Forget About Siri And Alexa – The 'NSA Reigns Supreme' in Voice Identification

Why are listening sensors being installed in light poles, bus stops and cameras all over smart cities? "As soon as you can identify someone's voice, you can immediately find them whenever they're having a conversation.." Technocrats rely on total surveillance for comprehensive social engineering of the entire population. TN Editor

At the height of the Cold War, during the winter of 1980, FBI agents recorded a phone call in which a man arranged a secret meeting with the Soviet embassy in Washington, D.C. On the day of his appointment, however, agents were unable to catch sight of the man entering the embassy. At the time, they had no way to put a name to the caller from just the sound of his voice, so the spy remained anonymous. Over the next five years, he sold details about several secret U.S. programs to the USSR.

It wasn't until 1985 that the FBI, thanks to intelligence provided by a Russian defector, was able to establish the caller as Ronald Pelton, a former analyst at the National Security Agency. The next year, Pelton was convicted of espionage.

Today, FBI and NSA agents would have identified Pelton within seconds of his first call to the Soviets. A classified NSA memo from January 2006 describes NSA analysts using a "technology that identifies people by the sound of their voices" to successfully match old audio files of Pelton to one another. "Had such technologies been available twenty years ago," the memo stated, "early detection and apprehension could have been possible, reducing the considerable damage Pelton did to national security."

These and other classified documents provided by former NSA contractor Edward Snowden reveal that the NSA has developed technology not just to record and transcribe private conversations but to automatically identify the speakers.

Americans most regularly encounter this technology, known as speaker recognition, or speaker identification, when they wake up Amazon's Alexa or call their bank. But a decade before voice commands like "Hello Siri" and "OK Google" became common household phrases, the NSA was using speaker recognition to monitor terrorists, politicians, drug lords, spies, and even agency employees.

The technology works by analyzing the physical and behavioral features that make each person's voice distinctive, such as the pitch, shape of the mouth, and length of the larynx. An algorithm then creates a dynamic computer model of the individual's vocal characteristics. This is what's popularly referred to as a "voiceprint." The entire process — capturing a few spoken words, turning those words into a voiceprint, and comparing that representation to other "voiceprints" already stored in the database — can happen almost instantaneously. Although the NSA is known to rely on finger and face prints to identify targets, voiceprints, according to a 2008 agency document, are "where NSA reigns supreme."

It's not difficult to see why. By intercepting and recording millions of

overseas telephone conversations, video teleconferences, and internet calls — in addition to capturing, with or without warrants, the domestic conversations of Americans — the NSA has built an unrivaled collection of distinct voices. Documents from the Snowden archive reveal that analysts fed some of these recordings to speaker recognition algorithms that could connect individuals to their past utterances, even when they had used unknown phone numbers, secret code words, or multiple languages.

As early as Operation Iraqi Freedom, analysts were using speaker recognition to verify that audio which "appeared to be of deposed leader Saddam Hussein was indeed his, contrary to prevalent beliefs." Memos further show that NSA analysts created voiceprints for Osama bin Laden, whose voice was "unmistakable and remarkably consistent across several transmissions;" for Ayman al-Zawahri, Al Qaeda's current leader; and for Abu Musab al-Zarqawi, then the group's third in command. They used Zarqawi's voiceprint to identify him as the speaker in audio files posted online.

The classified documents, dating from 2004 to 2012, show the NSA refining increasingly sophisticated iterations of its speaker recognition technology. They confirm the uses of speaker recognition in counterterrorism operations and overseas drug busts. And they suggest that the agency planned to deploy the technology not just to retroactively identify spies like Pelton but to prevent whistleblowers like Snowden.

Always Listening

Civil liberty experts are worried that these and other expanding uses of speaker recognition imperil the right to privacy. "This creates a new intelligence capability and a new capability for abuse," explained Timothy Edgar, a former White House adviser to the Director of National Intelligence. "Our voice is traveling across all sorts of communication channels where we're not there. In an age of mass surveillance, this kind of capability has profound implications for all of our privacy."

Edgar and other experts pointed to the relatively stable nature of the

human voice, which is far more difficult to change or disguise than a name, address, password, phone number, or PIN. This makes it “far easier” to track people, according to Jamie Williams, an attorney with the Electronic Frontier Foundation. “As soon as you can identify someone’s voice,” she said, “you can immediately find them whenever they’re having a conversation, assuming you are recording or listening to it.”

The voice is a unique and readily accessible biometric: Unlike DNA, it can be collected passively and from a great distance, without a subject’s knowledge or consent. Accuracy varies considerably depending on how closely the conditions of the collected voice match those of previous recordings. But in controlled settings — with low background noise, a familiar acoustic environment, and good signal quality — the technology can use a few spoken sentences to precisely match individuals. And the more samples of a given voice that are fed into the computer’s model, the stronger and more “mature” that model becomes.

Read full story here…