The Value of Privacy More in this Business Report »

Wiping Away Your Siri "Fingerprint"

Your voice can be a biometric identifier, like your fingerprint. Does Apple really have to store it on its own servers?

3 comments

DAVID TALBOT
Thursday, June 28, 2012

istock | blankaboskov

Even in an age of vanishing privacy, people using Apple's digital assistant Siri share a distinct concern. Recordings of their actual voices, asking questions that might be personal, travel over the Internet to a remote Apple server for processing. Then they remain stored there; Apple won't say for how long.

That voice recording, unlike most of the data produced by smart phones and other computers, is an actual biometric identifier. A voiceprint—if disclosed by accident, hack, or subpoena—can be linked to a specific person. And with the current boom in speech recognition apps, Apple isn't the only one amassing such data.

There may be a way to keep this identifier more private. Researchers say Apple and others developing voice recognition applications like Siri could do part of the data processing right on the phone. Then, instead of sending out the full recording, they could transmit specific information that is harder to definitively link to an individual.

"Maybe anything that IDs you should stay on the phone," says Prem Natarajan, executive vice president at Raytheon BBN Technologies in Cambridge, Massachusetts, a major center for speech recognition research. He says it might be wiser for Apple to "transmit features from speech—and not the speech itself."

More in this Business Report

High Stakes in Internet Tracking
17 comments

The Curious Case of Internet Privacy
45 comments

A Dollar For Your Data
3 comments

Keeping Things Private at Microsoft
4 comments

More from this Business Report:
The Value of Privacy »

Technology Review Lists

Technologies **Innovators** **Companies**

TR10 Our list of the 10 most innovative technologies of 2012. See list »

Egg Stem Cells

A recent discovery could

While this approach would put more burden on the phone's processor and battery, it wouldn't hurt the quality of the speech recognition. "I think it is safe to say that not having access to the [full voice] signal does not impose any meaningful penalty," Natarajan says. Limiting the amount of biometric data that gets shared would follow the example of devices such as Microsoft's Kinect, which for privacy reasons have been engineered to keep such data onboard.

Trudy Muller, an Apple spokeswoman, confirmed that voice recordings are stored when users ask a spoken question like "What's the weather now?" "This data is only used for Siri's operation and to help Siri improve its understanding and recognition," she said. Muller added that the company takes privacy "very seriously," noting that questions and responses that Siri sends over the Internet are encrypted, and that recordings of your voice are not linked to other information Apple has generated about you. (Siri does upload your contact list, location, and list of stored songs, though, to help it respond to your requests.)

While voiceprints are not as unique as fingerprints, they can positively identify the speaker in many circumstances. The U.S. Department of Homeland Security uses voiceprints to identify frequent travelers who have enrolled in a system to allow speedy border crossings.

To see why voiceprints could matter, consider the murder trial of Casey Anthony, the Florida mother acquitted last year in the death of her two-year-old daughter, Caylee. At one point prosecutors pointed to Internet searches—for "chloroform" and other incriminating terms—made from the accused's computer. Anthony's mother testified to having typed in the search term herself, as a misspelling of "chlorophyll." If the searches had been made by voice on Siri, it might have been possible for prosecutors—and jurors—to determine who actually said "chloroform." (Apple declined to say whether it has ever received a subpoena for anyone's voiceprint.)

Meanwhile, if you dictated an inappropriate text or asked Siri about a sensitive medical matter and Apple got hacked (or a malicious employee released data), not only would the embarrassing communication be released, but it would be in your own voice. Natarajan says biometrics could raise entirely new privacy questions. For example, someone searching for the location of a protest against a repressive regime could be in trouble if the data became available to that government. "If you have a group of people asking about protests, you now unfortunately have voice biometrics for those people," he says.

Some observers, including large technology firms, are raising broader questions about Siri. Last month *Technology Review* reported that IBM had asked its employees not to use the feature, a decision IBM said was motivated by the need to protect contact lists and other sensitive company information. It's a concern that other organizations should share, some experts believe. "If I were to run an intelligence agency or a large corporation, I would not allow such a service in-house," says Radu Sion, a computer scientist at Stony Brook University and a leading researcher on cloud computing security.

Siri's voice recognition works like this: you speak a question or request, and the voice recording is sent to an Apple server. There, the recording is broken down in a process called feature extraction, which numerically transforms the sound wave and pulls out relevant features. These are run through a speech recognition engine to interpret what you are saying and render it into text. Siri then uses resources that may include the Internet, your contact list ("Call Dad"), or your location ("Where is the nearest Thai food?") to respond to your need.

There is no reason why the initial job of feature extraction couldn't be done directly on the phone so that some elements could stay there. Pitch pattern, for example, is important for identifying the speaker but not for recognizing what was said. From a technology perspective, "you could send out the stuff the recognizer is going to work on, but not the full waveform," Natarajan says. While this might not be a perfect solution, he says, "it would meaningfully improve privacy—and, perhaps more importantly, the perception of privacy, because you can't reconstruct the voice signal from the features."

James Glass, a senior research scientist at MIT and head of its Spoken Language Systems group, says that onboard processing, also known as distributed speech recognition, has been studied extensively. It doesn't offer complete protection, he cautions: "Biometric

increase older women's chances of having babies.

Read more »

Explore our TR10 List:

the data, if that was your goal."

He adds that the easiest way to anonymize a voiceprint is to disassociate the recordings from other data, like the cell-phone number. "It would mean that it would be harder for systems to personalize to your voice and queries, but some people might prefer that option if it gave them more privacy," he says. "This is the position I would advocate for, as it is similar to how some apps ask permission to use your location right now."

As more voice applications crop up in more settings, protecting biometric identifiers will become more important, says Andrew Sudbury, cofounder of Abine, an online privacy software company in Boston that helps consumers block tracking of their online activities. "It's really almost a watershed moment, in that this is going to herald a very rapid rise of voice recognition being used in lots of places," he says. "And it will get easier to do a fairly good job of identifying people through their voice."

Indeed, one reason Apple might want to store full voiceprints is to retain the option of providing such services. In theory, a speech recognizer could know that it's you talking, not your spouse or child, and give you personally tailored answers. "It would be pretty cool if you called in from a different phone and they could identify you," Natarajan says.

A vast database of people's actual voices is what would make this possible. Such features are still speculative, he cautions. But "all innovation is about doing things that nobody is planning right now," he says. "I, too, would want access to all of that data."

Business, Business Impact, Privacy

David Talbot

Chief Correspondent
I'm *Technology Review*'s chief correspondent, keeping an eye most often on the world of information and communication technologies—and asking my kids when I don't...
See full bio »

PART OF OUR BUSINESS REPORT:

The Value of Privacy

Internet advertising is the global $70 billion business that powers services like Google and Facebook. But has tracking of Web users gone too far?

MORE FROM THIS REPORT

- **High Stakes in Internet Tracking**
- **The Curious Case of Internet Privacy**
- **A Dollar For Your Data**

see 10 more »

Related Articles:

The FTC's Privacy Cop Cracks Down

Jessica Leber

Privacy Laws Turn Europe into Economic Laboratory

Lucas Laursen

Ad Men and Browser Geeks Collide Over Web Protocols

Tom Simonite