

FORUM:	Human Rights Council
ISSUE:	Measures to Prevent Voice Cloning Fraud and AI-Generated Impersonation Scams
STUDENT OFFICER:	Olivia Kwon
POSITION:	Head Chair of Human Rights Council

Introduction

The development of Artificial Intelligence (AI) has revolutionized the way in which modern communication is done. With AI, people have been able to produce advanced speech synthesis, translation, and creation of digital content, and these technologies have improved user convenience and accessibility. From these competing technologies, the one that brings particular attention is the voice cloning technology—where a person's voice is turned into a very convincing and real-sounding synthetic audio sample by AI—which shows significant potentials across industries. This method, however, is often exploited for frauds such as identity theft, financial fraud, and the spread of public misinformation, which have created widespread problems globally. As the voice cloning system becomes less expensive, more accessible, and harder to distinguish from a real human voice, the concerns surrounding such misuse have intensified with time.



AI voice cloning technology that enables synthetic speech

The growing accessibility of voice cloning has already led to a substantial rise in AI-enabled fraud. Consumers reported losing more than \$2.95 billion to impersonation scams in 2024, according to the Federal Trade Commission (FTC), highlighting the increasing financial toll of false impersonation. As artificial intelligence (AI) tools become more accessible, voice cloning can further empower these scams by allowing criminals to impersonate trusted individuals with more accuracy and credibility.

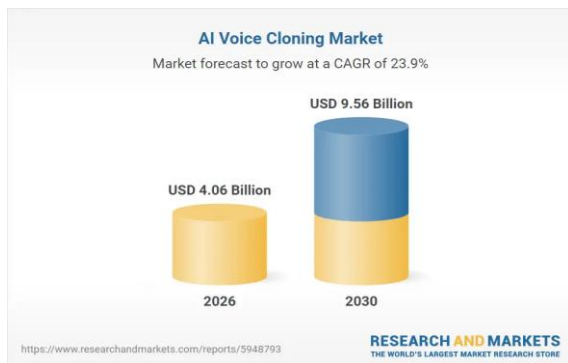
Most victims of these kinds are those of the companies that utilize audio recordings from social media to simulate a human voice. Now criminal organizations can take advantage of publicly published recordings made on various social media sites and create highly convincing synthesized voices for use in emergency scams, in financial transactions, and in any number of other deceptive communications that target both individuals and businesses. Fraud with the use of AI and financial services could become a worldwide menace as it allows for the execution of such crime from anywhere in the world (the



perpetrator, victim, bank, and IT provider could all be located in different countries), which makes it difficult for law enforcement to cooperate due to different jurisdictions. Yet, the technology also prompts more general questions about privacy, informed consent, protection of biometric data, and public confidence in digital communications.

Background

Voice cloning is a generative artificial intelligence technique for generating realistic synthetic speech from very small amounts of recorded audio. Unlike earlier text-to-text systems, modern voice cloning can mimic voices and the pitch, emotion, and cadence of expression. This technology was originally developed to be used in positive contexts, for example, assisting individuals with speech impairments, saving voices for medical purposes, and improving media production.



Estimated market growth for AI voice cloning technology

Recent advances in generative AI have significantly lowered the technical and financial barriers to producing realistic synthetic voices. With voice cloning technologies democratizing and becoming widely affordable, some people are exploiting these for maladaptive purposes. Criminals are now using AI-generated voices to pretend to be relatives, CEOs of companies, government officials or even celebrities to carry out fraud, spread misinformation or to swing public opinion. Such synthetic human voices are

increasingly indistinguishable from real humans and are being used increasingly in scams and fraud. In turn, governments and global organizations are setting up regulatory and technical safeguards. National regulators, including the U.S. Federal Trade Commission (FTC), are starting to urge AI developers to add robust safeguards against abuse. Still, regulators' approach to dealing with this type of problem is not uniformly distributed across jurisdictions, creating enforcement gaps that malicious actors can exploit.

Problems Raised

Privacy and Identity Theft

The misuse of voice cloning technology has raised significant concerns regarding privacy, consent, and the protection of biometric data. A person's voice is a unique biometric identifier that can be gathered from sources which people share online without the individual's consent. Unlike passwords or

identification numbers which are capable of changes when stolen, biometric characteristics cannot be easily modified once they are taken, , making unauthorized voice replication particularly concerning.

Many countries have not established the ownership and use of voice data. As such, individuals often lack the opportunity to receive legal protection against unauthorized voice cloning or identity theft. These challenges highlight the need for governments to consider stronger protections for biometric information while ensuring that legitimate applications of voice cloning technology remain available.

Escalating Financial Fraud

The rapid progress of AI voice cloning technology has made financial fraud more common and increasingly sophisticated. Unlike tricks that use basic phone calls or fake emails, AI voices impersonate familiar voices such as family members, company bosses, government workers, or even bank people. Through such manipulation, AI-generated voices exploit victim's trust to make convincing requests and fraudulent financial instructions.



Financial fraud remains one of the most common consequences of AI-generated voice cloning and impersonation scams

The widespread availability of voice cloning tools has further intensified this problem. Consumer Reports in 2025 tested six voice-cloning products and discovered four of them could generate convincing voice clones from publicly available audio. These four products did not have any technical mechanisms to verify that the speaker has given their consent to have their voice cloned, demonstrating how easily accessible voice-cloning technology can be misused for impersonation and fraud. In fact, criminals only need a snippet of audio, for example taken from public sources, to create convincing voice copies within minutes. These scams often have perpetrators and victims across borders, so combating AI-enabled fraud requires international cooperation. Governments, financial institutions, technology companies and law enforcement agencies across the globe must collaborate to proactively manage this escalating threat.

Misinformation and Public Trust

The concern of AI-generated voice cloning goes beyond just financial issues. Synthetic voice can produce counterfeit speeches, political endorsements, or emergency announcements, which further obscures the distinction between authentic and fake audio recordings. When the fabricated audio is published on social media, it could be misleading before it is verified to be true. A notable example occurred in January 2024, when an AI-generated robocall imitating U.S. President Joe Biden's voice was sent to New Hampshire voters and falsely encouraged them not to participate



in the presidential primary. The incident demonstrated how voice cloning can be used to interfere with political participation and spread false information at scale.

International Actions

United Nations Initiatives

The United Nations has taken note of growing concerns about artificial intelligence, including disinformation created by AI, cybercrime and impersonation online. In March 2026, the UN reiterated its commitment to developing governance norms that encourage innovation, while ensuring that AI technologies are safe and secure at the global level. In building partnerships on global AI governance, the UN aspires to partner with Member States while also protecting human rights and preventing generative AI from being misused and being used against the interests of society. An important outcome of such partnerships was the 2024 Global Digital Compact which set out common principles for international cooperation on digital technologies and AI governance. The UN has also set up the Independent International Scientific Panel on AI and the Global Dialog on AI Governance, providing forums for Member States to exchange scientific knowledge and harmonize international approaches to AI governance. However, these initiatives are mainly based on common principles and cooperation mechanisms and are not based on legally binding requirements. This means that their effectiveness depends largely on the implementation by the Member States and on their continued cooperation.

National Regulations and Consumer Protection



U.S. Senator Maggie Hassan addresses the growing threat of AI-enabled voice cloning scams

To help combat voice cloning scams enabled by AI, multiple governments have begun to put into effect policies. The US Federal Trade Commission (FTC) has warned consumers of AI voice cloning scams and encouraged tech companies to impose safeguards that prevent voices from being cloned without consent. U.S Senator Maggie Hassan urged the leading AI voice-cloning firms to strengthen identity verification procedures, improve transparency, and prevent scammers from exploiting their platforms. Meanwhile, various

countries and regional organizations are considering AI laws that are expected to make personal data regulation more responsible, transparent, and more precise.

European Union Artificial Intelligence Act



TIANMUN

In 2024, the European Union adopted the EU Artificial Intelligence Act, the first comprehensive legal framework for AI regulation at the regional level, taking a major step in regulating artificial intelligence. The Act sets different requirements depending on the risks posed by the artificial intelligence systems and introduces transparency obligations for certain AI-generated and manipulated content. Such requirements can help mitigate the risks of AI-generated impersonation by encouraging transparency about synthetic content and responsible development and use of artificial intelligence (AI) technologies. The Act demonstrates how governments can establish legally binding standards for AI, but due to its limited direct legal applicability to the European Union, it does not offer a worldwide framework to handle cross-border.



Protesters in Germany advocating for AI regulation

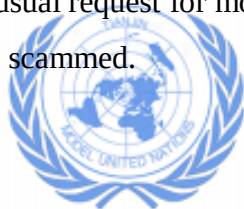
Key Players

United Nations (UN)

The United Nations has been a central player in framing AI-generated mimicry and misinformation as global issues requiring global responses. At the 2026 Global Dialogue on AI Governance, the UN stressed the need for AI to remain safe, secure, and in line with international human rights. The body advocates for collective partnerships and the formation of joint governance models to mitigate against the abuse of AI technologies for cybercrime and financial crime. Since AI fraud schemes tend to be multinational, the UN is calling on all member states to cooperate in tackling the transnational aspect of AI-facilitated crimes rather than focusing on national measures alone.

Federal Trade Commission (FTC)

The Federal Trade Commission is the primary U.S. agency with the responsibility of ensuring US consumers are not courted with unfair or deceptive trade practices. It has indeed named AI voice cloning an emerging issue for consumer protection and has cautioned that con artists “can generate believable synthetic voices based on just a few seconds of publicly available audio.” In 2024, the FTC finalized its Impersonation Rule, which strengthens the agency’s ability to take enforcement action against individuals and businesses that impersonate governments or companies through deceptive means and seek civil penalties for violations. The FTC also advises consumers to confirm on another channel if they receive an unexpected or unusual request for money and encourages AI companies to put in place protections that make it harder to get scammed.



AI Voice Cloning Companies

Platforms such as Eleven Labs, Resemble AI, Plait, Speechify, Microsoft, and OpenAI have created extremely sophisticated voice synthesis systems used in healthcare, education, entertainment and customer service. In response to some people weaponizing these tools for scams and identity theft, several companies have implemented security features such as identity verification and consent, as well



Resemble AI is a leading provider of AI voice cloning technology

as watermarking and content moderation. However, some members of the public still have questions about whether the current safeguards are effective, especially as the machine learning aids in AI tools become more realistic and accessible for a wider audience.

Possible Solutions

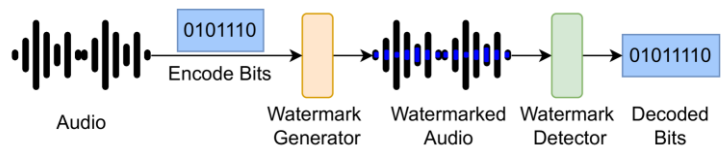
Strengthening AI Safety Measures

Governments and AI developers can work together to implement stronger safeguards within voice cloning

technologies. Safeguards may include

measures such as checking the user's identity

before permitting voice cloning use, building digital watermarks into the AI-created audio, and strengthening technologies to detect synthetic speech. These safeguards would make it harder for attackers to abuse voice cloning, while permitting its legitimate and productive uses to go on.



Audio Watermarking Scenario

Enhancing International Cooperation

Since AI-enabled frauds are usually transnational, more international cooperation is needed. Member States shall intensify the exchange of information and approximate their laws and cooperate in matters concerning cross-border investigations. Current international legal structures, like the Budapest Convention on Cybercrime, can act as a model for improving cooperation in the investigation and prosecution of AI-generated impersonation scams, especially through mechanisms for sharing electronic evidence and facilitating cross-border investigations. Greater coordination between governments, law



TIANMUN

enforcement agencies, financial institutions and technology companies will also help to detect, prevent, and prosecute AI-generated impersonation scams. This cooperation could furthermore contribute to the development of more uniform international standards regarding responsible AI use.

Glossary

Voice Cloning

The use of artificial intelligence and machine learning to create a digital replica of someone's voice.

Generative AI

Artificial intelligence designed to produce output, especially text or images, normally requiring human intelligence, typically by applying machine learning techniques to large collections of data.

Deep Fake

A video or sound recording that replaces someone's face or voice with that of someone else, in a way that appears real

Biometric Data

A process that identifies or recognizes human characteristics by scanning their physical or behavioral traits.

Water Marking

The process of embedding hidden digital markers into AI-generated content to indicate its origin and authenticity.

Identity Theft

The unauthorized use of another person's personal information or identity, often for financial or criminal purposes.

Digital Authentication

Methods used to verify the identity of users or confirm the authenticity of digital communications or content.

Sources

- “AI Voice Scams.” *defraud Prevention*TM, <https://efraudprevention.com/ai-voice.html>
- Barrington, Sarah, et al. “People Are Poorly Equipped to Detect AI-Powered Voice Clones.” *Scientific Reports*, vol. 15, no. 1, Springer Science and Business Media LLC, Mar. 2025, <https://doi.org/10.1038/s41598-025-94170-3>.
- “Consumer Federation of America Urges FTC and State Attorneys General to Investigate Speechify Over AI Voice-Cloning Practices.” *Consumer Federation of America*, 27 July 2026, <https://consumerfed.org/news/press-releases/consumer-federation-of-america-urges-ftc-and-state-attorneys-general-to-investigate-speechify-over-ai-voice-cloning-practices/>
- Consumer Reports. “Consumer Reports Assessment of AI Voice Cloning Products.” *Consumer Reports*, 13 Mar. 2025.
- Duffy, Claire. “AI ‘Voice-Cloning’ Scams Are on the Rise. Here's How to Protect Yourself.” *CNN*, 29 May 2026, <https://edition.cnn.com/2026/05/29/tech/ai-voice-cloning-scams-protect-yourself>.
- Federal Trade Commission. “Preventing Harms from AI-Enabled Voice Cloning.” *Federal Trade Commission*, 16 Nov. 2023, <https://www.ftc.gov/policy/advocacy-research/tech-at-ft/2023/11/preventing-harms-ai-enabled-voice-cloning>.
- Gedye, Grace. “New Report: Do These 6 AI Voice Cloning Companies Do Enough to Prevent Misuse?” *Innovation at Consumer Reports*, 10 Mar. 2025, <https://innovation.consumerreports.org/new-report-do-these-6-ai-voice-cloning-companies-do-enough-to-prevent-misuse/>
- Gil, Laura. “Deepfakes, voice cloning and weaponized AI: Global wake-up call to organized fraud.” *UN News*, 16 Mar. 2026, <https://news.un.org/en/story/2026/03/1167144>.
- Hartman, Elijah. “Deepfakes, Voice Cloning, and AI Impersonation: The Global Rules Are Already Here, and They Don’t Agree.” *Harris Sliwoski LLP*, 27 Apr. 2026, <https://harris-sliwoski.com/blog/deepfakes-voice-cloning-and-ai-impersonation-the-global-rules-are-already-here-and-they-don’t-agree/>
- Hassan, Maggie. “Senator Hassan Presses Leading AI Voice Cloning Companies to Prevent Exploitation by Scammers.” *Joint Economic Committee Democrats*, 16 Apr. 2026, <https://www.jec.senate.gov/public/index.cfm/democrats/2026/4/senator-hassan-presses-leading-ai-voice-cloning-companies-to-prevent-exploitation-by-scammers>.
- International AI Safety Report. *International AI Safety Report 2026*. Feb. 2026, <https://internationalaisafetyreport.org/sites/default/files/2026-02/international-ai-safety-report-2026.pdf>



TIANMUN

Naffi, Nadia. “Deepfakes and the Crisis of Knowing.” *UNESCO*, 1 Oct.

2025, <https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing>.

Ramirez, Sofia. “AI Voice Cloning Fraud Statistics 2026: Alarming Trends You Must Know Now.” *SQ Magazine*, 7 Apr. 2026, <https://sqmagazine.co.uk/ai-voice-cloning-fraud-statistics/>

“Shut Down AI Impersonation Scams.” *United Nations Federal Credit Union (UNFCU)*, <https://www.unfcu.org/financial-wellness/shut-down-ai-impersonation-scams/>

“UN Global Dialogue Opens with Urgent Call for Safe and Inclusive AI That Benefits All.” *UNESCO*, 6 July 2026, <https://www.unesco.org/en/articles/un-global-dialogue-opens-urgent-call-safe-and-inclusive-ai-benefits-all>.

“UN Global Dialogue on AI Governance.” *U.S. Mission to International Organizations in Geneva*, 8 July 2026, <https://geneva.usmission.gov/2026/07/08/un-global-dialogue-on-ai-governance/>

Vasan, Anjana. “Voice Biometrics: A Detailed Walkthrough.” *Parole*, 11 Aug. 2025, <https://www.parloa.com/knowledge-hub/voice-biometrics/>

Weeks, Jeff. “How to Protect Yourself and Your Business from AI Scams and Deepfakes.” *First National Bank of Omaha (FNBO)*, 1 July 2026, <https://www.fnbo.com/insights/fraud-and-security-tips/2026/how-to-protect-against-ai-scams-and-deepfakes>.

