BlipTrack Privacy Concerns

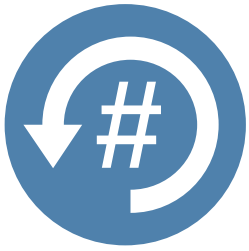
When using sensors to detect wireless signals, there are always concerns about data security and protection of personal data. At BLIP Systems we take pride in anonymizing all collected data and go to great lengths to maintain a high standard of protective measures.

Detecting Devices

BlipTrack works by detecting Bluetooth and Wi-Fi devices in the proximity of a BlipTrack sensor. A device can be a mobile phone, tablet, IVI system, laptop and more.

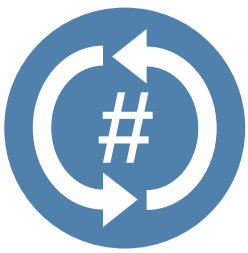
MAC Addresses, Privacy

Each device has a unique MAC address which is assigned to the device during manufacturing and cannot be modified. MAC addresses do **NOT** link to any individual user data, thus personal information is not revealed.



One Way Hash and SSL Encryption

When a BlipTrack sensor detects a device, it generates a one way hash code using a SHA-256 algorithm. Only part of the hash code is transmitted, making it impossible to revert hash codes back to real MAC addresses. Communications between the sensor and the server are encrypted using SSL.



Re-Hashing

BlipTrack supports re-hashing of MAC address device hashes, in compliance with the EU directive about privacy (WP 185 chapter 5.5). By changing the secondary hash code on a daily basis, it is impossible to identify specific devices, keeping travel patterns private.