### **Our Project Idea**

This project aims to develop a Privacy Mitigation Tool that enhances bystander awareness and control over data collection by smart sensors in public spaces. Many individuals are unaware of the presence of IOT devices that may collect their data in streets, malls, and even universities

#### **Key Objectives:**

* **Identify and raise awareness** of sensors in public spaces, including their capabilities and data collection policies.
* **Suggest privacy mitigation strategies** based on the user’s surroundings and personal preferences.
* **Resolve privacy conflicts** when multiple individuals in the same space have different privacy concerns.

#### **System Design:**

The system consists of:  
 An Intermediary Device or App – Detects sensors via wireless signals, APIs, or public sensor registries.  
 A Privacy Mitigation Tool – Notifies users about nearby sensors, explains their function, and suggests mitigation strategies

**Research Paper #1 : BLEBeacon: A Real-Subject Trial Dataset from Mobile Bluetooth Low Energy Beacons**

This research paper provides valuable insights into detecting and identifying sensors, which aligns with our project’s goal of informing users about hidden tracking technologies in public spaces. This research paper demonstrates how Bluetooth beacons passively track individuals using Raspberry Pi-based scanners, similar to our approach of detecting sensors and extracting data collected by them.

Both projects focus on sensor identification through unique IDs. BLEBeacon extracts Universally Unique Identifiers (UUIDs) from BLE beacons to differentiate devices, which we can apply to identify and categorize sensors in our tool. Additionally, BLEBeacon utilizes Received Signal Strength Indicator (RSSI) values to estimate a user's proximity to tracking devices, a method we can incorporate to analyze and notify users of sensor activity in their vicinity.

Furthermore, BLEBeacon highlights how individuals are unknowingly tracked, reinforcing the need for real-time privacy notifications—a key component of our project. By integrating BLEBeacon’s sensor detection and signal analysis techniques, our tool can identify tracking systems, retrieve sensor details, and provide users with transparency about surveillance practices.

Ultimately, BLEBeacon’s data collection and analysis methods serve as a strong foundation for improving sensor detection, metadata extraction, and privacy awareness in our project.

**Research Paper #2 :“It would probably turn into a social faux-pas”: Users’ and Bystanders’ Preferences of Privacy Awareness Mechanisms in Smart Homes**

This research paper focuses on privacy awareness in smart homes provides key insights for enhancing our project. It highlights the need for privacy notifications, multi-user privacy controls, and unobtrusive alerts. We can adapt its notification mechanisms (e.g., dashboards, mobile alerts) to inform users about surveillance devices in public areas. Additionally, it emphasizes privacy conflicts in shared spaces, which we can address by integrating negotiation-based privacy settings. The main key difference between this and our research paper is that our tool focuses on informing users about data extracted from sensors, ensuring they are better equipped to make informed decisions.

**Key differences**

| **Feature** | **Our Research** | **Smart Home Privacy Awareness Paper** |
| --- | --- | --- |
| **Notification Mechanisms** | Uses real-time alerts via an intermediary device to notify users about sensor-based data collection. | Evaluates different privacy awareness methods, such as dashboards, ambient lighting, and mobile alerts. |
| **Scope** | Public Spaces | Focuses on privacy awareness in smart homes, mainly for residents and bystanders. |
| **Privacy Risks Addressed** | Identifies real-time surveillance risks and informs users about location of nearby tracking devices in public settings. | Examines opaque data practices of smart home IoT devices and their impact on owners and bystanders |

**Similarities**

* Both aim to increase transparency regarding privacy risks in monitored spaces.
* Both explore user-friendly privacy notifications to ensure bystanders understand data collection practices.

**Research Paper #3 - Privacy-preserving human activity sensing: A survey**

**Key Differences**

| **Feature** | **Privacy Mitigation Tool (Our Project)** | **Privacy-Preserving Human Activity Sensing (PPHAS)** |
| --- | --- | --- |
| Detection Mechanism | Uses an intermediary device or app to detect nearby sensors (CCTV, beacons, IoT devices). | Uses signal processing, encryption, and federated learning to secure user data. |
| Goal | Increase public awareness of sensors and suggest mitigation strategies. | Ensure privacy in human activity sensing while maintaining data utility |
| Scope | Public Spaces | Private Spaces |
| Challenges | Depends on user awareness and sensor visibility | Requires high computational resources for privacy-preserving AI processing |

**Key Similarities**

* Both aim to protect individuals' privacy from unauthorized data collection and invasive surveillance.
* Both require mechanisms to detect and identify sensors that collect information about individuals.
* Both address privacy conflicts in multi-user environments, ensuring that individuals retain control over their data.

**Research Paper #4- The Privacy-Invading Potential of Sensor Data by** [**Jacob Leon Kröger**](https://www.researchgate.net/profile/Jacob-Kroeger?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19)

**Summary :**

Kröger’s research highlights how sensor data from IoT, smartphones, and wearables can be exploited for inference attacks, revealing sensitive details like identity and location. While users are aware of privacy risks from cameras and GPS, they often overlook seemingly harmless sensors like accelerometers and gyroscopes, which can still be misused. The paper emphasizes that current data protection laws are insufficient, as they do not regulate inferred data. Kröger advocates for classifying all sensor data as personal data and implementing transparency measures to safeguard privacy. The study underscores the urgent need for privacy-preserving AI techniques and stronger legal protections to counteract hidden privacy threats.

**Key differences**

| **Feature** | **Our Research** | **Kröger (2022) - The Privacy-Invading Potential of Sensor Data** |
| --- | --- | --- |
| **Objective** | Increase public awareness of sensors and suggest mitigation strategies. | Highlights how sensor data can be exploited for privacy-invasive inferences |
| **Scope** | Public Spaces | Focuses on IoT, smartphones, and wearables, analyzing hidden risks of sensor data collection. |
| **Legal & Ethical Considerations** | Highlights gaps in data protection laws | Provides a practical tool that helps individuals navigate privacy risks in real-world settings. |
| **User Awareness** | Provides a practical tool that helps individuals navigate privacy risks in real-world settings. | Provides users with real-time information on privacy risks, allowing them to take preventive actions. |

**Similarities :-**

* Both acknowledge that privacy issues are more complex in shared environments where different users may have conflicting preferences.
* Both highlight how sensor-based data collection can compromise privacy without user awareness.