Microphones & the Internet of Things
Understanding Uses of Audio Sensors in Connected Devices

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.

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.

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
- State Anti-Surveillance Statutes
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Insurance Portability and Accountability Act (HIPAA)
- 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.

FOR MORE, VISIT FFP.ORG