



BETA ABOUT (/ABOUT)

THE

CHANNELS



AMERICAS (/TOPIC/AMERICAS)

The Growing Use of 'Voiceprint' Passwords Is Another Threat to Your Privacy

f Share t Tweet -

t g+ i e

By John Dyer (/contributor/john-dyer)

October 13, 2014 | 5:35 pm

Electronic snoops are increasingly treating our voices like fingerprints — traces of ourselves we unwittingly leave all over the place, often on other people's property where anyone with enough know-how can collect it.

The Associated Press (http://hosted.ap.org/dynamic/stories/E/EU_THE_VOICE_HARVESTERS_GROWING_USES?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT) reported today that governments and corporations around the world have compiled at least 65 million so-called voiceprints in databases used for security, surveillance, and commerce.

For now, at least, voiceprint technology appears mostly benign. South Africa uses 7 million voice recordings to verify the identities of



(<https://news.vice.com/article/the-growing-use-of-voiceprint-passwords-i...>)
claiming their benefits, the AP reported. Then, the Pennsylvania-based Vanguard Group investment firm prevents fraudsters from accessing tens of thousands of accounts by asking customers to say, "At Vanguard, my voice is my password," when they call into the company's system.



The use of voiceprints — one of many biometrics that include fingerprints, and face and iris recognition — is trending upwards, too. The AP reported that the voice recognition industry earned less than \$400 million last year but could generate as much as \$900 billion in revenues in 2015.

The DEA is using Facebook to bust drug dealers and is now getting sued for it. Read more here. (<https://news.vice.com/article/the-dea-is-using-facebook-to-bust-drug-dealers-and-is-now-getting-sued-for-it>)

But tech experts and civil rights advocates caution that voiceprints could represent the worst of both worlds when it comes to digital safety: they might not work and they'll surely compromise peoples' privacy.

Radu Sion, an associate professor of Computer Science at Stony Brook University, told VICE News there's little hope of keeping others from recording and analyzing our voices.

Phone conversations, whether by landline or cell phone, routinely involve a handful of different companies and jurisdictions, so we should never assume our conversations are 100 percent private, he said. "We lost that war the moment the phone became digital in the 1970s," Sion added.

'Using biometrics as a single means of authentication is a terrible idea.'

But the ubiquitousness of our voices is precisely why South Africa, Vanguard, and others shouldn't depend on them too heavily for security, he continued.

Passwords work well because people can change them. We can't change our voices, however, or at least not enough to fool technology that can identify people even when they have a cold or other throat ailment. So anyone who takes the time to record someone else's voice could conceivably impersonate them.

"Using biometrics as a single means of authentication is a terrible idea," Sion said.

In theory — even if it's the National Security Agency eavesdropping on a foreign call — authorities need to obtain warrants before listening in on phone conversations. Yet it's not clear if people enjoy any legal privacy protections when it comes to analyzing the bits and bytes of those chats, Sion added.

"I can record 20 separate syllables from 20 different conversations during calls to reconstitute how you say a certain phrase, but the phrase has absolutely nothing to do with any of those calls," he said. "Is that recording your call or recording a speech pattern?"

Chicago's high-tech surveillance experiment brings privacy fears. Read more here. (<https://news.vice.com/article/chicago-high-tech-surveillance-experiment-brings-privacy-fears>)

Jay Stanley, a senior policy analyst at the American Civil Liberties Union, wondered whether voice recognition would scare off anonymous whistleblowers who call the police to report crimes in progress, warn government inspectors about official malfeasance, and tip off journalists.

Stanley also questioned whether our voices might someday become more grist for the vast marketing machine that now targets advertisements based on the words folks type online. Could the same occur based on words shared during a conversation in public?

"It's the same issue as the mass collection of data — demographic information is bought and sold on a daily basis," he told VICE News. "It's pretty much the Wild West. It's a problem that we're facing. Voiceprints might become valuable in the future in ways we don't anticipate."

Follow John Dyer on Twitter: [@johnjdyerjr](https://twitter.com/johnjdyerjr) (<https://twitter.com/johnjdyerjr>)