Forbes

Capital Flows Contributor

Guest commentary curated by Forbes Opinion. Avik Roy, Opinion Editor.

Opinions expressed by Forbes Contributors are their own.

OPINION 10/06/2016 @ 5:16PM | 1.292 views

Voice Recognition: Risks To Our Privacy

GUEST POST WRITTEN BY
Oleksandr Pastukhov and Els Kindt
Dr. Pastukhov is a Senior Lecturer at the University of Malta. Dr. Kindt is a Post-Doctoral Researcher at KU Leuven (Belgium).

These days, intelligence agencies around the world are capable of not only watching every breath you take and tracing every step you make. They can also hear every word you say. And yes, every single day. But how do “men in black” know that the words belong to you? Voice recognition comes to their aid.

What voice recognition is all about?

Biometric technologies, to which voice recognition technologies belong, allow the use of unique human characteristics – such as voice, speech, gait, fingerprints, iris or retina patterns – to identify (i.e. link to a known identity) or at least to recognize someone (i.e. verify someone’s identity or single him or her out “in the crowd”). Such characteristics are known as “identifiers” – the “pointers” that facilitate linking a person’s physical features with his or her identity. While such biometric characteristics were initially used to control access to military and other high-risk infrastructure (e.g., iris scans), or were collected from people arrested for breaking the law (e.g., photographs and fingerprints), this type of personal data are now used at many other – even most unexpected – places, such as Disneyland.

Also on Forbes:

Unlike many other identifiers (paper or plastic IDs, IP addresses, passwords, etc.) biometric ones cannot be discarded, disposed of, or replaced: the person is born with them and is stuck with them for the rest of his or her life. The physical characteristics of one’s voice and the manner of speaking are unique to every person and are

stable enough to be used for extremely reliable identification.

Based on voice samples that became known (directly or indirectly) to belong to certain individuals (e.g., customers of a telephone banking service) and that would be typically stored in a database, it is possible to identify those persons at any moment in the future solely on the basis of the person's voice, even if no other identifiers would be revealed. In this way, people captured on CCTV videos with soundtracks or parties to phone (or VoIP) conversations can be identified.

What are the risks for our privacy?

While using speech for speaker recognition, such as the owner of a car or mobile phone, presents only minor privacy problems (the typical question here is: is this the same person?), the use for identification purposes (typically, the question here is: who is this person?) is a very different story. The place where the voice or speech sample is stored makes all the difference: if the storage is only local (e.g., on the mobile phone), the purpose of recognizing the person can be perfectly reached with no or at least no systematic outside access and hence with a minimum risk to privacy. It is primarily the central storage of such samples that creates considerable risks, such as its (later) use for identification and related purposes other than those for which the samples were initially collected. This problem is known as the "function creep".

Any speech-to-text or voice-operated app is a perfect potential data mining tool for the NSA and other intelligence agencies. Whether they actually do that or not, we don't know, but if they are able to collect or hope to collect voice/speech samples using those apps in the future, the intelligence community can only welcome such technological advances. The samples thus collected, coupled with the texts generated by the apps, tremendously reinforce data/text mining, referencing and cross-referencing, i.e. what the intelligence agencies are supposed to do: turning raw data into information and information – into intelligence.

All this automatically brings in privacy issues, since speech recognition technologies pierce the "veil of anonymity" by matching a voice or speech sample against a database of such samples, a person can be identified and "tagged" forever. Not only the person's identity can be revealed, but all of his or her voice communications can be intercepted and movements traced for the rest of one's life. This amounts to targeted surveillance and computers make it possible to extend the practice to entire populations, turning it into a

mass surveillance scheme.

Speech recognition, alone or combined with other technologies, such as those used for telecom data retention and geo-location, are potentially extremely privacy-invasive and bring with them a whole spectrum of problems related not only to the right for privacy, but also many other human rights and freedoms, such as the freedom of expression and the freedom of movement. Mass – in fact, global – surveillance by nosy governments aided by complaisant private companies is no science fiction any more: we had known for a fact that an eavesdropping of Gargantuan proportions was actually happening long before Snowden – at least since it became known about the ECHELON program in 1988.

There are many other risks of using biometrics for identification purposes, such as that the process of identification is subject to mistakes, the data may reveal information about someone's health or even racial or ethnic origin, that (mostly depending on the place of storage of such data) while data collected for one specific purpose (e.g., someone consenting to recording his or her voice as evidence in a commercial transaction), the data could be misused for other purposes as a result of the function creep (e.g., for criminal investigations and sorting someone out as being a suspect), stored data can be stolen, etc.

For these reasons, one – whether a private company or a public authority – should use biometrics with utmost care, and, in our view, such use should be tightly regulated. It is especially the centralized storage of such data, often by a third party, that should be made subject to strict legal rules. The local storage of the data, which the individual can keep under his or her control, poses less risks. However, individuals are often unaware of where their data are stored.

Aren't there laws protecting us?

Identification and identity management by public authorities and private companies interfere with someone's private life and this why it is subject to specific legislation (detailing who is entitled to do what, under what circumstances, after obtaining which papers, etc.) in the EU, the U.S. and many other countries. However, speech recognition allows to achieve identification without leaving a "paper trail" or even without the individual knowing about it. In case identification is needed for a criminal investigation, this could only be done on the basis of reasonable suspicions and under particular circumstances, and many detailed procedural rules would apply. In other words, someone can be a suspect only if there are indications that someone did something wrong. A whole society cannot be treated as a suspect. In

case of blanket communications interception operations of the PRISM type, this is exactly what is happening, however.

What is being done and what should be done about that?

Regretfully, legal problems brought about by the advent of the technologies utilizing biometrics have not reached the level of attention they deserve. Thus, in the U.S., legislative initiatives come mostly from individual states (e.g., Illinois, Texas, California, Washington) that start to consider and enact rules on biometric information collection and use, limiting information retention periods, and specifying procedures to be followed when protecting the information. In October 2012, the FTC has come up with a set of guidelines on using face recognition technologies, but not other types of biometric technologies.

In Europe, the still valid EU Data Protection Directive does not even mention the term "biometric data", let alone define it. The General Data Protection Regulation that will replace the Directive defines biometric data in Art. 4(14) as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" and classifies them as one of the "special categories of personal data" in Art. 9(1). The special categories of personal data, known as "sensitive data" is the type of personal data that enjoys the highest degree of protection and can be processed only under conditions listed in Art. 9(2). Moreover, the Regulation in its Art. 35 requires a "data protection impact assessment" prior to processing them on a large scale.

We welcome the Regulation's novelties and see them as steps in the right direction, since biometric data are no less sensitive than, say, health data that are already recognized as such by the current Directive. Besides legal safeguards, we believe, technological protection measures are also necessary, including those that utilize voice de-identification and strong end-to-end encryption. Such measures, in turn, we submit, should be made mandatory by law.

The authors collaborated under the European Cooperation in Science and Technology (COST) Action IC1206 "De-Identification for Privacy Protection in Multimedia Content" in 2013-2015.

Workplace