-generated audio to create false media of not only these persons, but also influencers, newscasters, and the like), and could be modified to do so.

*Norwich Order*

A Norwich Order may be obtained to compel a social media platform to assist with the investigation of a crime committed on the platform. For example, the platform may be compelled by a court to reveal the identities of anonymous users utilizing the services of that platform. A Norwich Order is granted when:

1. there is a valid, bona fide or reasonable claim;
2. there is a relationship between the applicant for the order and the third party from whom the information is sought, such that the third party is somehow involved in the acts complained of;
3. the third party is the only practicable source of the information available;
4. the third party can be indemnified for costs to which the third party may be exposed because of the disclosure; and
5. the interests of justice favour obtaining the disclosure.[2]

Accordingly, legal mechanisms already exist to compel social media platforms to reveal the identities of anonymous users. Generally, law-abiding third parties subject to such orders comply with the terms thereof. In the context of anonymous deepfake videos that are published on a social media platform, it is reasonable to expect that the social media platform would respond positively to a Norwich Order and provide the required information that is relevant to the investigation.

*Public Disclosure of Private Facts*

The Ontario Superior Court of Justice recently recognized as actionable the tort of public disclosure of private facts.[3] This tort may be established when:

1. the defendant publicized an aspect of the plaintiff's private life;
2. the plaintiff did not consent to the publication;
3. the matter publicized or its publication would be highly offensive to a reasonable person; and
4. the publication was not of legitimate concern to the public.

While this tort has not yet been recognized in other provinces, Ontario has set a clear example of how to address instances of revenge porn or unauthorized disclosure of private images. The adoption of this tort is a step in the right direction in placing restrictions on the ability of individuals to share intimate details of another person's life without their consent and demonstrates the court's willingness to combat these issues. This tort could likely be used against the creators or proliferators of deepfakes so long as the four criteria are established on the facts.

*Unjust Enrichment*

There is room for Canadian courts to expand the tort of unjust enrichment and to recognize the tort of false light (discussed in the next section). Either of these torts might then be useful causes of action against the creators and proliferators of deepfakes.

In Canada, to successfully claim unjust enrichment, a claimant must prove the following:

1. the person received a benefit;
2. the claimant suffered a loss corresponding in some way to the benefit; and
3. there was no juristic reason for the benefit and the loss.[4]

The tort of unjust enrichment has generally been upheld in cases involving an economic loss suffered by the claimant. However, it is reasonable to argue that the concept of "losses" should be expanded to cover other forms of "losses" that may not be quantifiable in dollars and cents. If the concept of "loss" as it pertains to unjust enrichment claims is expanded, this tort might become a viable option in combatting the proliferation of deepfakes.

*Tort of False Light*

The tort of false light currently exists in some states in the U.S. The tort of false light is similar to defamation. It allows the victim of a non-consensual publication of his or her private or intimate images to bring a suit for invasion of privacy, particularly false light in the public eye, against the person who published the images. In order for this cause of action to succeed, a plaintiff must establish:

1. the false light in which the plaintiff was placed would be highly offensive to a reasonable person; and
2. the actor had knowledge of or acted in reckless disregard as to the falsity of the disseminated

information and the false light in which the other would be placed.[5]

Canadian courts have not yet recognized this tort. The province of Manitoba has expressed its view that such a tort does not exist in Manitoban common law.[6] In Ontario, it has been recognized that there may come a time where the court is presented with a case that makes it appropriate to consider further evolving the common law to recognize as actionable publicity which places the plaintiff in a false light in the public eye.[7] Canadian courts may begin to rethink their position on the tort of false light as a result of the proliferation of deepfakes in the past year. Even if this tort does not become recognized under Canadian common law, it is within the power of a provincial government to enact it into statutory code, thereby creating its existence via statutory form.

**Holistic Recourse: What to Do About Deepfakes, and a Caution about Legislative Remedies**

While civil remedies are available, pursuing one of them in the courts, particularly in the international context of the Internet, might often be too-heavy a burden to place on the victim of a deepfake video.[8] The court process is often laborious and slow and is unlikely to result in any meaningful result or justice before the damage has long been done. So what can be done?

It is important to remember that deepfakes and computer simulation will be yet another, but hardly the only, tool that can be used to create convincingly fake videos. The motivations for these range from pure salaciousness, to parody, to commercial gain, to even blackmail or political manipulation. While “deepfakes” are technologically novel, they do not necessarily present a unique problem in the world of fraud, crime, parody, commercial use or election interference, but instead are just another topical issue that needs to be addressed.

While deepfake videos and other AI-assisted technologies hold immense promise for visual effects companies, video game makers, technology manufacturers and comedians, it is inevitable that deepfake-enhanced videos will sometimes be used for nefarious purposes—this technology allows a video representation of a person’s likeness to be convincingly falsified, and this could be done for political manipulation or societal interference. However, we have seen this in the realm of photography and staged videos for a long time (see, Adobe® Photoshop).

The government has too vested an interest in ensuring that these malicious actions are efficiently and effectively handled to leave it entirely to the realm of victim-pursued civil remedies or just let the Internet be the “wild west”. We note that Canada has experience in trying to legislate malicious Internet actions, to varying degrees of success. Canada’s privacy law places security standards upon the institutions and organizations that hold personal information. Canada’s anti-spam laws have regulated the manner of electronic commercial communications conducted in Canada, which undoubtedly has given Canadians some extra measure of control over their inbox. Legislators can, and should, ensure that existing legal remedies allow the state and

victims to pursue malicious falsified media, but "deepfake technologies" are likely too specific a tool to justify any specific legislation.

In the cybersecurity arms race between the holders of personal information and the malicious actors who want access to it, or between communication providers and networks and those who wish to spam or commit fraud over it, we cannot lose sight of two key facts: first, an intermediary, network, service provider or media outlet will always be attacked by malicious actors, and these platforms are just as much victims of these malicious acts as those that use their services; and, second, the continued susceptibility of individuals to fall victim to fraud, fake news or cyberattack speaks to the fact that humans are, inherently, combinations of emotional, irrational and rational actors.

It is for these reasons that any legislative response must appropriately address education, digital literacy, news literacy, and skeptical thinking, starting from early education through to targeted campaigns during elections. Every individual that uses a platform, and even the platform itself, can potentially be a stopping point for falsified information, be it through traditional means or deepfake videos.

Viral media does not share itself; instead, they are forwarded, tweeted, or emailed by the masses. While deepfake videos will inevitably give additional credence to falsified information, without limiting the tools that individuals, law enforcement and the state should have to prevent and pursue malicious actors, better information and better education can prevent fake news from playing a role that improperly influences society.

by Ryan J. Black, Pablo Tseng and Rosie Schlagintweit, Articled Student

[1] *Canada Elections Act*, SC 2000, c 9, s 480.1.
[2] *Alberta Treasury Branches v Leahy*, 200 ABQB 575 at para 106.
[3] *Jane Doe 72511 v Morgan,* 2018 ONSC 6607. In this decision, the anonymous plaintiff brought an action against her former boyfriend and his parents for posting a sexually explicit video of the plaintiff on a pornographic website without her knowledge or consent. The Court recognized the tort of public disclosure of private facts and found that the plaintiff had established the requirements of the tort. The plaintiff was awarded $50,000 in general damages, $25,000 in aggravated damages, and $25,000 in punitive damages.
[4] *Garland v Consumers' Gas Co.*, 2004 SCC 24 at para 30.
[5] Restatement of the Law, Second, Torts 2d (June 2018 Update), vol 3, p 394, § 652E.
[6] *Parasiuk v Canadian Newspapers Co.*, [1988] 2 WWR 737 (MBQB) at para 5.
[7] *Chandra v Canadian Broadcasting Corp.*, 2015 ONSC 5303 at paras 43-44.
[8] For example, a woman victimized by deepfake pornography or a politician victimized by a deepfake controversy.

**A Cautionary Note**