



A face covered by a wireframe, which is used to create a deepfake image. Reuters TV, via Reuters

As Deepfakes Flourish, Countries Struggle With Response

Few governments have approved regulations, often because of free-speech concerns. New mandates from China could change the tone of the debate on digital forgeries.

 Give this article    120



By **Tiffany Hsu**

Jan. 22, 2023

Deepfake technology — software that allows people to swap faces, voices and other characteristics to create digital forgeries — has been used in recent years to make a synthetic substitute of Elon Musk that shilled a [cryptocurrency scam](#), to [digitally “undress”](#) more than 100,000 women on Telegram and to [steal millions of dollars](#) from companies by [mimicking their executives’ voices](#) on the phone.

In most of the world, the authorities can’t do much about it. Even as the software grows more sophisticated and accessible, few laws exist to manage its spread.

China hopes to be the exception. This month, the country adopted [expansive rules](#) requiring that manipulated material have the subject’s consent and bear digital signatures or watermarks, and that deepfake service providers offer ways to “refute rumors.”

But China faces the same hurdles that have stymied other efforts to govern deepfakes: The worst abusers of the technology tend to be the

hardest to catch, operating anonymously, adapting quickly and sharing their synthetic creations through borderless online platforms. China's move has also highlighted another reason that few countries have adopted rules: Many people worry that the government could use the rules to curtail free speech.

But simply by forging ahead with its mandates, tech experts said, Beijing could influence how other governments deal with the machine learning and artificial intelligence that power deepfake technology. With limited precedent in the field, lawmakers around the world are looking for test cases to mimic or reject.

"The A.I. scene is an interesting place for global politics, because countries are competing with one another on who's going to set the tone," said Ravit Dotan, a postdoctoral researcher who runs the Collaborative A.I. Responsibility Lab at the University of Pittsburgh. "We know that laws are coming, but we don't know what they are yet, so there's a lot of unpredictability."

Deepfakes hold great promise in many industries. Last year, the Dutch police [revived a 2003 cold case](#) by creating a digital avatar of the 13-year-old murder victim and publicizing footage of him walking through a group of his family and friends in the present day. The technology is also used for parody and satire, for online shoppers trying on clothes in virtual fitting rooms, for dynamic museum dioramas and for actors hoping to speak multiple languages in international movie releases. Researchers at the M.I.T. Media Lab and UNICEF used similar techniques to study empathy by transforming images of North American and European cities into [the battle-scarred landscapes](#) caused by the Syrian war.



Apartment rubble in Aleppo, Syria, in 2014. Salih Mahmud Leyla/Anadolu Agency, via Getty Images

Boston's Back Bay neighborhood in 2009. Greg Lyons/Flickr

Researchers at the M.I.T. Media Lab trained an artificial intelligence system with images of Aleppo and then asked it to show what other cities would look like after similar destruction. It transformed the Boston scene into this deepfake. Pinar Yanardag/M.I.T. Media Lab

But problematic applications are also plentiful. Legal experts worry that deepfakes could be misused to erode trust in surveillance videos, body cameras and other evidence. ([A doctored recording](#) submitted in a British child custody case in 2019 appeared to show a parent making violent threats, according to the parent's lawyer.) Digital forgeries could discredit or incite violence against police officers, or send them on wild goose chases. The [Department of Homeland Security](#) has also identified risks including cyberbullying, blackmail, stock manipulation and political instability.

Some experts predict that [as much as 90 percent](#) of online content could be synthetically generated within a few years.

Better Understand the Relations Between China and the U.S.

The two nations are jockeying for influence on the global stage, maneuvering for advantages on land, in the economy and in cyberspace.

- **Submarine Deal:** President Biden took his most aggressive step yet to counter China's military expansion in the Asia-Pacific region, formally unveiling plans with Britain and Australia to [develop and deploy nuclear-powered attack submarines](#).
- **Increasing Hostility:** Days after Xi Jinping [denounced](#) what he called a U.S.-led campaign of "encirclement and suppression of China," the top U.S. intelligence official [warned that Beijing is increasingly convinced](#) that it can only expand its power by diminishing American influence.
- **Industrial Espionage:** The downfall of a Chinese intelligence agent [reveals the astonishing depth of Chinese efforts](#) to steal American trade secrets and intellectual property.
- **Support for Russia:** As China sends Russia large volumes of goods that either civilians or the military could use, U.S. officials have vowed to crack down on such shipments, [but that has proved hard to police](#).

The increasing volume of deepfakes could lead to a situation where "citizens no longer have a shared reality, or could create societal confusion about which information sources are reliable; a situation sometimes referred to as 'information apocalypse' or 'reality apathy,'" the European law enforcement agency Europol [wrote in a report](#) last year.

British officials last year [cited threats](#) such as a website that "virtually strips women naked" and that was visited 38 million times in the first eight months of 2021. But [there](#) and in the [European Union](#), proposals to set guardrails for the technology have yet to become law.

Attempts in the United States to create a federal task force to examine deepfake technology have stalled. Representative Yvette D. Clarke, a New York Democrat, proposed a bill in 2019 and again in 2021 — the Defending Each and Every Person From False Appearances by Keeping Exploitation Subject to Accountability Act — that has yet to come to a vote. She said she planned to reintroduce the bill this year.

Ms. Clarke said her bill, which would require deepfakes to bear watermarks or identifying labels, was "a protective measure." By contrast, she described the new Chinese rules as "more of a control mechanism."

"Many of the sophisticated civil societies recognize how this can be weaponized and destructive," she said, adding that the United States should be bolder in setting its own standards rather than trailing another front-runner.

"We don't want the Chinese eating our lunch in the tech space at all," Ms. Clarke said. "We want to be able to set the baseline for our expectations around the tech industry, around consumer protections in that space."

But law enforcement officials [have said](#) the industry is still unable to detect deepfakes and struggles to manage malicious uses of the technology. A lawyer in California [wrote in a law journal](#) in 2021 that certain deepfake rules had “an almost insurmountable feasibility problem” and were “functionally unenforceable” because (usually anonymous) abusers can easily cover their tracks.

The rules that do exist in the United States are largely aimed at political or pornographic deepfakes. Marc Berman, a Democrat in California’s State Assembly who represents parts of Silicon Valley and has sponsored such legislation, said he was unaware of any efforts to enforce his laws via lawsuits or fines. But he said that, in deference to one of his laws, a deepfaking app had removed the ability to mimic President Donald J. Trump before the 2020 election.

Only a handful of other states, including New York, restrict deepfake pornography. While running for re-election in 2019, Houston’s mayor said a critical ad from a fellow candidate [broke a Texas law](#) that bans certain misleading political deepfakes.

“Half of the value is causing more people to be a little bit more skeptical about what they’re seeing on a social media platforms and encourage folks not to take everything at face value,” Mr. Berman said.

Representative Peter Welch, Democrat of Vermont, during a hearing on deepfakes in 2019. Chip Somodevilla/Getty Images

But even as technology experts, lawmakers and victims call for stronger protections, they also urge caution. Deepfake laws, they said, risk being both overreaching but also toothless. Forcing labels or disclaimers onto deepfakes designed as valid commentary on politics or culture could also make the content appear less trustworthy, they added.

Digital rights groups such as the Electronic Frontier Foundation are pushing legislators to relinquish deepfake policing to tech companies, or to use an existing legal framework that addresses issues such as fraud, copyright infringement, obscenity and defamation.

“That’s the best remedy against harms, rather than the governmental interference, which in its implementation is almost always going to capture material that is not harmful, that chills people from legitimate, productive speech,” said David Greene, a civil liberties lawyer for the Electronic Frontier Foundation.

[Several months ago](#), Google began prohibiting people from using its Colaboratory platform, a data analysis tool, to train A.I. systems to generate deepfakes. In the fall, the company behind Stable Diffusion, an image-generating tool, launched an update that hamstrings users trying to create nude and pornographic content, [according to The Verge](#). Meta, TikTok, YouTube and Reddit ban deepfakes that are intended to be misleading.

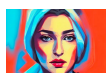
But laws or bans may struggle to contain a technology that is designed to continually adapt and improve. Last year, researchers from the RAND Corporation demonstrated how difficult deepfakes can be to identify when they showed a set of videos to more than 3,000 test subjects and asked them to identify the ones that were manipulated (such as a deepfake of the climate activist Greta Thunberg disavowing the existence of climate change).

[The group was wrong](#) more than a third of the time. Even a subset of several dozen students studying machine learning at Carnegie Mellon University were wrong more than 20 percent of the time.

Initiatives from companies such as Microsoft and Adobe now try to authenticate media and train moderation technology to recognize the inconsistencies that mark synthetic content. But they are in a constant struggle to outpace deepfake creators who often discover new ways to fix defects, remove watermarks and alter metadata to cover their tracks.

“There is a technological arms race between deepfake creators and deepfake detectors,” said Jared Mondschein, a physical scientist at RAND. “Until we start coming up with ways to better detect deepfakes, it’ll be really hard for any amount of legislation to have any teeth.”

Eyes Deceive Us



How Is Everyone Making Those A.I. Selfies?
Dec. 7, 2022



Worries Grow That TikTok Is New Home for Manipulated Video and Photos
Nov. 4, 2022



We Need to Talk About How Good A.I. Is Getting
Aug. 24, 2022



A.I. Is Becoming More Conversational. But Will It Get More Honest?
Jan. 10, 2023

Tiffany Hsu is a tech reporter covering misinformation and disinformation. [@tiffkhsu](#)

A version of this article appears in print on Jan. 23, 2023, Section B, Page 1 of the New York edition with the headline: As Deepfakes Proliferate, Nations Struggle to React. [Order Reprints](#) | [Today's Paper](#) | [Subscribe](#)

READ 120 COMMENTS



Give this article



120

More in Media ›

Your Annoying Roommate Is Slaying on TikTok

‘Hi, This Is Oprah Winfrey. I Read Your Novel and Loved It So Much.’

5 Times Tucker Carlson Privately Reviled Trump: ‘I Hate Him’

Politico’s Executive Editor Steps Down After a Year in the Job

Records Show Fox and G.O.P.’s Shared Quandary: Trump

Lachlan Murdoch Defends Fox News’s Chief Executive Amid Defamation Suit

Editors’ Picks

Kids Love These Recipes!

This Dress Survived for More Than Three Centuries at the Bottom of the Sea

Red Beans and Rice Feed New Orleans’ Soul

Most Popular

How Much Skin Should I Show Under a Sheer Dress?

The Trump Juror Who Got Under America’s Skin

A 1,600-Year-Old Coffin May Shed Light on Roman Britain

Pro Golfers Are Hitting Balls Way Too Far. Some Say It Has to Stop.

A Giant Blob of Seaweed is Heading to Florida

Opinion: It’s a Spectacular Scandal, and a Warning to Europe

Clinton, N.J.: A ‘Small but Elegant’ Town With Friendly People

A Mossad Agent’s Treasure Trove of Photos

To Fall in Love With Cabbage, Do This

Inside Vanity Fair’s Oscar Party: Every Star, All at Once

The New York Times

[Go to Home Page »](#)

© 2023 The New York Times Company

[NYTCo](#) [Contact Us](#) [Accessibility](#) [Work with us](#) [Advertise](#) [T Brand Studio](#) [Your Ad Choices](#) [Privacy Policy](#) [Terms of Service](#) [Terms of Sale](#) [Site Map](#) [Help](#) [Subscriptions](#)
[Do Not Sell/Share My Personal Information](#) [California Notices](#) [Limit the Use of My Sensitive Information](#)

