NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

How our voices age

Brett Beranek | Vice President & General Manager, Security & Biometrics

January 26, 2017

Voice biometrics has been embraced by hundreds of organizations, and millions of consumers around the globe as a more convenient and secure method of authentication for customer service. It not only improves security and customer experience, but it boosts efficiency within an organization as well. Given the complexity of the human voice and how much it seemingly changes as we age (to the human ear), it may seem that a person's ability to use a voice biometrics system might also change or their voice might "degrade" over time. It turns out that age matters very little to a voice biometrics system – whether you are 25, 45, 65 or 85.

One of the anxieties that I've often heard expressed regarding voice biometrics is how does the technology account for the natural aging of our voice? Through our personal experience, we all know that the voice we had as a child is quite different from the voice we now have as an adult. Fortunately, as I'll demonstrate with a series of examples, voice biometrics is quite indifferent to the age of our voice!

To prove this point, I performed several tests using the voices of well know actors that have a wealth of voice recordings available in the public domain. In full disclosure, to perform these tests I had to disable Nuance's standard playback detection algorithms in our voice biometric system.

The first test that I conducted involves my childhood action movie idol, Arnold Schwarzenegger. The Austrian-born star of the Terminator film series, who would later become the governor of California, has an instantly recognizable voice. Our very own brain-powered voice biometric engines can easily identify his voice, whether we are listening to a rerun of the 1984 movie *Terminator*, or a recent interview featuring Mr. Schwarzenegger. So, given this, how does a voice biometric engine perform? To find out I

enrolled 40 seconds of his voice from an interview Mr. Schwarzenegger delivered in 2015 that was available on YouTube. I then ran a voice biometric check on three seconds of Mr. Schwarzenegger's voice from the movie *Pumping Iron* from 1977 that was also available on YouTube. Despite a 38-year difference between these two recordings, the voice biometric engine had no trouble recognizing that this was the same person, at banking-grade security settings.

Now this first test was very favorable, because even though there was a 38-year difference between the two clips, in both cases Mr. Schwarzenegger was in his adult years in which the voice changes very little. When *Pumping Iron* was filmed, Mr. Schwarzenegger was 30 years old, and in 2015 when the interview was recorded he was 68.

The real challenge is how will voice biometrics perform during the two periods of our lives when our voices change more rapidly, which are during our teenage years and during the latter years of our adult lives.

To explore this question, I performed a voice biometrics test with another famous actor whose voice is instantly recognizable as well, Morgan Freeman. Born in 1937, Mr. Freeman has blessed us with a wealth of quality acting over a period that exceeds five decades. In 2017, Mr. Freeman celebrated his 80th birthday. In this test, I enrolled Mr. Freeman's voice in one of our biometrics programs with 40 seconds from the movie *The Execution of Raymond Graham*, a movie that was produced in 1985 when Mr. Freeman was 48 years old. I then passed 3 seconds of audio in the system from Mr. Freeman's voice from a recently-produced National Geographic series titled *The Story of God*, filmed in 2016 when Mr. Freeman was 79 years old. Excerpts from this series can be viewed on National Geographic's YouTube channel. Once again, age did not impact the performance of the voice biometric engine; it validated Mr. Freeman's voice at 79 as belonging to the same person as Mr. Freeman's voice at age 48, despite 31-years separating these two recordings of his voice. Once again, the system was set to banking-grade security performance levels.

However, there is a period during our lives where our voices do change in a material way, and that is during the transition from our childhood to our adult years. You may nevertheless be surprised how robust voice biometrics can be, even during a period of what we perceive as a rapid change of our voice. To illustrate the point, I performed a test with the voice of Candace Cameron Bure, the actress that gained notoriety playing the role of D.J. Tanner in the American TV series *Full House*. I chose Ms. Bure because she started acting in Full House as a child, at the age of 11, and ended as a young adult at age 18. This provided me with yearly voice samples as Ms. Bure matured to adulthood.

To perform the test, I enrolled 40 seconds of Ms. Bure's voice from an episode of Full House in season one, which was recorded in 1987. I then performed verification tests with three seconds of audio from each subsequent season, until season eight when Ms. Bure was 18 years old in 1994. Even in this test, despite a seven-year difference between the enrollment audio and the last verification audio, the voice biometric engine had no issue identifying Ms. Bure's voice. As with previous tests, the system was configured to banking-grade security levels. In fact, it isn't until Ms. Bure reached the age of 21 in 1997, that a voice sample from her performance in the movie *NightScream* where the voice biometric engine is no longer able to match Ms. Bure's voice to her voice sample from the age of 11. The voice biometric engine concluded that there was approximately a 90% probability that these two voice samples belonged to the same person. To achieve a banking-grade level of performance, the probability needs to exceed 99%.

There is however a solution to even this voice-aging challenge. It's a capability that is called smart-adaptation in the solution. It automatically adapts the voiceprint on file for an individual with each successful authentication to the system without compromising security. As such, in the example with Ms. Bure's voice, if her voice was enrolled at age 11, and then was heard again at age 18, then the voice would have been automatically adapted so that when at age 21 her voice was verified again, it would have been successfully matched. The cases where a person's voice is enrolled as a child and is there only heard again as an adult will in most use-cases be extremely rare. In such cases, the individual's voice will need to be re-enrolled.

These examples showcase that age is, for virtually all practical use-cases, a non-material factor in the performance of voice biometrics. One could enroll in a voice biometric system at age 30, and then verify for the first time 40 years later at the age of 70, with the same layer of security across all ages. Indeed, our voices change very little during our adult years. In cases where children's voices need to be enrolled, the use of smart adaptation can automatically address the changing voice characteristics that occur naturally during our teenage years. Age may be a very sensitive topic, requiring tact when the subject arises in conversation, but to an adaptable voice biometric engine, your voice is wonderful no matter what your age.

Tags: Fraud prevention, Biometric authentication

More Information

The Security Value of Voice Biometrics for IVRs and Call Centers

As the need for tighter security across all channels increases, voice biometric solutions eliminate several security vulnerabilities that exist in IVRs and call centers. These include the weaknesses associated to PIN credentials used to secure IVR self-serve functions, as well as the vulnerabilities inherent in an agent security question verification process.

Learn more

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek