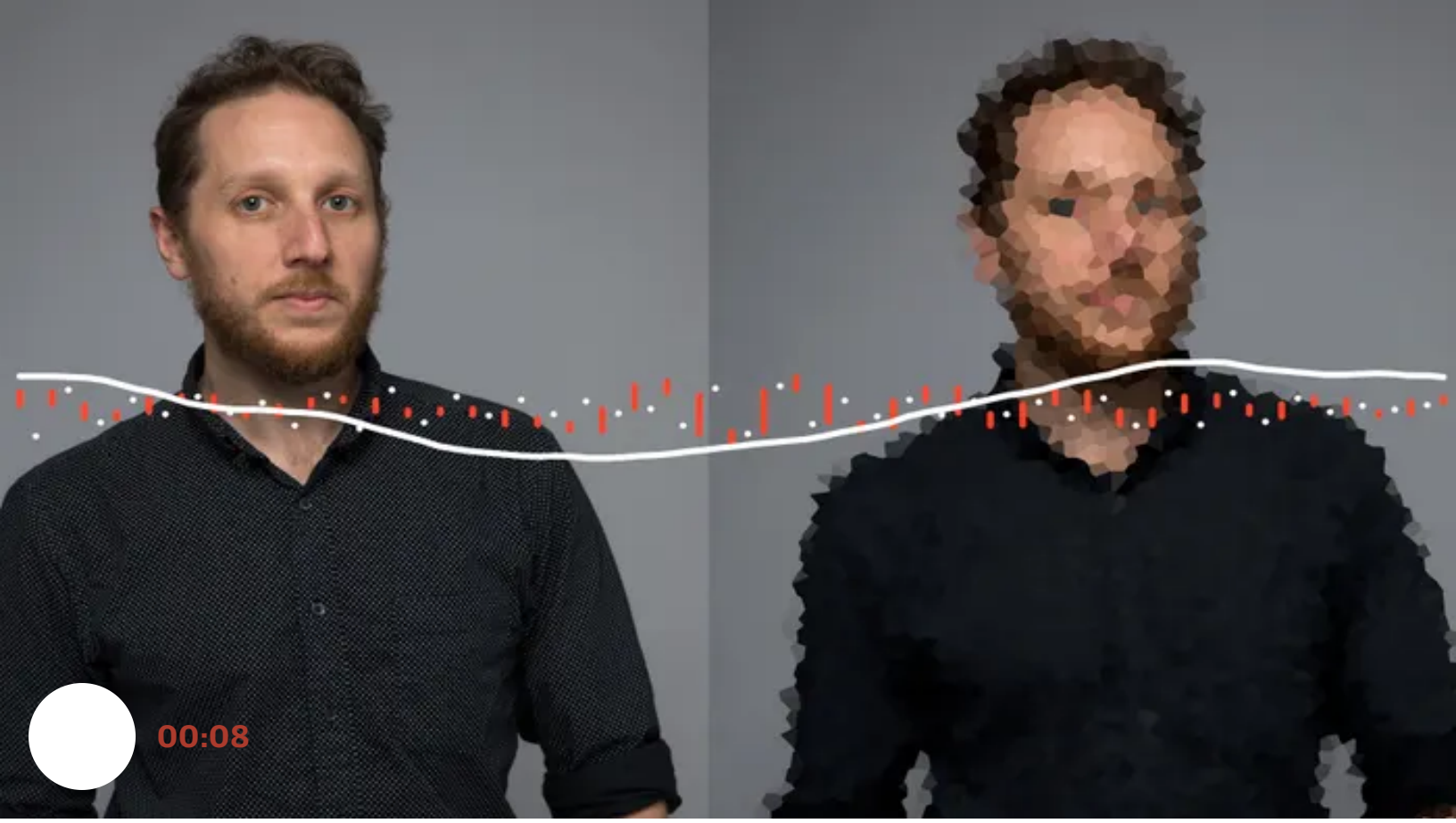

Can you tell the difference between Guardian journalist's voice and an AI-generated 'clone'? – audio

Artificial intelligence (AI)

AI can fool voice recognition used to verify identity by Centrelink and Australian tax office

Exclusive: Voiceprint program used by millions of Australians to access data held by government agencies shown to have a serious security flaw

Nick Evershed *and* Josh Taylor

Thu 16 Mar 2023 10.00 EDT

A voice identification system used by the Australian government for millions of people has a serious security flaw, a Guardian Australia investigation has found.

Centrelink and the Australian Taxation Office (ATO) both give people the option of using a "voiceprint", along with other information, to verify their identity over the phone, allowing them to then access sensitive information from their accounts.

But following reports that an AI-generated voice trained to sound like a specific person could be used to access phone-banking services overseas, Guardian Australia has confirmed that the voiceprint system can also be fooled by an AI-generated voice.

Using just four minutes of audio, a Guardian Australia journalist was able to generate a clone of their own voice and was then able to use this, combined with their customer reference number, to gain access to their own Centrelink self-service account.

The voiceprint service, described as the "digital representation of the sound, rhythm, physical characteristics and patterns of your voice", was used by 3.8 million Centrelink clients as of the end of February, and more than 7.1 million people had verified their voice with the ATO.

Services Australia, the department that oversees Centrelink, says on its website the service is "secure, accurate and reliable".

"It's very difficult for someone to access your personal information. The system can tell when someone is pretending to be you or using a recording of your voice. We won't give them access to your details."

Anyone trying to use voiceprint also needs to know the account-holder's customer reference number, which is not normally publicly available, but the number is not treated as securely as a password and is included in correspondence from Centrelink and other service providers, such as childcare centres.

The self-service phone system allows people to access sensitive material such as information on their payment of benefits and to request documents to be sent by mail, including replacement concession or healthcare cards.

When Guardian Australia contacted Services Australia with details of the security vulnerability, it declined to say if the voiceprint technology would be changed or removed from Centrelink.

A spokesperson, Hank Jongen, said Services Australia "has the capacity to continually assess risks and update processes accordingly" and that voice ID is a "highly secure authentication method" used by Centrelink.

"We continually scan for potential threats and make ongoing enhancements to ensure customer security," he said.

"If we identify unusual circumstances in how customers use our authentication systems, we apply additional tests to confirm a caller's identity."

Centrelink's self-service phone line uses voiceprint in an automated system in lieu of a password, but the ATO and at least one Australian bank - Bank Australia - offer voiceprint as an option during conversations with staff to reduce the need for verification questions. This may be less vulnerable to exploitation by AI-generated voice software as it is more difficult to respond with high-quality responses in real time, but the technology to do so is steadily improving.

Toby Walsh, the chief scientist at the University of New South Wales' AI Institute, told Guardian Australia he was able to clone his own voice within five minutes, and the ease with which AI could bypass biometric identification showed its limits as a security tool. Walsh did not use the cloned voice to test access to any services.

"I think the basic lesson here is that biometrics is not going to save us from the hassle we have today with passwords and two-factor authentication," he said.

"If you've contacted the person by multiple routes - through their phone or internet account - then you have some confidence that the person is [who they say they are], but just seeing their face or hearing their voice is not going to be enough."

Ed Santow, a former human rights commissioner and now director of policy at the Human Technology Institute at the University of Technology Sydney, said government agencies using biometrics as a form of verification needed to ensure they had the best systems in place, and that there was legislation underpinning those systems.

"It needs really clear legislation to make sure that the guardrails are in place from the government perspective, [as well as] basic standards," he said. "So that the government agency

is only using technology when it is safe and reliable, and is not going to be subjected to misuse and cybercrime."

A spokesperson for the ATO said the agency had robust measures in place to protect the system from threats including AI voice cloning.

"The ATO actively scans for potential vulnerabilities and enhances its system as required to ensure the security and protection of ATO client data, and appropriate controls are embedded in the digital services we offer to the Australian community."

A spokesperson for Bank Australia said the bank worked "closely with our technology partners to regularly monitor and continuously improve our systems to ensure that we stay ahead of new threats, including those posed by emerging AI and machine learning tools".

Nuance, the company whose technology is used for the voiceprint service, did not specifically address questions about the vulnerability, but directed Guardian Australia to a blog post from February, in which it addressed the issue of "synthetic voices".

In the blog post, the company outlined its efforts to detect synthetic voices, and claimed its latest technology could accurately detect and flag the use of cloned voices in 86% to 99% of cases, depending on the technology used.

"At Nuance, we know we can't rest on our laurels, and fraudsters will continually look for ways to get around our security technologies. That's why we devote a huge amount of R&D effort into anticipating criminals' next steps and constantly staying one step ahead," the post said.

Voice cloning, a relatively new technology using machine learning, is offered by a number of apps and websites either free or for a small fee, and a voice model can be created with only a handful of recordings of a person.

While the voice generated is better with high-quality recordings, anyone with public recordings of themselves on social media, or who has been recorded elsewhere, could be vulnerable to having their voice reproduced.

---

everything we do, we know there is a right and a wrong position in the fight against racism and for reproductive justice. When we report on issues like the climate crisis, we're not afraid to name who is responsible. And as a global news organization, we're able to provide a fresh, outsider perspective on US politics - one so often missing from the insular American media bubble.

Around the world, readers can access the Guardian's paywall-free journalism because of our unique reader-supported model. That's because of people like you. Our readers keep us independent, beholden to no outside influence and accessible to everyone - whether they can afford to pay for news, or not.

If you can, please consider supporting the Guardian today. Thank you.

Betsy Reed
Editor, Guardian US

Most viewed