Traffic Data Gathering

UDOT 06-06

Effective: April 13, 2017

Revision: NEW

Purpose

The purpose of this policy is to define the means whereby UDOT can obtain vehicle location and other traffic data that is generated by electronic devices not owned by UDOT.

Background

UDOT gathers various types of traffic data in order to assess and manage the performance of state highways, and provide accurate data to the public. This data often includes vehicle speed, vehicle location, volumes of vehicles, and travel times, for example. This data has typically been gathered using non-intrusive inductance loops and radar sensors. Recent technologies now make it possible to detect vehicle presence by reading signals emitted from personal electronic devices, including Bluetooth and wifi MAC (media access control) addresses. (The MAC address is a unique hardware identification number, similar to an IP address for a computer). Future developments will introduce other methods of data gathering; this policy applies to any of these that detect transmissions from privately-owned devices. Data gathered through these techniques can be used to determine travel times, produce origin-destination data, and other information. The data is valuable to UDOT functions in planning, project development, design, construction, traffic operations, traffic safety, and other areas.

The Legislature clarified (HB 369) the ability of governmental entities to gather data from personally held electronic devices, in 2016. In part, the legislation states:

> "a government entity may not obtain the location information, stored data, or transmitted data of an electronic device without a search warrant issued by a court upon probable cause.
> (2) (a) A government entity may obtain location information . . . with the informed, affirmative consent of the owner or user of the electronic device;
> (4) (a) a government entity may receive and utilize electronic data containing the location information of an electronic device from a non-government entity as long as the electronic data contains no information that includes, or may reveal, the identity of an individual."

Obtaining consent from the many owners of these electronic devices is impractical, except in limited cases, such as a study or a defined fleet.

Policy

When UDOT deems it useful to have location information gathered from private electronic devices (cell phones for example), such information will be obtained with affirmative owner consent or through appropriate agreements from a third party, non-governmental entity. This information will contain no information that can be used to determine the owner of the device.

In cases where UDOT contracts with third parties to provide vehicle location or travel times at specific locations (as opposed to aggregated data from multiple sources) based on MAC address identification or similar unique network identifiers, the vendor will be required to encrypt that data after it is detected in a way that prevents it from being connected to the original device or owner.

MAC Reader devices owned by UDOT prior to August 1, 2016: it will be determined if those devices send data directly to a private vendor. UDOT can continue to use these devices on state roads to obtain vehicle location and travel time data if this is the case, and it is not possible for UDOT to obtain raw data directly from the device, and the vendor does not have, and cannot provide, personally identifiable information from their database. .

UDOT will not purchase any additional MAC Reader devices.

UDOT may contract with non-governmental entities to collect vehicle data using MAC address detection. UDOT may also participate in the installation of these devices, owned by others, to facilitate the efficient gathering of information. Vendors providing this equipment will conform to an encryption process that conforms to this policy, similar to the following:

1. MAC addresses will be encrypted at the field device so that raw MAC addresses are never transmitted.
2. MAC addresses will be “salted and hashed” prior to transmission, processing and storage to create a unique, non-reversible information string that cannot be linked back to the raw MAC address.
3. The “salt” string will be randomly generated and changed each day, and the prior “salt” strings will be deleted.

There may be other types of devices that detect signals from private electronic devices, but do not specifically use MAC address technology. In this event, UDOT will conform to this same policy, for example, UDOT will not purchase or use said equipment (except for cases where the private device owner grants consent to the data), and UDOT may obtain data generated by this equipment from non-governmental entities only when appropriate encryption processes have been employed and no personally identifiable data is included.

UDOT may obtain and use traffic data from vendors who aggregate this data from many sources, including MAC address and GPS (global positioning system) data, provided that said traffic data does not include any personally identifiable information or facilitate the determination of that information.

Procedures

Responsibility: Operations Engineer

Actions

1. Educate Region leaders about the traffic data gathering policy and appropriate actions.

2. Identify any existing devices owned by UDOT that read MAC addresses and determine whether these send data directly to a non-governmental entity, restrict access to raw data at the device, and employ acceptable encryption procedures. Determine the appropriate disposition of devices that do not meet this criteria.

Responsibility: Procurement Officers

Actions

3. Review procurement requests to verify that devices that do not comply with this policy are not purchased by UDOT.

Responsibility: Region Traffic Engineers

Actions

4. Review Maintenance of Traffic plans for UDOT construction projects to identify any technologies that might be used to measure traffic conditions during construction and verify that those procedures meet the requirements of this policy.

Responsibility: Traffic Management Engineer

Actions

5. Oversee and review plans to obtain traffic data, specifically those that use technology to obtain this data, in whole or in part, by collecting data emitted from private electronic devices, and verify that the requirements of this policy are met.