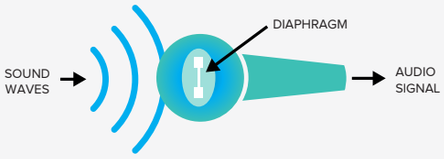
Microphones & the Internet of Things

Understanding Uses of Audio Sensors in Connected Devices

Produced by
FUTURE OF PRIVACY FORUM
August 2017

MICROPHONES *are devices that convert sound waves (acoustic energy) into electrical signals, dating back over 100 years. In the last five years, the "voice first revolution" has brought new uses of microphones as sensors into the Internet of Things (IoT). In order to enable the benefits of new voice-based services while protecting data privacy, this infographic attempts to explain the range of possible uses of microphones in consumer devices.*



ACTIVATION: Manual, Always Ready, or Always On?

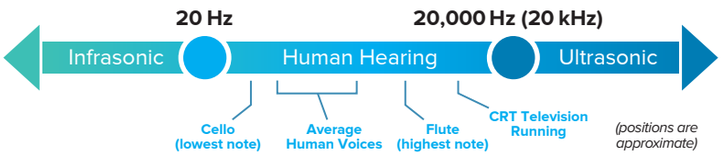
By their method of **activation**, consumer devices can be categorized as **manual, always ready, or always on.** In the past, most recording devices could be considered either on or off. Many new voice-based home assistants today can be considered "always ready" because they do not begin transmitting data off-site until they detect a wake phrase.

METHOD OF ACTIVATION	MANUAL	ALWAYS READY	ALWAYS ON
	Device begins transmitting audio externally when a **button or switch** is pressed or held down.	Device processes locally to detect a "wake phrase*" which **wakes/triggers** the device to begin transmitting data.	Device transmits data 100% of the time on a standalone basis, and further processing occurs externally.
	 *Examples: Smart TVs (some); Mattel's Hello Barbie*	 *Examples: Smart TVs (some); Home Assistant Devices, e.g. Google Home, Amazon Echo* **Familiar wake phrases include: "Hey, Siri" "OK, Google," "Hey Cortana," and "Alexa"*	 *Examples: Home security systems; CCTV; Body-worn cameras; Baby monitors*
BENEFITS	• ability to prevent unauthorized access through a hardware-linked microphone • avoids unintentional activation	• convenience of verbal activation • accessibility for users with physical limitations, e.g. mobility or visual impairment • contextual responses, e.g. a home security system that alerts the owner and begins transmitting data when it detects a noise	• enabling physical security for people and property • child safety

DATA TRANSMITTED

After a device is activated, it may sometimes transmit the full range of audible sounds (including voices), for example to enable cloud-based speech-to-text translation. However, other devices may not send audio at all, but instead may use the microphone to detect patterns and transmit other information about the user's environment.

AUDIO RECORDINGS



AUDIBLE TO HUMANS

Most microphones only detect sounds within the normal range of human hearing to enable, e.g., voice commands, speech-to-text translation, or music recognition. Depending on the sensitivity, the microphone might also detect unintended background noises (such as dogs barking, or traffic sirens).

SPECIALIZED RANGES

Sophisticated microphones might sometimes be designed to capture only certain ranges of audio data, such as very low or very high (even inaudible) sounds. For example, a microphone could be designed to detect a hummingbird's wings or a dog whistle.

NON-AUDIO

PATTERN RECOGNITION

Devices sometimes do not need to transmit audio recordings at all, but might use efficient local processing to detect sound patterns and convey data related to those patterns. For example, a city sensor might alert law enforcement when a "gunshot" pattern is detected.

METADATA

Data about when and how a device is used is known as "metadata," and may include, e.g., times and lengths of audio recordings, or where the recording took place. This data may not be as sensitive as a recording's content, but may nonetheless be revealing. For example, the times of day when a device is used may indicate when a person is typically at home.

LEGAL PROTECTIONS

Laws protecting audio data, especially voice communications, are sometimes robust — but also in flux as technologies evolve and courts grapple with the limitations of constitutional protection for data sent outside the home. Current applicable laws in the United States include:

The Wiretap Act, 18 U.S. Code § 2511
Federal Sectoral Laws for Sensitive Contexts or Populations, such as the Children's Online Privacy Protection Act (COPPA) or Health Insurance Portability and Accountability Act (HIPAA)
Federal Trade Commission (FTC)'s Section 5 Enforcement Authority
State Unfair & Deceptive Practices (UDAP) Laws
State Anti-Surveillance Statutes
Civil Tort Remedies for Invasion of Privacy

In a rapidly changing environment, trust is critical for developers seeking to innovate. Key privacy considerations include:

Data Security — regardless of how a device is activated, if the data being transmitted is sensitive (e.g. voices or data from inside the home), strong security is paramount. Product developers should design for technical safeguards, such as: limiting microphone sensitivity and range to the purpose of the device; enabling a hardware-linked on/off mute control; and filtering out unnecessary audio data at the point of collection.
Prominent Visual and Audible Notice — keeping in mind that users may not be comfortable with uses of their device's microphone related to detection of acoustic events or ambient noise if they are not aware of those uses or how they work.
Access to Information — companies should make it easy for users to access and delete their information, and be transparent about any third-party disclosures, including government requests for access.
Content vs. Metadata — although fewer legal protections exist for metadata, companies should be aware of how patterns of use for home devices can be revealing and take steps to mitigate possible privacy risks.

FOR MORE, VISIT FPF.ORG