New American

Written by **Angeline Tan** on December 14, 2022

China's Rules for "Deepfake" Technology to Take Effect Jan. 10

FotografieLink/iStock/Getty Images Plus

China's new regulations for content providers that modify facial and voice data will be enforced beginning January 10, as the country seeks to tightly monitor so-called deepfake, or deep synthesis, technology and services.

The Cyberspace Administration of China (CAC) published regulations December 11 to safeguard people from being impersonated without their consent by deepfakes. A deepfake is a digital, AI-generated representation of someone or something that very closely mimics the original, and can readily be used to manipulate or misinform others.

The CAC said the regulations were meant to curtail risks that might result from activities on platforms that use deep learning or virtual reality to adjust any online content. The CAC termed such platforms as "deep synthesis service providers."

Earlier in January 2022, China's cyberspace regulator issued draft rules for content providers that amend facial and voice data to fashion a cyberspace that endorses Chinese socialist values.

Documents published on the website of the CAC indicate that the rules would regulate technologies such as those using algorithms to produce and modify text, audio, images, and videos.

Any platform or company that uses deep learning or virtual reality to alter any online content would be expected to "respect social morality and ethics, adhere to the correct political direction."

"Where a deep synthesis service provider provides significant editing functions for biometric information such as face and human voice, it shall prompt the (provider) to notify and obtain the individual consent of the subject whose personal information is being edited," Article 12 of the draft stated.

The rules stipulate fines of between 10,000 and 100,000 yuan ($1,439 to $14,399) for first-time offenders, but violations can also result in civil and criminal prosecutions.

Moreover, the rules ensure a user complaints system and mechanisms to pre-empt deepfakes from being used to spread misinformation. App stores will be mandated to suspend or block providers of deepfake technology if necessary.

"Deep synthesis services are also used by some criminals to produce, copy, publish and disseminate illegal information; slander and degrade people's reputation, honor; as well as impersonating others' identities to commit fraud and other illegal acts — not only damaging the vital interests of the people, but even endangering national security and social stability," the rules stated.

"It is urgent to delineate 'bottom lines' and 'red lines.'"

In the increasingly digitized cyberworld in which we now live, the ordinary man on the street is largely unable to manage such deep power and potential for abuse.

The tools used to generate deepfakes have become more powerful and prevalent in recent years. These tools have also become more accessible online since 2020, sparking worries among analysts who study the role of technology in misinformation.

For example, deepfake creators and enthusiasts are posting their pre-trained AI models on online forums, enabling other users without much technical skills to download one and use it in their own videos in hours.

Without a pre-trained model, it could take days or even weeks of processing time to train one from scratch and produce a convincing fake face.

According to AI specialist Professor Terence Sim of the National University of Singapore's (NUS) School of Computing, deepfake technology has already advanced to the level where a skilled deepfake maker can generate images that are highly convincing and likely to deceive huge populations.

The professor, who researches deepfakes and other types of digitally altered images at the NUS Centre for Trusted Internet and Community (CTIC), remarked that people can be less vigilant and thus be easily deceived in various situations, such as during election campaigns.

"You could be in the midst of an election, where all the candidates are campaigning and certain words are being twisted deliberately, maliciously," Sim said.

In the near future, such technology may even be used to manipulate other types of images, such as a person's full body, inanimate objects, or parts of the environment, Sim added. After all, AI and machine-learning algorithms used to produce deepfakes are "agnostic" about the type of media they are fed.

What this means is that future deepfake creators may be able to transform a video of a person tearing apart a document into one of the person damaging an important artifact. The video could then provoke strong feelings and have serious ramifications.

"The barriers to entry are definitely much lower and the threat is real, so we do have to be watchful," Sim cautioned.

Dr. Maria Teresa Soto-Sanfiel, principal researcher at the CTIC, believes the technology might develop to the point where even trained experts could be deceived in as short as a decade's time.

Moreover, the spread and prevalence of deepfakes, let alone their mere existence, could erode public trust.

Dr. Soto-Sanfiel noted that people may begin to have misgivings about video messages from politicians, for example, even if these videos are authentic.

Such a skeptical mindset has already morphed into online theories such as those linked to Chinese athlete Peng Shuai and actor Zhang Zhehan.

Netizens online have speculated about whether Peng or Zhang's social-media photos and videos really depict them or whether they have actually "disappeared" and been replaced by deepfakes.

Harvard Business School professor Shoshana Zuboff's book *The Age Of Surveillance Capitalism* — the title of which aptly portrays the deep dark waters we have entered — covers the advancements of social-media and artificial intelligence technologies, their dangers, and solutions to using them.

In the book, Zuboff defined surveillance capitalism as the use of tools to garner data on individuals to influence future consumer behavioral decisions. The tools use “machine intelligence” to generate “prediction products” for future markets.

“Surveillance capitalism,” Zuboff wrote, “unilaterally claims human experience as free raw material for translation into behavioral data. Although some of these data are applied to service improvement, the rest are declared as a proprietary behavioral surplus, fed into advanced manufacturing processes known as ‘machine intelligence’, and fabricated into prediction products that anticipate what you will do now, soon and later. Finally, these prediction products are traded in a new kind of marketplace that I call behavioral futures markets. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are willing to lay bets on our future behavior.”

While artificial algorithms may seem to benefit users, Zuboff posits that the tools of surveillance capitalism insidiously mine users’ data to direct users’ future behavior. Zuboff casts aspersions on Big Tech’s ability to respect individual privacy, given that one such giant, Google, has this as a mantra: “To organize the world’s information and make it universally accessible and useful.”