From robocalls to fake porn: Going after AI's dark side

June 4 2024, by Flint McColgan, Boston Herald

Credit: Unsplash/CC0 Public Domain

New Hampshire voters received a barrage of robocalls in which a computer-generated imitation of President Biden discouraged them from voting in the January primary. While the admitted mastermind was slapped with felony charges and a proposed FCC fine, his deed is just one wound left by the cutting-edge technology law enforcement is struggling to catch up with: artificial intelligence.

Computer-generated "deepfakes" can impersonate not only the voice and face of anyone but can contribute to the manipulation of and the sexual and reputational harm to individuals and the public at large.

"I think AI is going to affect everything everyone in this room does on a daily basis, and it's certainly going to affect the work of the Department of Justice," acting U.S. Attorney for Massachusetts Joshua Levy said during a reporter roundtable. "How that's exactly going to play out, time will tell."

Of particular concern to Levy was the technology's ability to introduce new "doubts" to time-tested forensic evidence at trial.

"We rely a lot on … audiotape, videotape in prosecutor cases," he said. "We have to convince 12 strangers (the jury) beyond a reasonable doubt of someone's guilt. And when you introduce AI and doubts that can be created by that, it's a challenge for us."

Lawmakers across the nation and around the world are trying to catch up to the fast-growing technology and its legal analysis has become a hot academic topic.

Top-level moves

"We're going to see more technological change in the next 10, maybe next five, years than we've seen in the last 50 years and that's a fact," President Biden said in October just before signing an executive order to regulate the technology. "The most consequential technology of our time, artificial intelligence, is accelerating that change."

"AI is all around us," Biden continued. "To realize the promise of AI and avoid the risk, we need to govern this technology."

Among many other regulations, the order directed the Department of Commerce to develop a system of labeling AI-generated content to "protect Americans from AI-enabled fraud and deception" and attempts to strengthen privacy protections through funding research into those fields.

In February, the U.S. Department of Justice—of which Levy's office is a regional part—appointed its first "Artificial Intelligence Officer" to spearhead the department's understanding and efforts on the quickly emerging technologies.

"The Justice Department must keep pace with rapidly evolving scientific and technological developments in order to fulfill our mission to uphold the rule of law, keep our country safe, and protect civil rights," Attorney General Merrick Garland said in the announcement.

AI Officer Jonathan Mayer, an assistant professor at Princeton University, the DOJ explained, will be among a team of technical and policy experts that will advise leadership on technological areas like cybersecurity and AI.

Across the Atlantic, the European Union in March passed its own AI regulation framework, the AI Act, that had spent five years in development.

One of the legislative leaders on the issue, the Romanian lawmaker Dragos Tudorache, said ahead of the vote that the act "has nudged the future of AI in a human-centric direction, in a direction where humans are in control of the technology," according to the Associated Press.

Sam Altman, the CEO and cofounder of OpenAI—maker of the hugely popular ChatGPT service powered by AI large language models—in May of last year called on Congress to regulate his industry.

"There should be limits on what a deployed model is capable of and then what it actually does," he said at the Senate hearing, calling for an agency to license large AI operations, develop standards and conduct audits on compliance.

State-level moves

Biden's executive order is not permanent legislation. In the absence of federal-level laws, states are making their own moves to mold the technology the way they want it.

The software industry advocacy group BSA The Software Alliance tracked 407 AI-related bills across 41 U.S. states through Feb. 7 of this year, with more than half of them introduced in January alone. While the bills dealt with a medley of AI-related issues, nearly half of them—192—had to do with regulating "deepfake" issues.

In Massachusetts, Attorney General Andrea Campbell in April issued an "advisory" to guide "developers, suppliers, and users of AI" on how their products must work within existing regulatory and legal frameworks in the commonwealth, including its consumer protection, anti-discrimination and data security laws.

"There is no doubt that AI holds tremendous and exciting potential to benefit society and our Commonwealth in many ways, including fostering innovation and boosting efficiencies and cost-savings in the marketplace," Campbell said in the announcement. "Yet, those benefits do not outweigh the real risk of harm that, for example, any bias and lack of transparency within AI systems can cause our residents."

The Boston Herald asked the offices of both Campbell and Gov. Maura Healey about new developments on the AI regulation front. Healey's office referred the Herald to Campbell's office, which did not respond by deadline.

On the other coast, California is trying to lead the way on regulating the technology expanding into practically every sector at lightspeed—but not to regulate it so hard that the state becomes unattractive to the wealthy tech firms leading the charge.

"We want to dominate this space, and I'm too competitive to suggest otherwise," California Gov. Gavin Newsom said at an event announcing a summit in San Francisco where the state would consider AI tools to tackle thorny problems like homelessness. "I do think the world looks to us in many respects to lead in this space, and so we feel a deep sense of responsibility to get this right."

The risks: Manipulation

The New Orleans Democratic Party consultant who said he was behind the Biden-mimicking voice-cloning robocalls allegedly did so very cheaply and without elite technology: by paying a New Orleans street magician $150 to make the voice on his laptop.

The novel plot had no direct criminal codes involved. The New Hampshire attorney general on May 23 had mastermind Steven Kramer indicted on 13 counts each of felony voter suppression and misdemeanor impersonation of a candidate. The Federal Communications Commission the same day proposed a $6 million fine on him for violations of the "Truth in Caller ID Act" because the calls spoofed the number of a local party operative.

Just the day before, FCC Chairwoman Jessica Rosenworcel announced proposals to add transparency to AI-manipulated political messaging, but stopped short of suggesting the content be prohibited.

The announcement said that "AI is expected to play a substantial role in the creation of political ads in 2024 and beyond" and that public interest obliges the commission "to protect the public from false, misleading, or deceptive programming."

A look at the academic literature on the topic over the last several years is rife with examples of manipulations in foreign countries or by foreign actors operating here in the U.S.

"While deep-fake technology will bring certain benefits, it also will introduce many harms. The marketplace of ideas already suffers from truth decay as our networked information environment interacts in toxic ways with our cognitive biases," authors Bobby Chesney and Danielle Citron wrote in the California Law Review in 2019.

"Deep fakes will exacerbate this problem significantly. Individuals and businesses will face novel forms of exploitation, intimidation, and personal sabotage. The risks to our democracy and to national security are profound as well," their paper "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" continued.

Since 2021, a TikTok parody account called @deeptomcruise has illustrated just how powerful the technology has become by splicing Hollywood superstar Tom Cruise's face on others' bodies and cloning his voice. The playful experiment still required state-of-the-art graphics processing and copious footage to train the AI on Cruise's face.

"Over time, such videos will become cheaper to create and require less training footage," author Todd Helmus wrote in a 2022 RAND Corporation primer on the technology and the disinformation it can propel.

"The Tom Cruise deepfakes came on the heels of a series of deepfake videos that featured, for example, a 2018 deepfake of Barack Obama using profanity and a 2020 deepfake of a Richard Nixon speech—a speech Nixon never gave," Helmus wrote. "With each passing iteration, the quality of the videos becomes increasingly lifelike, and the synthetic components are more difficult to detect with the naked eye."

As for the risks of the technology, Helmus says, "The answer is limited only by one's imagination."

"Given the degree of trust that society places on video footage and the unlimited number of applications for such footage, it is not difficult to conceptualize many ways in which deepfakes could affect not only society but also national security."

Chesney and Citron's paper included a lengthy bulleted list of possible manipulations, from one similar to the Biden-aping robocalls to "Fake videos (that) could feature public officials taking bribes, displaying racism, or engaging in adultery" or officials and leaders discussing war crimes.

The risks: Sexual privacy

In a separate article for the *Yale Law Journal*, Citron, who was then a Boston University professor, reviewed the damage caused by deepfake pornography.

"Machine-learning technologies are being used to create 'deep-fake' sex videos—where people's faces and voices are inserted into real pornography," she wrote. "The end result is a realistic-looking video or audio that is increasingly difficult to debunk."

"Yet even though deep-fake videos do not depict featured individuals' actual genitals (and other private parts)," she continued, "they hijack people's sexual and intimate identities. … They are an affront to the sense that people's intimate identities are their own to share or keep to themselves."

Her paper included some horrific examples, in which celebrities like Gal Godot, Scarlett Johansson and Taylor Swift were subjected to the AI-generated porn treatment, in sometimes very nasty contexts. Others were detailed seeking help to generate such imagery of their former intimate partners. Fake porn was made of an Indian journalist and disseminated widely to destroy her reputation because the people who made it didn't like her coverage.

Citron concludes with a survey of legal steps that can be examined, but states that "Traditional privacy law is ill-equipped to address some of today's sexual privacy invasions."

At the roundtable meeting, U.S. Attorney Levy found the pornographic implications of the technology equally as troublesome as the other connotations.

"I'm not an expert on child pornography law, but if it's an artificial image, I think it's going to raise serious questions of whether that's prosecutable under federal law," he said. "I'm not taking an opinion on that, but that's a concern I think about."

2024 MediaNews Group, Inc. Distributed by Tribune Content Agency, LLC.

Citation: From robocalls to fake porn: Going after AI's dark side (2024, June 4) retrieved 25 June 2024 from https://techxplore.com/news/2024-06-robocalls-fake-porn-ai-dark.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.