LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

IN BRIEF

Deep Fakes: What Can Be Done About Synthetic Audio and Video?

Publication No. 2019-11-E
8 April 2019

B. J. Siekierski

Economics, Resources and International Affairs Division
Parliamentary Information and Research Service

Papers in the Library of Parliament's ***In Brief*** series are short briefings on current issues. At times, they may serve as overviews, referring readers to more substantive sources published on the same topic. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations in an objective, impartial manner.

Deep Fakes: What Can Be Done About Synthetic Audio and Video?
(In Brief)

Publication No. 2019-11-E

Ce document est également publié en français.

CONTENTS

DEEP FAKES: WHAT CAN BE DONE ABOUT SYNTHETIC AUDIO AND VIDEO?

1 INTRODUCTION

During the 2015 Canadian federal election campaign, a number of candidates withdrew after compromising videos and social media posts they had made in the past were made public online.[1] While the content varied, the videos and posts had at least one thing in common: the candidates did not deny that the content was real.

Now, however, because of the rapid development of what is known as "deep fake technology," Canadians might not necessarily be able to trust the videos they see or the audio clips they hear.

Deep fake technology, according to one definition, "leverages machine-learning algorithms to insert faces and voices into video and audio recordings of actual people and enables the creation of realistic impersonations."[2] Put more simply, the technology "makes it possible to create audio and video of real people saying and doing things they never said or did."[3]

Once only the domain of the artificial intelligence research community, deep fake technology first attracted public attention in December 2017 when an anonymous user on the online forum Reddit, who went by the name "Deepfakes," started posting synthetic pornographic videos in which the faces of celebrities were convincingly superimposed onto those of the original actors and actresses.[4] Around the same time, the same user released a software kit that allowed others to make their own synthetic videos.[5] The Defence Advanced Research Projects Agency (DARPA) – an agency of the United States Department of Defence – is of the view that now even the relatively unskilled can "manipulate and distort the message of the visual media."[6]

The general public was first alerted to the potential subversive implications of deep fake technology in July 2017, when University of Washington researchers released a synthetic video of former U.S. President Barack Obama.[7] But it was arguably a Belgian political party's intentionally low-quality deep fake video of President Donald Trump appearing to tell Belgians that they should withdraw from the Paris climate change agreement, posted to social media in May 2018, that demonstrated how easily the technology could be used to mislead voters.[8]

As American law professors Robert Chesney and Danielle Citron warned in a paper written in July 2018, "the potential to sway the outcome of an election is quite real, particularly if the attacker is able to time the distribution such that there will be enough window for the fake to circulate but not enough window for the victim to debunk it effectively."[9]

2 WHAT CAN CANADIAN LAW DO ABOUT DEEP FAKES?

The Canadian legal community has slowly begun grappling with how Canadian law might address the potential malicious use of deep fake technology.

The Chesney and Citron paper, though a comprehensive assessment of the potential legal and non-legal responses to deep fakes, focuses entirely on the American context.[10] At the time of writing, the closest Canadian equivalents to their work are three brief articles published by different law firms.[11]

One of the articles summarized a number of causes of action[12] that exist under current Canadian law and that could be applied "in addressing the wrongs committed by a person's misuse or abuse of deepfake technology."[13] Some examples include:

- Copyright infringement: If deep fake content uses copyrighted material, the copyright owner may have recourse to remedies under the *Copyright Act*[14] that include injunctions, damages and court-ordered destruction of the offending material.
- Defamation: When deep fake videos or audio "create false statements of fact about a person's presence and actions that lead to a loss of reputation of that person," that person could be "entitled to damage awards and in some cases injunctive relief to prevent the defamatory material from being further disseminated."
- Violation of privacy: Federal and provincial privacy legislation, including the *Personal Information Protection and Electronic Documents Act*[15] and the B.C. *Privacy Act*,[16] protect Canadians' personal information. According to the authors, however, deep fake videos may not create privacy issues because they do not necessarily expose any part of the victim's life or personal information.
- Appropriation of personality: The appropriation of personality cause of action could apply only if the offender attempted to gain an economic advantage by using the plaintiff's name, likeness, or personality without that person's consent.
- *Criminal Code*:[17] If pornographic deep fake videos depict someone under the age of 18, child pornography provisions could likely be applied. In addition, the *Criminal Code* has provisions against so-called revenge pornography, in which an "intimate image" is shared without consent. Finally, there are also *Criminal Code* provisions that address extortion, fraud and criminal harassment, all of which might apply in some cases.

Though parliamentarians and those aspiring to elected office could rely on these causes of action if victimized by the abusive use of deep fake technology, the *Canada Elections Act*[18] contains provisions that more directly address scenarios in which the technology could be employed to influence or disrupt a Canadian election. As one of the authors, Pablo Jorge Tseng, explained in his appearance before the House of Commons Committee on Access to Information, Privacy and Ethics in October 2018:

> Focusing on elections, we wish to highlight here that Parliament is forward-thinking in the fact that in 2014, they introduced a provision to the [*Canada*] *Elections Act* directed to the impersonation of certain kinds of people in the election process. While such provisions are not specifically targeted at deepfake videos, such videos may very well fall within the scope of this section.[19]

3 DEEP FAKE TECHNOLOGY AND THE *CANADA ELECTIONS ACT*

Tseng was referring to section 480.1 of the *Canada Elections Act* (which was amended in December 2018 to become section 480.1(1)).[20] This section, added to the Act by the 2014 *Fair Elections Act*, addresses impersonation, but there are other ways under the Act in which deep fakes could be prosecuted, including through provisions that were created by the more recent *Elections Modernization Act*, such as publishing false statements to affect election results (section 91(1)) and distributing, transmitting or publishing misleading publications (section 481(1)).[21]

A conviction for some of these offences carries the possibility of a fine of up to $50,000, a five-year imprisonment term, or both. In other words, the *Canada Elections Act* contains provisions that, to a certain degree, proactively address the deep fake threat.

Like Tseng, University of Ottawa professor Michael Pal, who specializes in elections law, has raised the possibility that the impersonation provisions in the *Canada Elections Act* (section 480.1) might cover deep fakes. In a podcast on 28 November 2018, Pal echoed Tseng's point about section 480.1, but added that it is far from clear that deep fakes would fall within the scope of the provisions.[22]

Pal also pointed out that exceptions for "parody and satire" added in section 480.1, while necessary for the protection of freedom of speech, make prosecutions all the more unlikely because of the large degree of subjectivity involved in making that distinction.[23] It should be noted that the new section 481 of the *Canada Elections Act*, which deals with misleading publications, also has an exception for parody and satire.

At first glance, the provisions of section 91(1) of the *Canada Elections Act*, which cover false statements published to affect an election result, could also be used to prosecute the malicious use of deep fakes during a campaign. While that section of the *Canada Elections Act* was previously broadly worded, the amendments contained in the *Elections Modernization Act* circumscribed what kinds of false statements are prohibited.

> **Publishing false statement to affect election results**
>
> 91(1) No person or entity shall, with the intention of affecting the results of an election, make or publish, during the election period,
>
> > (a) a false statement that a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party has committed an offence under an Act of Parliament or a regulation made under such an Act – or under an Act of the legislature of a province or a regulation made under such an Act – or has been charged with or is under investigation for such an offence; or
> >
> > (b) a false statement about the citizenship, place of birth, education, professional qualifications or membership in a group or association of a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party.

Though he was not referring to deep fakes specifically, in prepared remarks for the Senate of Canada's Committee of the Whole on 6 November 2018, the Commissioner of Canada Elections, Yves Côté (whose duty it is to enforce the *Canada Elections Act*), warned that the amendments to section 91 were "unnecessarily restrictive" and could limit false statements to very specific falsehoods, such as the citizenship or place of birth of a candidate.[24] He also said:

> This means that a whole range of false statements that are currently captured by section 91 would no longer be covered.
>
> More specifically, false allegations surrounding an act or conduct that clearly violates accepted community standards without constituting a criminal offence would henceforth be excluded from the scope of the offence.[25]

4 BEYOND THE LAW

On 30 January 2019, the Government of Canada released a "plan to safeguard Canada's 2019 election," which includes several components that could be used to mitigate the impact of deep fake technology.[26] One of those components is the Critical Election Incident Public Protocol, a process which includes a non-partisan panel consisting of the Clerk of the Privy Council, the National Security and Intelligence Advisor, and the deputy ministers of the Department of Justice Canada, Public Safety Canada, and Global Affairs Canada.[27] It will "respond to egregious incidents that meet a high threshold, occurring during the writ period, and that do not fall within Elections Canada's areas of responsibility for the effective administration of the election."[28] If, for example, the Government of Canada became aware of deep fake material that it considered attempted election interference, the heads of Canada's national security agencies would then brief the Critical Election Incident Public Protocol panel, which could then decide on a course of action.

The election safeguard plan committed $7 million to digital, news and civic literacy programming. It also established a permanent Security and Intelligence Threats to Election (SITE) Task Force consisting of the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, Global Affairs Canada, and the Communications Security Establishment. Its goal is to prevent "covert, clandestine, or criminal activities" from "interfering with or influencing electoral processes in Canada."[29]

In addition to its involvement in the new SITE Task Force, on 8 April 2019, the Canadian Centre for Cyber Security, housed within the Communications Security Establishment, released an update of its June 2017 report entitled *Cyber Threats to Canada's Democratic Process*. The initial report did not mention deep fake technology and touched only briefly and generally on the agency's efforts to mitigate other cyber threats. The update, however, made the following observation:

> New technology has created an emerging threat called *deep fakes*, which are synthetic videos often indistinguishable from real footage. Foreign adversaries can use this new technology to try to discredit candidates, and influence voters by, for example, creating forged footage of a candidate delivering a controversial speech or showing the candidate in embarrassing situations.
>
> Improvements in artificial intelligence (AI) are likely to enable interference activity to become increasingly powerful, precise, and cost-effective. Evolving technology underpinned by AI, such as deep fakes, will almost certainly allow threat actors to become more agile and effective when creating false or misleading content intended to influence voters, and make foreign cyber interference activity more difficult to detect and mitigate.[30]

Lastly, on 11 December 2018, the House of Commons Standing Committee on Access to Information, Privacy and Ethics published a report that included one deep fake–specific recommendation: that social media platforms – the primary vehicle for circulating deep fake video or audio – adhere to a code of practices that would require them to remove "defamatory, fraudulent, and maliciously manipulated content (e.g., 'deep fake' videos)."[31] The committee requested a government response to its report, which was presented in the House of Commons on 10 April 2019. In its response, the government stated that online platforms "have a responsibility to make sure they do not become tools for malicious actors interfering in democratic processes," that the government will continue to monitor their behaviour, and that it is "expecting greater action and specific measures to increase transparency, authenticity, integrity, and to combat the spread of disinformation."[32]

5 AMERICAN EFFORTS

In the United States, one promising development is DARPA's Media Forensics program (MediFor), which is trying to confront the deep fake threat in real time. According to the agency:

> If successful, the MediFor platform will automatically detect manipulations, provide detailed information about how these manipulations were performed, and reason about the overall integrity of visual media to facilitate decisions regarding the use of any questionable image or video.[33]

Currently, however, DARPA believes the playing field favours the manipulators of audio and video, which, increasingly, could be just about anyone.[34] "It could be something nation-state driven, trying to sway political or military action. It could come from a small, low-resource group," Matt Turek, the MediFor program manager, told *New Yorker* magazine in late 2018, "Potentially, it could come from an individual."[35]

6 CONCLUSION

During the 2015 federal election campaign, political parties had to contend with crank calls posted on the video-sharing platform YouTube and video footage of inappropriate workplace behaviour and offensive social media posts.[36] During the 2019 federal election campaign, they might also have to contend with deep fake video and audio that purports to be from their candidates.

Amendments to the *Canada Elections Act* that have added offences for unlawful impersonations and misleading publications, along with the Government of Canada's new Critical Election Incident Public Protocol and the SITE Task Force, may partially address the threat, and MediFor's research in the United States could lead to an indispensable tool in the future. For the time being, however, it remains to be seen whether these will be enough to mitigate the impact of deep fake video or audio.[37]

NOTES

1. Canadian Press, "A list of politicians who have made headlines for gaffes in the 2015 campaign," *CTV News*, 11 September 2015.
2. Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *California Law Review*, Vol. 107, 2019 (forthcoming), p. 4.
3. Ibid., p. 1.
4. Oscar Schwartz, "You thought fake news was bad? Deep fakes are where truth goes to die," *The Guardian*, 12 November 2018.
5. Joshua Rotman, "Afterimage: Now that everything can be faked, how will we know what's real?," *New Yorker*, 12 November 2018.
6. Matt Turek, "Media Forensics (MediFor)," *Defence Advanced Research Projects Agency*.
7. Cara McGoogan, "Scarily convincing fake video tool puts words in Obama's mouth," *The Telegraph*, 12 July 2017.
8. Schwartz (2018).
9. Chesney and Citron (2019, forthcoming), p. 22.
10. Ibid.
11. Ryan J. Black and Pablo Tseng, "What Can The Law Do About 'Deepfake'?," *Litigation and Intellectual Property Bulletin*, McMillan LLP, March 2018; Pablo Tseng et al., "What Can and Should the Law Do About 'Deepfake': An Update," McMillan LLP, December 2018; and Renato Mamucud, "The Rise of Deepfake and Media Synthetization," Pullan Kammerloch Frohlinger Lawyers, October 2018.
12. A cause of action, as defined by Philip H. Osborne in the *Law of Torts*, 5th ed., Irwin Law Inc., August 2015, refers to a "factual situation, the existence of which entitles a person to bring legal proceedings against another person and secure a remedy."
13. Black and Tseng (2018).
14. *Copyright Act*, R.S.C. 1985, c. C-42.
15. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

16. *Privacy Act*, RSBC 1996, c. 373.
17. *Criminal Code*, R.S.C. 1985, c. C-46.
18. *Canada Elections Act*, S.C. 2000, c. 9.
19. House of Commons, Standing Committee on Access to Information, Privacy and Ethics [ETHI], *Evidence*, 1st Session, 42nd Parliament, 16 October 2018, 1110 (Mr. Pablo Jorge Tseng, Associate, McMillan LLP, as an individual).
20. See *Elections Modernization Act*, S.C. 2018, c. 31, s. 322. This provision is scheduled to come into force by 13 June 2019 and had not come into force at the time of writing of this paper.
21. This provision is scheduled to come into force by 13 June 2019 and had not come into force at the time of writing of this paper.
22. Michael Pal, "Exercising Your Franchise without a Foreign Assist," *INTREPID*, Podcast, Episode 63, 28 November 2018.
23. Ibid.
24. Yves Côté, Commissioner of Canada Elections, "Speaking notes for an appearance before the Senate of Canada's Committee of the Whole," 6 November 2018.
25. Ibid.
26. Democratic Institutions, "Government of Canada unveils plan to safeguard Canada's 2019 election," News release, 30 January 2019.
27. Government of Canada, *Critical Election Incident Public Protocol*.
28. Democratic Institutions, "Enhancing citizen preparedness," Backgrounder.
29. Government of Canada, *Security and Intelligence Threats to Elections (SITE) Task Force*.
30. Communications Security Establishment, *2019 Update: Cyber Threats to Canada's Democratic Process*, p. 18. The original report was Communications Security Establishment, *Cyber Threats to Canada's Democratic Process*.
31. ETHI, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly*, 1st Session, 42nd Parliament, December 2018, p. 2.
32. Government of Canada, *Government Response to* Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly, 10 April 2019.
33. Turek, "Media Forensics (MediFor)."
34. Ibid.
35. Rotman (2018).
36. Canadian Press (2015).
37. Chesney and Citron (2019, forthcoming), p. 3.