Bluetooth Tracking Privacy Concerns

The BlipTrack™ solution is designed as a innovative and cost-effective solution to improve operations of road and traffic for the general public. The purpose is to collect information about the average travel time on a particular road segment at a given point in time. To measure travel time, BlipTrack™ use Bluetooth Wireless Technology to detect everyday Bluetooth devices that passes the BlipTrack™ sensors.

What is Bluetooth?

Bluetooth is a wireless technology that allows personal computers, lap tops, cell phones and other electronic devices to communicate with each other to transfer information/files from one device to another. It uses radio waves and is designed to be a secure and inexpensive way of connecting and exchanging information between devices wireless.

Detecting Bluetooth devices

BlipTrack™ works by detecting Bluetooth devices in proximity of a BlipTrack™ Access Point. A Bluetooth device can be a Mobile Phone, a PDA, a car with build-in Bluetooth. a GPS unit with Bluetooth support and more.
Bluetooth operates over a range from approximately 1 meter to 100 meters, depending on the class of the Bluetooth radio in the device, and the operating environment.

Bluetooth MAC address

Each Bluetooth radio has a unique address, similar to an Ethernet or Wi-Fi MAC address*, which is assigned to the device during manufacturing and cannot be modified. These unique addresses are commonly known as "burned-in addresses". This unique identifier prevents other devices from interfering with the operation between two paired Bluetooth devices.

One way hash

When a BlipTrack™ sensor detects a Bluetooth Device in its proximity, the sensor will generate a one way hash code from the Bluetooth address of the detected device using a SHA-256 algorithm. Only Bluetooth hash codes are transmitted to the central server. There is no way to revert hash codes back to real Bluetooth addresses, thereby preventing access to the Bluetooth MAC addresses of the tracked devices.

Re-hashing

In case the BlipTrack™ data was compromised, the attacker could try to correlate data between multiple systems and possibly, over time, be able to link a hash code of a Bluetooth device address to a record in another system, that could contain user information. To prevent this, BlipTrack supports Re-Hashing of Bluetooth Address device Hashes. By Re-Hashing the Hash codes using a new salt on a daily basis, a detected Bluetooth device will only have the same hash code for one day. The next day that user will be seen as a new user.

BLIP Systems does **NOT** permit third party access to the stored hash codes. The services provided by BLIP Systems relate to aggregate data only!

Bluetooth Address Privacy

Even though BlipTrack™ operates on one-way hashed Bluetooth addresses that cannot be reverted, Bluetooth has been designed to announce its Bluetooth Address. This is no different than the Wi-Fi in a mobile phone or the Ethernet adaptor in a Laptop Computer.

MAC addresses do **NOT** link to personal user information.

First of all non-mobile-phone-devices like a standard GPS unit cannot in any way be related to a specific user, simply because such a relation does not exist.

The Bluetooth address of a phone, GPS unit, hands free kit or car stereo is **NOT** recorded by the local sales team when the customer purchases the device

A MAC address is not an IME number: each phone handset has a unique IME number used to identify the location of the closest cellphone tower and then relaying text and phone messages to the cellphone via the closest cell tower. This IME number is stored by the cellphone company.

The cellphone company does **NOT** store MAC address numbers as they are only required for short range communication (<100m).