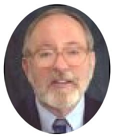
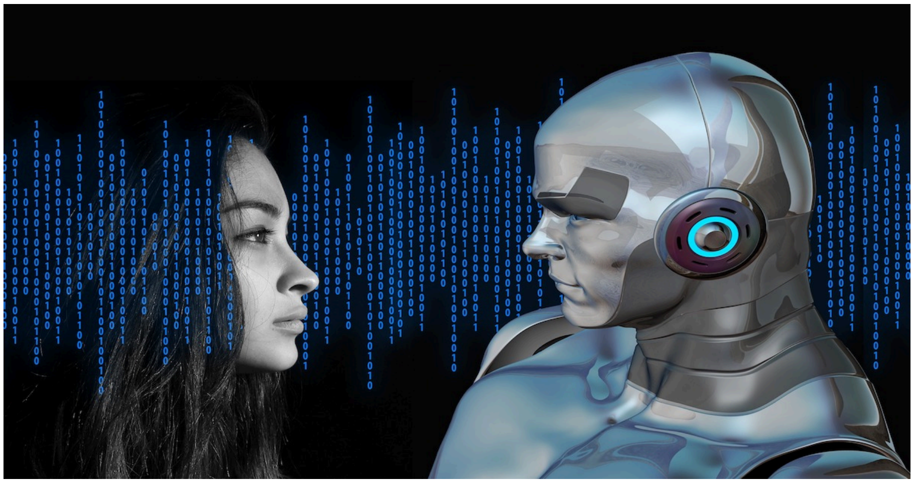
Speech TECHNOLOGY



September 21, 2023
By James A. Larson program co-chair, SpeechTEK 2021
Forward Thinking

Conversational Assistants and Privacy



Many conversational assistants—software that speaks and listens to humans using voice, text, and graphics—use data analysis software to extract and interpret information from the sound of your voice and the words that you speak. Your voice contains information about who you are, where you live, how you look, and how you feel. You might think of your voice as just a way to convey information to others, but speaking poses many challenges and risks, including these:

- Conversational assistants can **reveal sensitive and personal information**about you: your identity, location, age, gender, ethnicity, health condition, personality, traits, and mood. This information can be used for beneficial or harmful purposes, depending upon who accesses and uses the information.
- Conversational assistants can **introduce bias and discrimination**into decision-making processes. Some analyzers might favor certain accents or dialects over others or might misinterpret the emotions or intentions of a speaker based on their voice tone or pitch, which may influence decisions made using data from these analyzers.
- Conversational assistants might **store and share voice data without your consent or knowledge**and make you vulnerable to hacking or spoofing attacks. You have to be wary of conversational assistants that record your voice for "training and analysis purposes."

Trust is an essential ingredient for any scenario in which conversational assistants create developers and organizations involved with conversational assistants must ensure that they uphold established rights and foster positive social values to protect users.

Governments and governmental agencies in both the European Union and the United States have developed guidelines, recommendations, and laws to protect personal data, including data used by conversational assistants. Some of the most important developments are summarized in the table below.

Organization/ government body	Activity
General Data Protection Regulation (GDPR)	Gives EU citizens control over their personal data and simplifies the regulatory environment for international business within the EU.
European Data Protection Board (EDPB)	Specifies guidelines and recommendations for automated recognition of human features in publicly accessible spaces.
International Standards Organization (ISO)	Develops standards for generative AI to ensure it is used safely and responsibly; it also includes a framework for artificial intelligence systems using machine learning, guidance for risk management, treatment of unwanted bias in classification and regression machine learning tasks, and verification and validation analysis of AI systems.
National Institute of Standards and Technology (NIST) Generative AI Public Working Group	Ensures that generative AI technologies are used productively to address top challenges surrounding health, environment, climate change, and other areas.
Health Insurance Portability and Accountability Act (HIPAA)	Establishes national standards to protect individuals' medical records and other individually identifiable health information.
Federal Trade Commission Children's Online Privacy Protection Act (COPPA)	Spells out what operators of websites and online services must do to protect children's privacy and safety online.
NIST AI Risk Management Framework	Defines a framework to address the risks in the design, development, use, and evaluation of AI products, services, and systems in support of trustworthy AI.
European Union Artificial Intelligence Act	Expected to be approved by the European Parliament in late 2023 or early 2024. A two-year implementation period will follow the formal approval. Observers anticipate that the EU AIA will have a global impact similar to that of GDPR; its vocabulary and definitions of risk will be widely adopted.

The Open Voice Forum (OVON) Trustmark Initiative (https://openvoicenetwork.org/trustmark-initiative/) is seeking to establish a set of guiding principles for ensuring that conversational assistants follow an ethical path. It has outlined a vision for trustworthy conversational assistants consisting of of the six pillars described in the chart below.

Pillar	Description	Example of possible problems
1. Transparency	Users of conversational assistants have the right to understand how their data is being used and how conversational assistant make decisions.	A conversational assistant using a large language model (LLM) created with generative AI may not be able to explain how it derives recommendations or reference it sources.
2. Inclusivity	Conversational assistants should be designed to bring people in, not shut them out, and thus should be equipped to accommodate underrepresented populations.	There are few speech recognition software applications available for languages spoken by small numbers of people.
3. Accountability	All stakeholders working to create conversational assistants are accountable for the process of creating the assistants, as well as any outcomes they may cause.	Owners of a conversational assistant fail to detect and remove hallucinations generated by a conversational assistant based on generative AI and LLMs.
4. Sustainability	Conversational assistants should not compromise the economic, social, or environmental sustainability of our shared future.	The large amount of electrical energy required to train LLMs should be minimized and better managed.
5. Privacy	Conversational assistants should deliver information and services to users within publicly stated parameters and ensure that information about users is not leveraged beyond the intended purpose.	Confidential data may be leaked by conversational assistants using training data that contains private data.
6. Compliance	Conversational assistants should not align merely with an abstract sense of morality and ethics but should also comply in absolute terms with current	Legislative and policing actions are needed to deter bad actors from using conversational assistants and generative AI technologies for

Meeting the Rising Demand for Voice-Based Biometric Systems
Coming December 03, 2024

Avatar Platforms in Customer Service
Coming March 11, 2025

More Web Events

POPULAR ARTICLES

The Evolution and Importance of Voice Surveillance

Colossyan Introduces Instant Avatar Feature

Wondercraft Launches Director Mode

Agora Launches Conversational AI SDK

The Open Voice Network is also developing an online self-assessment maturity model for organizations that wish to see how their current structure and strategies line up with the OVON TrustMark Initiative's guiding principles. I encourage everyone to review their public training class and post the TrustMark logo on their websites.

James A. Larson is a senior scientist at Open Voice Network. He can be reached at jim42@larson-tech.com.

ALSO ON **SPEECH TECHNOLOGY MAGAZINE**

Rethinking Voice in a Digital World

5 years ago · 1 comment

For years, investments in the voice channel have taken a backseat to digital. But …

Speech Technology Has a Place in Ed Tech and …

4 years ago · 1 comment

Technology advances in speech recognition, pronunciation error …

Fiverr Introduces AI Auditions for …

2 years ago · 1 comment

Fiverr's AI Auditions gives customers instant access to personalized samples of …

0 Comments 1 Login ▾

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

♡ Share Best Newest Oldest

Be the first to comment.

Subscribe Privacy Do Not Sell My Data

RELATED ARTICLES