CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING
Volume 24, Number 3, 2021

DOI: 10.1089/cyber.2020.0272

REVIEW

The Real Threat of Deepfake Pornography: A Review of Canadian Policy

Vasileia Karasavva, MA, and Aalia Noorbhai, BSc

Abstract

Deepfakes may refer to algorithmically synthesized material wherein the face of a person is superimposed onto another body. To date, most deepfakes found online are pornographic, with the people depicted in them rarely consenting to their creation and publicization. Deepfakes leave anyone with an online presence vulnerable to victimization. As a testament to policy often being reactionary to antisocial behavior, current Canadian legislation offers no clear recourse to those who are victimized by deepfake pornography. We aim to provide a critical review of the legal mechanisms and remedies in place, including criminal charges, defamation, copyright infringement laws, and injunctive relief that could be applied in deepfake pornography cases. To combat deepfake pornography, we suggest current laws to be expanded to include language specific to falsely created pornography without the explicit consent of all depicted persons. We also discuss the extent to which host websites are responsible for vetting the uploaded content on their platforms. Finally, we present a call for action on a societal and research level to deal with deepfakes and better support victims of deepfake pornography.

Keywords: policy, deepfakes, pornography, image based sexual abuse, technology facilitated sexual violence

A COMMON TYPE OF deepfakes refers to videos that use artificial intelligence tools to seamlessly superimpose the face of a person onto another body, with the end product often being indecipherable from reality.[1] Deepfakes often work using generative adversarial networks, meaning they use two different machine-learning models with opposing goals.[2] In the case of deepfakes, one of the models is trained to create video forgeries and the other is trained to detect them.[2] The algorithm runs until the forger creates a video that is believable enough for the detector to miss.[2] Examples of deepfakes include a Tupac hologram performing at Coachella[3] (Fig. 1), the popular prank where Nicholas Cage replaces the faces of other actors in iconic movie scenes[4] (Fig. 2), and doctored videos of Barack Obama lip-syncing[5] (Fig. 3).

As amusing as deepfakes may appear based on these examples, a darker side of this technology exists. Concerns have already been raised over the use of deepfakes for the spreading of misinformation in politics and their potentially vast destabilizing impact.[6–8] Consequently, lawmakers in North America are debating the best ways to block the spread of misinformation and the defamation of public figures through deepfakes.[9]

Although these are all valid concerns that need to be taken seriously and addressed swiftly, policy should also closely examine the use of deepfake technology for the production of nonconsensual pornography, which reportedly accounts for 96% of the total deepfake videos found online.[10] These videos are distributed on websites dedicated to deepfake pornography that are becoming increasingly popular.[10] In fact, despite the earliest deepfake porn website registering in early 2018, by September 2019 the top four dedicated deepfake pornography websites alone had garnered >134 million views.[10]

As these tools become ever more sophisticated and user-friendly, it is important to consider how deepfake technology can be used as a tool for the perpetration and perpetuation of technology-facilitated sexual violence (TFSV).

Potential Harm of Deepfake Pornography

TFSV refers to criminal, civil, or otherwise harmful sexually aggressive, harassing, or coercive behaviors that are perpetuated with the aid of digital communication technology.[11] The weaponization of deepfakes has the potential to facilitate image-based sexual abuse, that is, the nonconsensual creation, distribution, or threat of distribution of explicit content. Consequently, deepfakes can radically revitalize ''revenge pornography'' and sextortion.

Because of the way the Internet works, deepfake pornographic images uploaded online can be shared and re-shared

Department of Psychology, Carleton University, Ottawa, Canada.

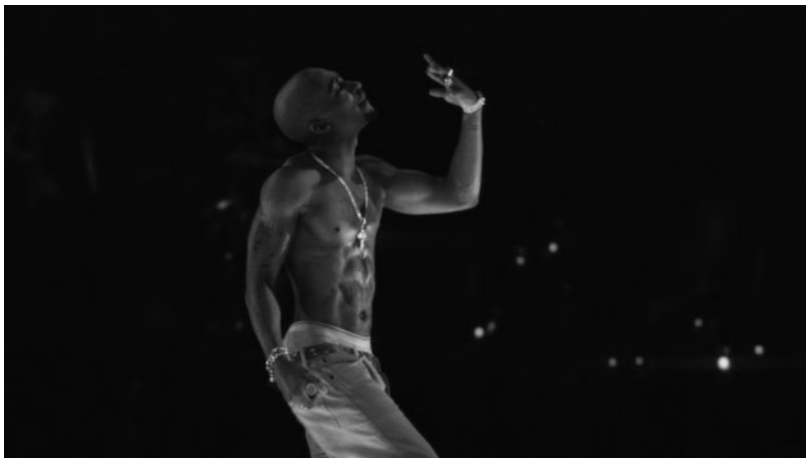

FIG. 1. Deepfaked hologram of Tupac performing in Coachella (Photo by Kevin Winter/Getty Images for Coachella).

hundreds of times on different websites.[12] The negative effects of online sexual abuse can be just as devastating as if they were experienced face-to-face. Although to date, no research has examined the effect of deepfakes on the victims, comparable work on the nonconsensual dissemination of intimate images shows victimization is associated with psychological distress consistent with a diagnosis of moderate to severe depression and/or anxiety disorder.[13] Worse, there have been multiple cases reported where victims that were threatened over the distribution of their sexual pictures attempted or even completed suicide as a direct result of their victimization.[14–16]

At the same time, the potential impact of deepfaked pornography on its viewers should also be considered. In general, mainstream pornography usage is high, especially among men.[17,18] Sexual arousal is not the only reason for viewing pornography, as research suggests some use it as a source of education about sexual practices.[19,20] Pornographic material has the potential to shape the sexual scripts, and ultimately, the behaviors of its consumers.[21] This means that pornography may impact the way individuals expect they should feel, think, and behave during a sexual encounter.[21] Routine exposure to pornography may increase the adherence to sexist and unhealthy notions of sex and relationships, and intensify attitudes related to violence and sexual coercion.[22,23]

In addition, pornography is also linked with sexual and relationship dissatisfaction, and a preference for more extreme, ''porn-like'' sexual activities.[24] Although to date empirical research on the impact of deepfake pornography on the viewer is scant, frequent encounters with it may have a very similar or even worse impact than mainstream pornography. Using deepfake technology, anyone could direct their own pornographic material, casting people from their own lives. This could create unrealistic expectations about sexual performance, likes and dislikes, and the willingness of partners to engage in certain acts. Research endeavors should tackle this issue and investigate the effect of frequent exposure to deepfake pornography on the mental, sexual, and psychological well-being of its viewers.

Democratization and Commodification of Deepfake Technology

In their infancy, deepfake technology required knowledge of complex artificial intelligence tools and algorithms and hundreds of pictures or videos of the potential victim for their creation.[25] However, as technology evolves, the technical threshold required to produce deepfake content is constantly reduced. First, open-source tools like Instagram Scraper or DownAlbum allow users to download all pictures and videos uploaded on publicly available Instagram and Facebook accounts. Thus, using these tools one can easily create the datasets necessary to train the deepfake algorithm and create pornographic material of practically anyone.

FIG. 2. Nicholas Cage as Captain Picard from Star Trek.[55]

FIG. 3. Stills from video of a deepfaked video showing Barack Obama lip-syncing.[56]

Another main driving force behind the increasing accessibility of deepfake technology is online communities and forums where users can exchange tips on creating better and more believable deepfakes. Although websites like Reddit[26] and Discord[27] have banned subreddits and discussion boards on deepfake pornography, other similar forum-based websites that are infamous for hosting unethical and often illegal activity like 4chan and 8chan continue to allow them on their platforms.[28] Furthermore, the face-swapping source code used in the deepfake algorithm is publicly available at no cost on the open-source code repository GitHub for anyone to download and use at their convenience. For those less technology-savvy, deepfake applications and software like FakeApp[29] and Dublicat,[30] or ZAO[31] that require little to no coding skills have been developed. Finally, reports indicate that there are even service portals that generate deepfake video as requested for a price as low as $2.99.[10]

All this indicates that creating a pornographic video using deepfake pornography is becoming increasingly easier and that there are stakeholders that are in prime position to get significant financial gain by the creation and distribution of deepfake pornography. The demand is there, and soon the supply for deepfake pornography is bound to catch up.

This surge in the accessibility and commodification of deepfake technology leaves public figures and private citizens vulnerable to victimization. At present, anyone with an online footprint and pictures of themselves on social media may appear without their consent, or even knowledge, in a pornographic video. In general, public policy is often reactionary, particularly to criminal behavior involving technology, which evolves at a rapid pace. Thus, perhaps unsurprisingly, current legal statutes both in and out of Canada provide no clear recourse to the threat deepfakes pose. However, it is necessary to note that the knee-jerk reaction of advocating for the complete ban and criminalization of deepfake technology may not be warranted. Such a move would put a stop to the beneficial applications of deepfakes, such as its use for parody, satire, and special effects in movies, as well as raising ethical and legal questions over freedom of speech and expression. Instead, we argue that existing laws should be used as guidelines to provide remedies for victims of deepfake pornography.

In this article, we will examine some of the challenges with litigating and regulating deepfake pornography, as well as Canadian legal statutes and torts of interest that may be applicable in cases of deepfake pornography. The purpose of this article was to shed light on the options of victims and call for action from legislators, policymakers, and researchers to investigate ways to better support victims.

Challenges in Regulating Deepfake Technology

First, it is necessary to acknowledge the unique challenges of cybercrime. Individuals who want to conceal their identity online may do so with relative ease, using tools that mask one's IP address. It is also entirely possible that the victims of deepfake pornography will not even become aware that such videos of themselves exist before they have been re-uploaded to multiple websites. Another issue that needs to be considered is that victims and perpetrators may be separated geographically, thus potentially falling under different jurisdictions.[12] Finally, perhaps the biggest hurdle to overcome when dealing with deepfake pornography is the extended timescale that the whole procedure, including the investigation, prosecution, and conviction would require. Crucially, even a conviction does not guarantee the takedown of pornographic material from the Internet. A 2018 report showed that police were unable to provide practical support to victims of revenge pornography, including ensuring the removal of the images of the victim from the internet.[32] Therefore, the effectiveness of policy implementation for deepfake pornography hinges on the cooperation across jurisdictions and the swift removal of nonconsensual deepfaked pornographic material. These challenges should be kept in mind when discussing the legal mechanisms in place in the next section of this article.

Current Legal Mechanisms and Remedies in Place

Criminal charges

One of the first lines of defense that Canadian law has against deepfake pornography is the Canadian Criminal Code. Child pornography laws protect against the depiction of any person under the age of 18 in pornography and specify that this includes material produced using electronic or mechanical means.[33] Thus, not only would the production of deepfake videos with the face of a minor fall into this category but posting such a video would also be prosecuted as an

act of distributing child pornography.[33] There is also precedence where individuals who superimposed images of minors on pornographic material were charged and prosecuted under the child pornography laws.[34,35]

In addition, as of 2015, the Canadian law offers protections against revenge pornography and stipulates that the publication of an intimate image without consent is reprehensible by law.[36] As the law currently stands, it covers sexual or nude images of a person that were produced using photographic, film, or video recordings,[36] leaving the inclusion of deepfake pornography, which is algorithmically synthesized, open to interpretation. However, the law could be expanded, in a manner parallel to child pornography, to include pornographic material produced using electronic means. Finally, the legislation that is currently in place for extortion[37] or fraud[38] would be sufficient to prosecute instances where fraudulent pornographic material created with deepfake technology is used to blackmail or harass. The relationship between the victim and the perpetrator would also affect the prosecution of the case. For example, if the deepfake video was created by a romantic partner, then the case could potentially fall under a domestic abuse statute.[39]

Taken together, conviction using the criminal justice system as is or with minor extensions is feasible; however, the timescale limitation that was previously discussed still holds.

Intentional infliction of mental suffering/harassment

Alternatively, victims could seek justice citing the internal suffering the deepfaked video caused. The tort of intentional infliction of mental suffering (IIMS) has three main requirements as the defendant's conduct needs to be shown to be: (1) flagrant and outrageous, (2) calculated to purposefully harm the victim, and (3) cause the victim harm in the form of visible and provable illness.[40] Two main difficulties arise when prosecuting a case on deepfake pornography using this tort. First, mental illness is not always visible/easy to prove, or some may never incur a mental illness in response to their victimization. Second, proving that the deepfake pornographic video was created with the purpose to hurt the person depicted in it could be challenging. The video creator may defend their actions by claiming that they did so for artistic purposes, satire, or even for their own private pleasure rather than the purposeful humiliation and consequent hurt of the victim.

A similar avenue of prosecuting a deepfake pornography case with a substantially lower threshold is that of harassment, which was recognized by the Ontario Superior Court of Justice in 2017 as a free-standing and tenable cause of action.[41] Similar to the IIMS tort, the conduct of the perpetrator needs to be shown to be outrageous.[41] However, the bar is considered lower here, as it is sufficient for the victim to have experienced severe emotional distress and for the perpetrator to have shown gross disregard over the potential harm of their actions.[41]

Defamation

The Canadian Charter of Rights and Freedoms guarantees the right to freely expressing one's thoughts, beliefs, and opinions.[42] Nonetheless, this freedom is not without its limitations as freedom of expression does not offer protection from the civil tort of defamation.[43,44] The purpose of the defamation tort is to protect a person's reputation from unjustified harm. A victim could argue that their reputation is sullied by the publicization of the deepfaked pornographic video and, under the defamation tort, would be entitled to seek damage awards.[42] However, a simple remedy for the deepfake creator would be to have a disclaimer that the video is produced using machine learning tools and does not depict real events. Doing so, the deepfake creator could argue that the presence of a disclaimer would make any reasonable viewer aware of the false nature of the video, allowing for the victim's reputation to remain intact. This constitutes a valid defense since, in cases of defamation, the law needs to balance the competing rights of protecting one's reputation with restricting someone else's rights to freedom of expression. Accordingly, the law does not offer protections to material that only injures someone's pride, and instead, ambiguous cases, including those regarding the portrayal of sex, tend to be resolved in favor of freedom of expression.[44]

Misappropriation of personality and copyright infringement laws

Depending on the website the deepfake was uploaded, victims may be able to prosecute the case using the appropriation of personality tort. As the commodification of online presence increases so does the value of personality (including likeness, voice, and name).[45] At present, in Canada, the provinces of British Columbia, Saskatchewan, and Newfoundland and Labrador have legislation in place that prohibits the use of a person's likeness for commercial purposes.[45] Posting a deepfake pornographic video on a website that monetizes it in some capacity, either in a pay-per-view manner or by monetizing traffic through advertisements, could represent a cause of action. This tort could also potentially be used to put more pressure on host websites to take on a more active role in vetting the material uploaded on their platforms.

In Canada, for a person to be eligible to assert copyright they need to demonstrate the following: (1) originality (2) their ownership, and (3) that the copyrighted material represents protected work.[46] Copyright infringement law may be one of the best solutions when dealing with revenge pornography,[47] but as the law currently stands, it would be challenging for a victim to claim a deepfake video through this avenue. A deepfake by definition is newly synthesized and not an exact copy of any given single picture or video. Alarmingly, from a copyright law perspective, the deepfake creator could be the one eligible to claim copyright authorship instead, as the originality threshold is relatively low.[46]

A note on injunctive relief and the responsibility of websites

Under certain circumstances, like harassment, a deepfake pornography victim who has won their case may be eligible for injunctive relief and can request links to the video to be deleted from searches of their name.[48] Nevertheless, this is not without limitations as it does not guarantee that the video will be deleted from the Internet or that it will remain offline. A video uploaded online may be downloaded and re-uploaded by multiple users hundreds of times on different websites. Some of these host websites might not

make upholding a legal or moral code their priority, or they could likely operate under different jurisdictions, making any investigation or enforcement of Canadian law challenging. Such host websites could also be fully operational without being indexed on Google or by relying on word-of-mouth for traffic. Links to deepfaked pornographic videos that are posted on such forums could also be found on Google if someone searched for relevant key words other than the victim's name.

In the United States, under Section 512 of the Digital Millennium to Copyright Act (DMCA), host websites are not considered liable for copyright infringement only in situations where they expeditiously remove or disable access to claimed material.[49] Thus, the DMCA takedown notice could represent an invaluable tool for victims of deepfake pornography in assisting them to remove deepfake videos of themselves from online spaces. Moreover, the takedown notice does not require a lawyer or an official copyright registration.[49] This could be adapted in the context of deepfake pornography, allowing victims to quickly and easily claim deepfaked pornographic videos that they appear in. Then, the onus on the removal of the video would fall on the host website.

Major content distribution platforms already have numerous legal obligations in place to control to a certain degree the content they host. These corporations also invest sizeable amounts of money every year in the development of cutting-edge technology that allows them to detect, flag, and remove illegal content. Pressure from legislation on host websites to vet the content they allow and ensure the safety of their users could not only help victims but indirectly move technological advances and research forward. However, the onus on researching this topic should not fall solely on the private industry, and an investment in the development of a task force within the government that would be dedicated to the use of deepfake technology for the perpetration and perpetuation of cybercrime would also be very helpful.

International policies on deepfake pornography

Similar to Canada, other countries seem equally ill-prepared for the major threat that deepfakes pose. For example, previous work has identified a regulatory and legal void when it comes to deepfaked pornographic material in the United Kingdom.[50] On the other end of the spectrum, a couple of notable examples include China and Australia. The Cyberspace Administration in China passed new legislation that will require a disclaimer notifying viewers that the material they are viewing is deepfaked.[51] Doing so may be helpful for the containment of fake news but will do little to protect victims, or to ensure that the material is taken down from the platform it is hosted. In Australia, under Section 91Q of the Crimes Act, individuals are prohibited to intentionally distribute the intimate image of another person without their consent. The language of this legislation is broad enough to be inclusive of deepfaked pornography.[52] At the same time, this approach does not offer any support to the victims who want to take the deepfaked material down and is also limited by the same timescale issues that were previously discussed.

Thus, it becomes apparent that recourse on deepfake pornography is limited globally. The majority of countries are yet to establish options for victims or to explicitly address deepfake pornography in legislation. Given the issues on the jurisdiction that were previously mentioned, deepfakes could represent a unique opportunity for countries to collaborate and address the real threat of deepfakes together.

Future directions

As the dangers of deepfake pornography loom closer, it is important to consider future avenues not only in policy but also in research and the societal level to curb their spreading. First, research should examine the attitudes surrounding deepfake pornography. Previous work on image-based sexual abuse has found that more often than not, victims of revenge pornography are blamed for their victimization, a trend that is likely bound to be repeated in deepfake pornography.[53] More specifically, it is also important for the attitudes of police forces on TFSV and deepfakes to be assessed. In a sample of police officers, more than 1 in 3 of the participants did not disagree with the statement that in-person harassment is more serious than online sexual harassment.[54]

Such attitudes from the general online audience and police forces could create barriers in reporting of victimization. Therefore, to avoid the pattern of underreporting found in in-person sexual abuse, efforts should be made on a societal level to raise public awareness and provide Internet literacy. Doing so could potentially help individuals spot deepfaked material when they encounter it or teach them to critically think about every piece of media they come across online. In addition, deepfake material is often posted online in public forums, and bystanders may choose to side with the perpetrator, the victim, or remain passive viewers of the incident. Educational efforts should also target bystanders, an effort that could result in better support for victims. Research should also closely examine the impact of deepfaked pornography on the psychological, sexual, and general well-being of the viewers, as well as the victims, both the depicted ''face'' and the depicted ''body'' included in the deepfake. Finally, given the potential of deepfakes to completely change the porn industry, research should also investigate the potential impact of deepfakes on attitudes related to sexual norms and scripts, consent, and sexual behaviors.

Conclusions

Deepfaked pornographic videos can negatively impact both the depicted victims and the viewers. Alarmingly, creating a deepfake video is becoming increasingly easier. The Canadian legal system leaves those victimized by deepfaked pornographic videos vulnerable, as it offers no clear recourse that can address their potential harms and ensure their removal from the Internet. Although legal remedies and expansions of current legal statutes would be a great first step, it is also crucial for online platforms to institute policies for the detection, flagging, and removal of deepfake pornography. Deepfaked pornography is becoming more accessible day by day and remedies for the victims should be put in place early on to improve the online experience of many. The responsibility to act swiftly and decisively falls not only on legislators, policymakers, and other stakeholders but also on researchers as well. Deepfake technology remains a largely

understudied topic in the empirical literature and we urge social scientists to take action to remedy this.

Author Disclosure Statement

No competing financial interests exist.

Funding Information

No funding was received in association with this paper.

References

1. McGlynn C, Rackley E, Houghton R. Beyond ''Revenge Porn:'' the continuum of image-based sexual abuse. Feminist Legal Studies 2017; 25:25–46.
2. Bansal A, Ma S, Ramanan D, et al. (2018) Recycle-GAN: unsupervised Video Retargeting. *Proceedings of the European Conference on Computer Vision (ECCV)*. pp. 119–135.
3. Donoughue P. Dead musicians are touring again, as holograms. It's tricky—technologically and legally. ABC News, 2018.
4. Haysom S. People are using face-swapping tech to add Nicolas Cage to randoom movies and what is 2018. Mashable, 2018.
5. Langston J. Lip-synching Obama: New Tools Turn Audio Clips into Realistic Tools. UW News, 2017.
6. Chesney R, Citron DK. Deepfakes and the new disinformation war: the coming age of post-truth geopolitics. Essays 2019; 98:147–155.
7. Blitz MJ. Lies, line drawing, and deep fake news. Oklahoma Law Review 2018; 71:59–116.
8. Vaccari C, Chadwick A. Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society 2020; 6:1–13.
9. Ruiz D. Deepfakes Laws and Proposals Flood US. Malwarebytes, 2020.
10. Ajder H, Patrini G, Cavalli F, et al. The state of deepfakes: landscape, threats, and impact. Deeptrace, 2019.
11. Henry N, Powell A. Technology-facilitated sexual violence: a literature review of empirical research. Trauma, Violence, & Abuse 2018; 19:195–208.
12. Franks MA. Drafting an effective ''Revenge Porn'' law: a guide for legislators. SSRN Electronic Journal, 2015. DOI: 10.2139/ssrn.2468823.
13. Henry N, Powell A, Flynn A. Not Just ''Revenge Pornography'': Australians' Experiences of Image-Based Abuse. A Summary Report. Melbourne: RMIT University, 2017.
14. Megas N. Sextortion Killed their Son. Cops Looked the Other Way. The Daily Beast, 2018.
15. Reavy P. Utah Family Sharing Sextortion Suicide Story ''Likely Saved Some Lives'' Police Say. DeseretNews .Com, 2019.
16. Dearden L. Five British men have killed themselves after falling victim to online ''Sextortion,'' police reveal. The Independent, 2019.
17. Albright J. Sex in America Online. An exploration of sex, marital status, and sexual identity in internet sex seeking and its impacts. Journal of Sex Research 2008; 45:175–186.
18. Morgan EM. Associations between young adults' use of sexually explicit materials and their sexual preferences, behaviors, and satisfaction. Journal of Sex Research 2011; 48:520–530.
19. Benjamin O, Tlusten D. Intimacy and/or degradation: heterosexual images of togetherness and women's embracement of pornography. Sexualities 2010; 13:599–623.
20. Parvez ZF. The labor of pleasure: how perceptions of emotional labor impact women's enjoyment of pornography. Gender & Society 2006; 20:605–631.
21. Wright PJ. Mass media effects on youth sexual behavior assessing the claim of causality. Annals of the International Communication Association 2011; 35:343–385.
22. Flood M. The harms of pornography exposure among children and young people. Child Abuse Review 2009; 18: 384–400.
23. Hald GM, Malamuth NN, Lange T. Pornography and sexist attitudes among heterosexuals. Journal of Communication 2013; 63:638–660.
24. Miller DJ, McBain KA, Li WW, et al. Pornography, preference for porn-like sex, masturbation, and men's sexual and relationship satisfaction. Personal Relationships 2019; 26:93–113.
25. Nguyen TT, Nguyen CM, Nguyen DT, et al. Deep Learning for Deepfakes Creation and Detection. arXiv Preprint 2019; 1909.11573.
26. Robertson A. Reddit bans 'Deepfakes' AI porn communities. The Verge, 2018.
27. Liptak A. Discord shut down a chat group that shared fake celebrity porn edited with artificial intelligence. The Verge, 2018.
28. Schumacher E. 'Deepfake' technology sees dramatic rise. Deutsche Welle, 2019.
29. Zucconi A. (2018) How to Install FakeApp. www .Alanzucconi.com (accessed Feb. 9, 2020).
30. Neocortex INC. Doublicat: Face Swap AI-tool 1.0.8 2020.
31. Vonau M. Viral Deepfake App ZAO Adds your Face to Famous Movie Scenes—if you're not Concerned with Privacy. Android Police, 2019.
32. North Yorkshire Police, Fire and Crime Commissioner. Suffering in Silence: Why Revenge Porn Victims are Afraid and Unwilling to Come Forward Because of a Fear they'll be Named and Shamed—and why that Needs to Change 2018.
33. Criminal Code, R.S.C. 1985, c. C-46, s. 163.1.[1]
34. R v H(C), 2010 ONCJ 270.
35. D(R) v S(G), 2011 BCSC 1118.
36. C-13, 41st Parliament, 2nd Session.
37. Criminal Code, R.S.C. 1985, c. C-46, s. 346.1.
38. Criminal Code, R.S.C. 1985, c. C-46, s. 380.1.
39. Domestic Violence Protection Act. S.O. 2000, c.33—Bill 117.
40. Boucher v. Wal-Mart Canada Corp.,2014 ONCA 419.
41. Merrifield v. The Attorney General of Canada, 2017 ONSC 1333.
42. Canadian Charter of Rights and Freedoms, s 2, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.
43. Walker J. Hate speech and freedom of expression: legal boundaries in Canada. Library of Parliament, 2018.
44. Libel and Slander Act, R.S.O. 1990, c.L.12.
45. R. v. Butler, 1992 1 S.C.R. 452.
46. McMillan LLP. Appropriation of pesonality. McMillan Intellectual Property Bulletin, 2012.
47. Copyright Act, R.S.C. 1985, c. C-42.

48. Levendowski A. Using copyright to combat revenge porn. The NYU Journal of Intellectual Property and Entertainment Law 2013; 3:423–439.
49. Google Inc., v. Equustek Solutions, Inc., 2017 1 S.C.R. 824.
50. 17 U.S. Code § 512.
51. ''China Issued Measures for Cybersecurity Review,'' *Privacy & Information Security Law Blog*, April 29, 2020. https://www.huntonprivacyblog.com/2020/04/29/china-issued-the-measures-for-cybersecurity-review/ (accessed Mar. 9, 2020).
52. Farish K. Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of the deepfake. Journal of Intellectual Property Law & Practice 2020; 15:40–48.
53. Mckinlay T, Lavis T. Why did she send it in the first place? Victim blame in the context of ''revenge porn.'' Psychiatry, Psychology and Law 2020; 27:1–11.
54. Holt TJ, Bossler AM. Police perceptions of computer crimes in two southeastern cities: an examination from the viewpoint of patrol officers. American Journal of Criminal Justice 2012; 37:396–412.
55. [deepfakes] (January, 2018). International Treasure | Deepfakes Replacement. Youtube. https://www.youtube.com/watch?v=xia1qQ9uNQc&fbclid=IwAR1HeQf4smBIbhmSVHNyjz7BttBUfQj7XSs0Moyb8eEOrkqIVZrpDMB9k3w&ab_channel=derpfakes (accessed Aug. 16, 2020).
56. Suwajanakorn S, Seitz SM, Kemelmacher-Shlizerman I. Synthesizing obama: learning lip sync from audio. ACM Transactions on Graphics 2017; 36:1–13.

Address correspondence to:
Vasileia Karasavva
Department of Psychology
Carleton University
319 Lebreton Street South
Ottawa K1S 4L4
Ontario
Canada

E-mail: vasiakarasavva@cmail.carleton.ca