EWF
Alta Associates'
Executive Women's Forum
Information Security, Risk Management & Privacy

Voice Privacy Guiding Principles

Document Purpose

This document lists initial guiding principles for voice data privacy.

Summary

Voice technology has the potential to enable individuals, companies and society in new and innovative ways. In order create such technologies; voice is one type of data that companies may collect, store, and use. As such, it is subject to the privacy and security requirements that govern data in general. In recognition that voice is part of one's person, some jurisdictions consider voice data in and of itself personal information; as such it may be subject to the more stringent rules governing personal data as well. Voice can be used as a biometric, meaning that it can be used to authenticate a person's identity, which merits additional consideration.

Risk Analysis

The privacy/security risks associated with voice data differ minimally from general data risks.
First let us consider Voice Biometrics. A person's voice is individual and is an essential *physical* characteristic. In contrast, data entered via keyboard (e.g. a typed password) is an abstraction, or one layer removed from the person. Voice is a unique physical characteristic and as such can be used as a biometric. For this purpose we should distinguish use of voice for *verification/authentication* versus *identification* purposes:

> In a closed system with known enrolled users, identity verification can be very accurate and voice data should be secured accordingly.
>
> However, the risk of identification through voice has been measured and is extremely low when the candidates to be matched are open (that is, in the millions i.e. the general population even of any specific area)

Otherwise the risk of a privacy breach of the contents of voice data is in fact *lower* than for text data. Consider that individuals with electronic devices generally have the ability to read, aggregate, classify, and otherwise process text data—accessing information from many files and individuals quickly. While someone can listen to voice data, they can only listen to one file at a time. Tools to aggregate, classify, or otherwise process audio contents are more specialized and less accurate.

Ideologies

Let's consider some underlying ideologies:

- Everyone has individual sovereignty over their own data, including voice data.

- Voice is considered personal data in and of itself in some jurisdictions, and as such may be subject to additional legal and/or regulatory rules.
- All privacy and security controls must consider that voice can be used to authenticate a person locally and remotely.
- Any information obtained through characteristics of voice (e.g. gender, disabilities) is also subject to the ADA and all other laws barring discrimination.

Guiding Principles

Voice data is subject to the same principles guiding the use of all data to safeguard privacy. Voice data should only be used within the limits of applicable laws and regulations. These include but are not limited to:

Statement of Purpose / Notice:

- Entities should clearly & simply state the purpose of the collection of voice data.

Choice & Consent:

- Entities should give the choice for Consumers regarding the use and sharing of voice data, and to Opt out at any point.
- Informed consent terms should be written clearly & simply enough that Consumers understand the collection, use, security, sharing, retention, and destruction.

Awareness & Training:

- Entities should provide training in general Data Privacy to their staff.

Collection, Use & Distribution:

- Entities should limit the collection of data to the minimum necessary.
- Entities must obey all laws governing the transmission of data across jurisdictional boundaries.
- Use of voice data should conform to the stated purpose

Access Controls:

- Access to data should be only as needed and use Role Based Access Controls.

Other Technical Controls:

- Voice data that is disassociated from the user and processed or masked such as to be non-identifiable in practice is no longer considered private

Monitoring (Audit/Validation):

- Entities should have assigned responsible and accountable personnel overseeing Data Privacy.
- Entities should include Voice Data Privacy monitoring in their routine GRC/internal audit programs.