**Static Microphone scenario**

**Scenario 1**: User enters the room, scan the app, locate the microphone

Mitigation strategy: Ask user to move these (Range-Current distance) away from microphone

**Scenario 2**: User enters the room, scan the app, locate the microphone, Found no blind spots inside the room

Mitigation strategy: Ask the user to move to another room or to the corridor.

**Scenario 3**: User enters the room, scan the app, locate the microphone, can’t change thier current location

Mitigation strategy: user ask the admin to mute the microphone

**Scenario 4:** The user scans for IoT sensors at a later stage after which they found out that the location was not secure (audio is already recorded).

Mitigation strategy: Microphone already recorded the data, then contact admin to delete data

**Scenario 5:** User enters the room, scan the app, locate the microphone (carrying additional items with the user)

Mitigation strategy: Suggest users to carry a Microphone cover or White noise generator or leave the room.

**Scenario 6:** User finds themselves in a sensitive meeting with static microphones and cannot move to another location or mute the devices.

Mitigation strategy: Use non-verbal methods of communication (like written notes or secure messaging apps) to discuss sensitive information.

**Scenario 7:** During a private conversation, a user realizes they are surrounded by IoT devices with recording capabilities and no direct control over them.

Mitigation strategy: The user should immediately cease sensitive discussions and use encrypted communication tools until a safer environment is available.

**Scenario 8:** User enters a room for a confidential call and discovers a static microphone that cannot be turned off.

Mitigation strategy: User could employ sound masking devices that emit ambient sound to obscure the conversation. Alternatively, using an ultra-directional speaker that limits sound dispersion can help contain audio within a very limited area.

**Scenario 9:** In an open office environment, static microphones are present for voice command features and user needs to discuss sensitive information.

Mitigation strategy: The user can use a mobile app that interferes with microphone functionality by sending out non-audible frequencies that disrupt recording capabilities temporarily.

**Moving Microphone scenario**

1. Scenario: User enters the room, scans the app, and locates the microphone

Mitigation strategy: Ask user to move these (Range-Current distance) away from microphone

1. Scenario: User enters the room, scans the app, and locates the microphone,can’t change their current location

Mitigation strategy: request moving sensors to mute their microphone.

1. Scenario: The microphone already records unintended conversations.

Mitigation strategy: request moving sensor to delete the data.

1. Scenario: : User enters the room, scans the app, and locates the microphone, and found no blind spots

Mitigation strategy: Ask the user to move to another room or to the corridor.

1. Scenario: user located the microphone

Mitigation strategy: Not so feasible solution carrying a white noise generator along with the user.

1. Scenario: At a tech convention, moving microphones are used to capture audience reactions, but the user needs to converse confidentially with a client.

Mitigation strategy: Utilize a mobile app specifically designed to create localized sound bubbles where the external microphone signals are heavily distorted or muted, ensuring that conversations within the bubble are kept private.

1. Scenario : User discovers moving microphones in a fixed conference setup without the possibility to leave or access admin controls.

Mitigation strategy: Recommend scheduling the meeting at a different time or location via a secure communication channel, or postpone discussions on sensitive topics until privacy can be ensured.

**Static & Moving Microphone scenario**

**Scenario 1**: User enters a room equipped with both static and moving microphones, identified through an app.

Mitigation strategy: advised to stay in designated 'quiet zones'

**Scenario 2**: User enters a room equipped with both static and moving microphones, identified through an app.Idedentify no quiet zones

Mitigation strategy: use personal privacy devices like a microphone jammer.

**Scenario 3**: User identifies both static and moving microphones and none can be muted due to lack of admin access.

Mitigation strategy: User should carry a portable white noise generator to mask their conversation

**Scenario 4**: User identifies both static and moving microphones and none can be muted due to lack of admin access.

Mitigation strategy: personal devices like headphones to limit sound emission.

**Scenario 5:** Both types of microphones have captured sensitive conversations before the user could locate them.

Mitigation strategy: If the conversation is highly sensitive, the user should report the incident to a privacy officer or legal authority to explore data deletion or privacy breach procedures.

**Scenario 6:** In a hybrid meeting room equipped with both types of microphones, confidential strategy discussions need to take place.

Mitigation Strategy: Use a centralized control system to temporarily disable microphones, or set them to a privacy mode where they only activate when specifically called upon.

**Scenario 7:** At a trade show, booths are equipped with static and moving microphones to monitor customer feedback and crowd noise.

Mitigation Strategy: Use a specialized app that jams nearby microphones or masks the user's voice to prevent eavesdropping while discussing sensitive information.

**Scenario 8:** In a hospital where patient confidentiality is paramount, rooms are monitored with both types of microphones for safety and operational efficiency.

Mitigation Strategy: Implement a policy where microphones automatically mute when sensitive data is being discussed, signaled by a coded phrase or manually via a secure device.

**Scenario 9:** At a sensitive legal deposition taking place in a smart building, ensuring the privacy of testimonies against unauthorized recording is critical.

Mitigation Strategy: Install an on-demand electromagnetic shielding system in designated rooms that can block all electronic eavesdropping temporarily.

**Scenario 10:** In a high-security government facility, conversations often involve classified information, with microphones installed for security.

Mitigation Strategy: Designate secure communication rooms that are shielded and soundproof with all microphones externally controlled and disabled during sensitive discussions.

**Scenario 11:** During a corporate retreat in a tech-enabled resort, private executive meetings occur with non-disable-able smart microphones.

Mitigation Strategy: Distribute personal microphone blocking devices to all attendees which emit noise interference specifically tuned to the microphone's frequencies.

**Scenario 12:** In a public library that uses smart monitoring for noise control, students discuss collaborative projects involving proprietary research.

Mitigation Strategy: Provide sound isolation booths where the internal environment is controlled to disable microphones, or use tech wearables that disrupt recording.

**Scenario 13:** At an international conference, press rooms are rigged with both static and moving microphones to capture the event.

Mitigation Strategy: Negotiate with conference organizers for non-monitored zones or use privacy tents where conversations cannot be recorded.

**Scenario 14:** In a co-working space that is fully monitored for ambient experience enhancement, startups work on confidential product developments.

Mitigation Strategy: Offer portable privacy screens that include sound-absorbing materials and integrated microphone jamming technology.

**Scenario 15:** During a private counseling session in a smart health center, ensuring patient-therapist confidentiality against smart monitoring systems.

Mitigation Strategy: Utilize therapy rooms designed with adaptive soundproofing and selective microphone deactivation technology controlled by the therapist.

Camera sensor scenario [Wasim Ahamed Syed](mailto:wsyed4@asu.edu)

1. Scenario: User enters the room, scans the app, locates the camera sensor.

Mitigation strategy: Ask the user to move away from the camera's field of view or adjust the camera angle to avoid capturing the user's activities.

1. Scenario: User enters the room, scans the app, locates the camera sensor, cant change their current location.

Mitigation strategy: User asks the admin to turn off the camera.