AI deepfakes within politics: Navigating the business of it

BUSI 3302: Connecting Bauer to Business

KPMG US | UH Bauer Fall 2024

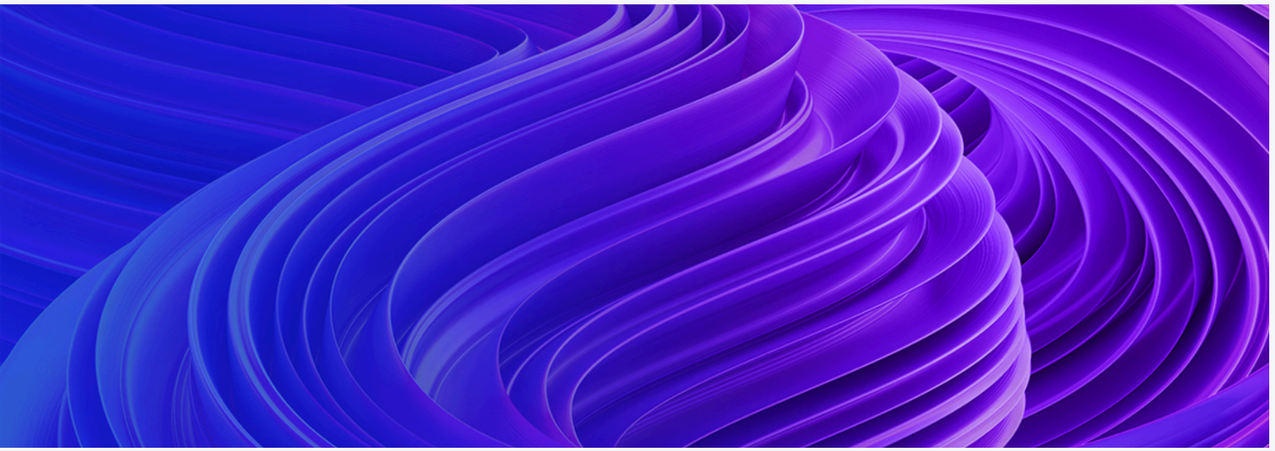
What is a deepfake?

An Al deepfake is a form of synthetic media that is generated by artificial intelligence. The most common forms of Al deepfakes are videos. Al deepfakes are different forms of realistic looking content that can alter peoples' actions, words, and appearance.

To create an AI deepfake, one must simply type what they would like to see, and this intricate technology will do its best to create what it is told. Deepfakes are usually produced without consent and done with ill intent. As this new technology has rapidly grown, it has become a rising issue in politics, business, and even has negative societal effects.

Ethical issues of AI deepfakes

The harm that AI deepfakes cause can come in different forms. Some of the forms of harm include psychological, emotional, financial, and discriminatory. Spreading of false information can cause psychological and emotional harm through negative backlash. AI deepfakes allow people to cross boundaries and invade privacy. It exploits and exposes people.



Deepfakes are usually produced without consent and done with ill intent. The results of Al deepfakes have the potential to ruin people's reputations by spreading misinformation. This new technology is especially dangerous because there are no federal laws specifically surrounding Al deepfakes.

We believe that not all Al deepfakes are produced with ill intent. Accessibility is a crucial factor when it comes to inclusivity. Al deepfakes can be used to translate content for those who speak different languages and can also provide subtitles for people without hearing.

Fraud and misinformation

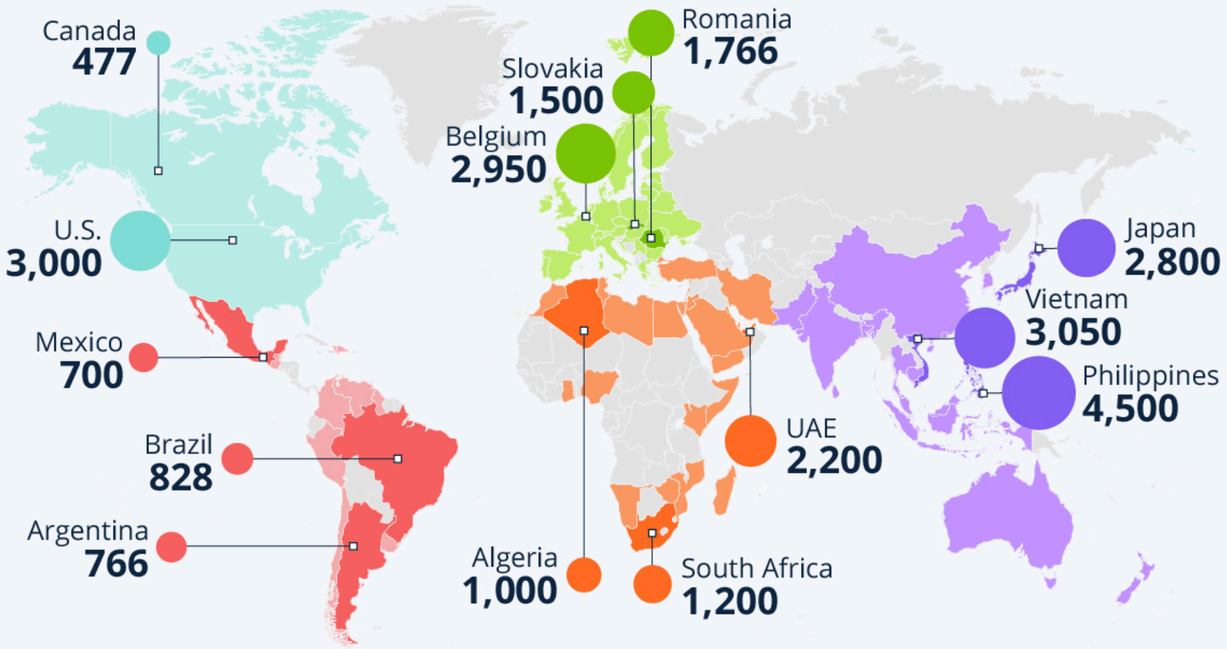
Deepfakes have been linked to misinformation and fraud. AI deepfakes of public figures have been used for the wrong purpose, leading to concerns about privacy and reputation.

The Taylor Swift deepfake

For example, deepfakes of Taylor Swift's images have been used in fake videos and ads without her consent which misleads fans and tarnishes her image. Moreover, they are used to spread false and unethical information using her name. These unauthorized deepfakes blur the line between reality and fiction; it creates potential for reputational harm, legal issues, and exploitation. This demonstrates how deepfakes can be weaponized to impersonate celebrities, causing confusion and loss of control over their own likeness and public image.

The Explosive Growth of AI-Powered Fraud

Countries per region with biggest increases in deepfake-specific fraud cases from 2022 to 2023 (in %)*



The report analyses +2M cases of identity fraud attempts from 224 countries/territories.
All data is aggregated and anonymized * Regions according to source

Source: Sumsub Identity Fraud Report 2023

Rapid growth

Fruadulent activity has seen rapid growth in deepfake-specific fraud in recent times.

Philippines
4,500% increase

Vietnam
3,050% increase

United States
3,000% increase

Belgium
2,950% increase

A global threat

Deepfakes pose a high risk within poilitical campaigns on a global scale.

Misinformation has the highest impact severity rank for global risk over the next 2 years.

1st risk in India
Over 1.4bn (nearly 50% internet penetration) head for a general election in April-May 2024

6th risk in the United States
Nearly 340m (92% internet penetration) head for a presidential election in November 2024

8th risk in European Union
Nearly 450m (89% internet penetration) elect the EU Parliament in June 2024

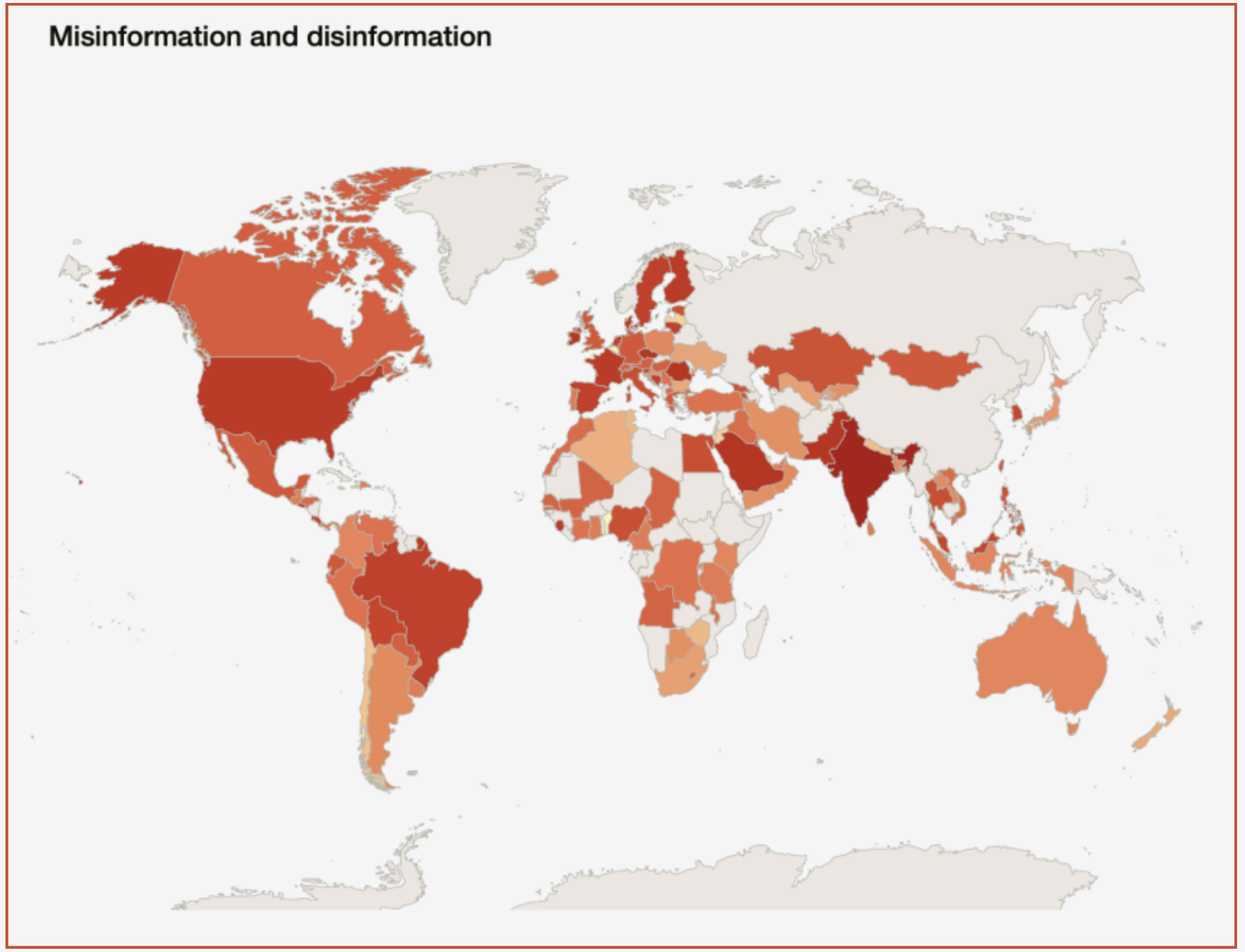
11th risk in United Kingdom
Nearly 68m (98% internet penetration) head for a general election by January 2025

11th risk in Mexico
128m (79% internet penetration) head for a general election in June 2024

18th risk in Indonesia
Nearly 278m (88% internet penetration) head for a presidential election in March 2024

22nd risk in South Africa
Over 60m (72% internet penetration) head for a general election in 2024

Russia
Around 145m (88% internet penetration) head for a presidential election in March 2024



Source
World Economic Forum Executive Opinion Survey 2023; Worldometer, 2023; Statista, 2023; DataReportal, 2023.

Note
EU excludes Slovakia.

Rank
1st 10th 20th 30th 36th

The negative impact on politics

In February 2024, a deepfake audio using Joe Biden’s voice was used to target Democratic voters in the state of New Hampshire with an automated phone call. In the phone call, there was a message influencing people to not vote in the state’s primary election using a fake voice of Joe Biden. Another example is a deepfake video of President Volodymyr Zelenskiy of Ukraine showed the President seemingly urging his army to surrender to Russia. The convincing video was spread globally and left many to wonder if the video was real or not, including his own troops.

This illustrates how deepfake technology can erode trust in leaders and distort reality. The misuse of deepfakes has the potential to sway public opinion and influence election outcomes.

Technology in the new world

The impact that AI deepfake technology has seen within politics is not all bad. Advancements of deepfakes has allowed voters to become closer with thier candidates.

Connecting People to Politicians

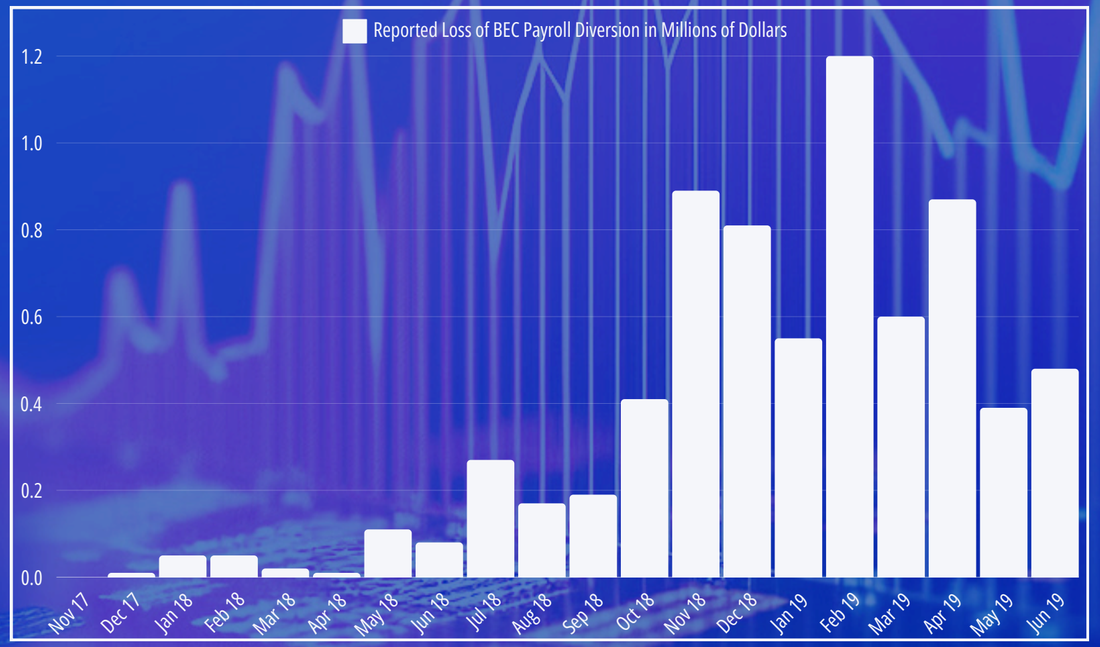
AI Steve is a chatbot that uses deepfake voicing of Steve Endacott, the real life AI Steve, to communicate with his supporters and voters within Brighton and Hove. The feedback recived from the chatbot is relayed in Parliament and thus the people decide how their council representative will vote. This is just one example of a positive impact from AI deepfake technology.

The financial impact

Financial losses due to AI deepfakes are a real and growing threat to companies and individuals.

BEC scams

Business email compromise (BEC) scams are one of the most successful forms of cyber attack. Between 2013 and 2019, the FBI reported over a $26.2 billion domestic and international exposed dollar loss to this scam. The scam typically inlcudes only an email requesting a wire transfer for a certain amount of money, but with the advancements of deepfake technology, these scams now inlcude synthetic audio and video calls in real time.



Societal benefits

AI deepfakes are not all harmful though. It is constantly evolving and revolutionizing the way we go about our daily lives within the creative arts and educational fields.

Deepfakes can be used to recreate historical figures or events and translate famous speeches from global leaders. This can transform education and benefit learners audibly and visually.

Technology: AI

Creative and Artistic

Deepfake technology is revolutionizing the entertainment and arts industry

People can now re-live reproductions of their favorite deceaced actors and actresses through the usage of AI deepfake technology. This use of deepfake technology is not only limited to film and entertainment though.

Current legal limitations

The Federal Trade Commission (FTC) currently takes action against AI Deepfake situations that are harmful to whoever is targeted. They currently try to detect any false harmful information with the tools they possess. The FTC has come out with a Government and Business Impersonation rule that indicates that they obtain stronger materials to identify scammers who try to impersonate government agencies or businesses. With this rule, the FTC has been able to file federal court cases against scammers who have tried profiting off of them with false information and are obligated to return any money made off of scamming.

Legal limitations

While there are currently no federal bills pertaining to AI deepfakes that have passed congress, a few states have passed bills regulating deepfake content. These regulations are to protect the integrity of democracy and the people of the United States against digital manipulation and technological misuse.

There are currently 17 states that have passed legislation regarding AI deepfake technology within political campaigns and non-consensual sexual conduct. Texas is one of these states.

Texas SB 751: Criminalizes the fabrication of deceptive videos intended to harm a candidate or influence election outcomes

Florida SB 1798: Criminalizes the creation, alteration, or modification of images depicting identifiable minors engaged in sexual conduct

California AB 602: Allows individuals to sue if a deepfake of them in sexual content is distributed without consent

California AB 730: Bans distribution of deepfakes intended to harm political candidates within 60 days of an election

Strategic initiatives

AI deepfakes hold the potential to revolutionize media and education though cost-effective content creation. However, significant legal and ethical concerns remain, along with the threat of misinformation and security risks.

Strengths: Cost-effective content creation
AI deepfakes are affordable to create synthetic audio and video.

Weaknesses: Ethical and legal concerns
Concerns around underdeveloped legal framework and ethical questions on consent.

Opportunities: Entertainment and Educational
AI deepfakes have endless opportunity within entertainment and education.

Threats: Misinformation and Fruad
Fraudulent deepfakes create misinformation and political distrust, posing security and financial risks.

Plan of Action

What steps can we take?

With the growing use of AI technology and the increasing accessibility to create and manipulate synthetic content, it is essential to combat the threats associated with AI deepfakes. How can we mitigate the risks associated with AI deepfake technology while also leveraging their potential benefits for both society and businesses?

We propose to focus on detection systems, legal regulation, educational campaigns, and promoting responsible innovation.

Detection algorithms: Develop technological algortithms to identify and verifiy synthetic deepfake material

Regulation and laws: Establish legal regulations to hold people and businesses accountable for creating unethical content

Government educational campaigns: Launch government sponsored campaigns to educate the public about the risks associated with AI deepfakes and promote healthy usage

Verification systems: Establish and promote ethical guidelines for businesses and creators to follow when using deepfake technology

Nikole Welcome
Team Lead

Tracy Hoang
Internal Communications

Naomi Lopez
Internal Communications

Hien Tran
Lead Writer

Manning Ngo
Records and Tracking

Braden Abramowitz
Reseach Lead

Enes Goktas
Display Lead

Mike Schubarth
Milestone Lead

Monique Vu, EA
Team Coach, Manager
Vialto Partners

Contributors

This project was done in collaboration with The University of Houston’s Bauer College of Business and KPMG US.

We thank KPMG US for sponsoring this ethics case competition and Rockwell Career Center for organizing the event.

We would also like to thank our coach, Monique Vu for providing us feedback and mentorship throughout the durations of this project.