**Pourna Sengupta   
Project Description**

**CYBR 4400**

**February 7, 2020**

**Deepfake Technology**

*Social Media and Political Deepfake*

***Introduction***

Deepfake technology is the creation of videos including audio that depict an individual doing and/or saying something that is either completely fabricated or is an altered version of the original. Deepfakes are created using neural networks. Neural networks are algorithms that mimic the human brain that take real data and translate it into vectors and find patterns[[1]](#footnote-1). Deepfakes target social media and other widely used public platforms, spreading false or altered information. These platforms make it easy to circulate deepfakes which can easily be sent and shared with very few clicks. Deepfakes can impersonate a range of people, including politicians and celebrities.

***Background***

There are four types of deepfakes: hobbyists created deepfakes, politically motivated deepfakes, fraud deepfakes, and legitimate actors. Communities of hobbyists create deepfakes as a source of entertainment and may gain following on social media or other public platforms. Their work includes porn and movie deepfakes. Politically motivated deepfakes come from foreign governments and activist societies. They conduct “disinformation campaigns to manipulate public opinion and undermine confidence in a given country’s institutions”[[2]](#footnote-2). Fraud deepfakes are used to carry out fraud by individuals or groups. Legitimate actors, commonly TV companies, may use deepfake to include actors that have passed away[[3]](#footnote-3).

There is discussion of policy that can help address the host of issues brought on by deepfake. This includes legislation and regulation to address issues through civil or criminal law. Current laws could be adapted to include issues arising from deepfake such as “libel, defamation, identity fraud, or impersonating a government official”[[4]](#footnote-4). Corporations themselves also have the ability to implement regulation. This includes a discussion of ethics and transitioning from a company focus of generating publicity and profit to providing secure and authentic media for its users. Companies must  **“**proactively enforce transparent, shared policies to block and remove deepfakes”4.

Implementing anti-deepfake technology is the general approach to addressing and combatting the issues that arise with the growing use of deepfake technology on public platforms. “Deepfake developers tend to use results from published deepfake research to improve their technology and get around new detection systems”[[5]](#footnote-5). This means that anti-deepfake technology must be focused on detecting and preventing the creation of deepfake to reduce the amount of accessible deepfake, slowing developers ability to continuously improve their creation of deepfakes. Integration of digital watermarks or “noise” are plausible methods to authenticate content and allow differentiation between real and deepfake content.

***Research Focus***

Deepfake is used throughout many platforms with various uses. Therefore, there are many areas of focus such as entertainment and political use. Regulating deepfake can be difficult since regulation regarding one are of focus may not always apply flawlessly to another. Throughout my research into deepfake, I’d like to focus on deepfake on social media and it’s use in political (smear) campaigns. What government and company regulations can be put in place to reduce the use of deepfake technology on social media as a tool for political gain without threatening company and individual first amendment rights?

***Research Methodology***

The first step to researching this is to find as much research from journal articles, government articles and reports, conference reports, and other academic articles that discuss deepfake technology in social media. This allows for familiarity with the use of deepfake on social media and how it impacts deepfake developers, the corporation, and individual users. The research can then narrow into deepfake technology in social media with political motivation. This allows focus on the affects and dangers deepfake poses to political campaigns, issues publicly voted on, and the rise of activism and/or movements as a result of misinformation. The last section of research includes current and/or possible legislation and regulation of social media and specifically politically motivated deepfake. This research should include discussion of who imposes and implements regulation, whether it be the corporation, government, or internet providers.

Based on the research, the interdisciplinary framework can be used to formulate an argument on whether or not regulation is necessary. This is based on how issues arising from politically motivated deepfake affect public misinformation and whether or not legislation and/or regulation can address and solve these issues. From there, the argument can be built and supported using proposed and current regulation, discussing how they address the issues of political deepfake in social media. Once a policy analysis has been conducted, we can assess how these regulations abide by the first amendment. If they threaten freedom of speech, the policy must be adjusted so that it abides the first amendment, making it usable in current day social media platforms.

***Bibliography***

Chesney, Bobby, and Danielle Citron. 2019. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107: 1753–1820.

Nicholson, Chris. n.d. “A Beginner’s Guide to Neural Networks and Deep Learning.” Wiki. Pathmind. Accessed February 2, 2020. https://pathmind.com/wiki/neural-network.

Siekierski, B. J. 2019. “Deep Fakes: What Can Be Done About Synthetic Audio and Video?” *No. 2019-11-E*, Economics, Resources and International Affairs Division Parliamentary Information and Research Service, , April. https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/InBriefs/PDF/2019-11-e.pdf.

Westerlund, Mika. 2019. “The Emergence of Deepfake Technology: A Review.” *Technology Innovation Management Review* 9 (11): 39–52.

1. (Nicholson n.d.) [↑](#footnote-ref-1)
2. Page 42, (Westerlund 2019) [↑](#footnote-ref-2)
3. (Westerlund 2019) [↑](#footnote-ref-3)
4. Page 44, (Westerlund 2019) [↑](#footnote-ref-4)
5. Page 45, (Westerlund 2019) [↑](#footnote-ref-5)