Technical Disclosure Commons

Defensive Publications Series

October 2020

Utilizing In-Vehicle Computing Devices to Exchange Information During a Traffic Stop

Michael Angermann

Tajinder Gadh

Utilizing In-Vehicle Computing Devices to Exchange Information During a Traffic Stop

Abstract:

This publication describes techniques directed at utilizing in-vehicle computing devices to facilitate an electronic traffic stop process that enables the electronic exchange of information between a police officer and a vehicle operator. This electronic exchange of information facilitates safer and less-stressful interactions during traffic stops. The information exchanged through this process includes, but is not limited to, copies of the operator's driver's license, vehicle registration, and proof of insurance. By exchanging the information electronically, a police officer can perform their initial investigation without approaching the vehicle on foot.

Keywords:

Traffic stop, police officer, public safety official, vehicle, operator, driver, computing device, in-vehicle computing device, wireless connection, driver's license, vehicle registration

Background:

A public safety official (*e.g.*, police officer), driving an emergency vehicle (*e.g.*, a police vehicle), may initiate a traffic control stop ("traffic stop") of a vehicle by activating the audible and visible signals (*e.g.,* activating a flashing light bar and/or siren) located on the emergency vehicle. A traffic stop involves the temporary detention of the operator (driver) of the vehicle by the officer in connection with the officer's investigation of a possible crime or minor violation of the law (*e.g.*, a traffic violation).

The face-to-face interaction between the officer and the operator in a traffic stop is frequently stressful for all parties involved. The investigation of some types of traffic stops may not require such a face-to-face interaction for the officer to complete their investigation. For example, a traffic stop resulting from a minor traffic violation (*e.g.*, operator did not use a turn signal before changing lanes) or a minor vehicle safety violation (*e.g.*, operator's vehicle tail light has shorted and is not operable) may not require a face-to-face interaction.

Description:

In a traditional traffic stop, when both the operator's vehicle and the police vehicle have come to a stop, the officer exits their vehicle, approaches the operator's vehicle on foot, and asks the operator to provide operator identification information (*e.g.*, driver's license, vehicle registration information, proof of insurance). After receiving the operator identification (Operator ID) information from the operator, the officer may return to the police vehicle and verify the information provided by the operator. The officer may utilize a computer terminal (*e.g.*, mobile data terminal (MDT), mobile digital computer (MDC), in-car computer, laptop computer, tablet computer) located in the police vehicle to perform this verification. For example, the officer may utilize the computer terminal to electronically check for outstanding arrest warrants, outstanding citations, valid driver's license privileges, the validity of the vehicle registration, and the like. Upon the completion of their investigation, the officer may return to the operator's vehicle to indicate that the operator is free to go, perform a further investigation, write a citation (a ticket) to the operator (*e.g.*, for violating a traffic law), give a verbal or written warning to the operator, or take other action.

This publication describes techniques for utilizing in-vehicle computing devices (*e.g.*, a police officer computing device and a vehicle operator computing device) to facilitate an electronic traffic stop process that enables the electronic exchange of information between a police officer and a vehicle operator (driver). This electronic exchange of information facilitates safer and less-stressful interactions during traffic stops.

The computing devices may include one or more processors, transceivers (*e.g.*, a wireless local area network (WLAN) transceiver, a Bluetooth™ transceiver, a Bluetooth™ Low Energy (BLE) transceiver) for transmitting data to and receiving data from another computing device, sensors (*e.g.*, a location sensor, a global navigation satellite system (GNSS) receiver, global positioning satellite (GPS) receiver), a computer-readable medium (CRM), or an input/output device (*e.g.*, a display, a speaker, a microphone). The CRM may include any suitable memory or storage device such as random-access memory (RAM), static RAM (SRAM), dynamic RAM (DRAM), non-volatile RAM (NVRAM), read-only memory (ROM), or flash memory. The CRM includes device data, for example, user data, multimedia data, applications, and/or an operating system of the device, which are executable by the processor(s) to enable the techniques described herein.

Figure 1 (below) is a sequence diagram illustrating an example electronic traffic stop sequence that begins when an officer pulls over an operator. In the example illustrated in Figure 1, the computing device of the police officer is a mobile data terminal (MDT) located in the police vehicle and the computing device of the operator is the operator's smartphone. Once both vehicles have come to a stop and are standing, the operator and/or the officer may utilize their respective computing devices to begin the process. The process begins with the establishment of a wireless connection (*e.g.*, a wireless ad hoc network, peer-to-peer connection) between the MDT of the

officer and the smartphone of the operator. The wireless connection enables bidirectional communication between the officer and the operator, which may include the exchange of messages, text information, audio and/or video communications, images, and the like. If a wireless connection cannot be established, the officer may proceed with a typical face-to-face traffic stop interaction with the operator.

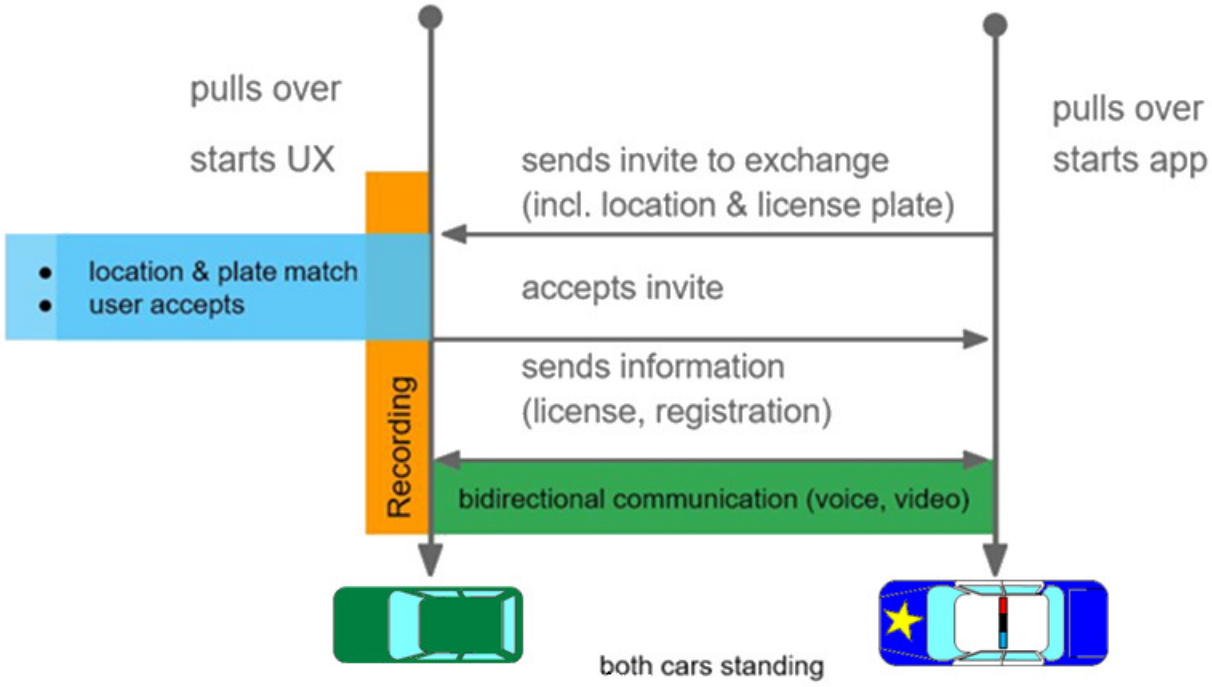

Figure 1: Electronic Traffic Stop Sequence

Once a wireless connection is established, an invitation may be sent by the officer's MDT to the operator's smartphone requesting participation in an electronic traffic stop, and a notification displayed on the user experience (UX) of the operator's smartphone. The invitation may include information confirming the identity and/or location of one or both of the officer and/or the operator, for example, geolocation information and license plate information enabling the operator to verify that the party requesting the information is the officer. The license plate information may include the operator's license plate information and/or the officer's license plate information.

Responsive to receiving the invitation requesting participation in an electronic traffic stop from the officer, the operator may confirm if the location and license plate information received is correct and accept the invite. If the operator declines the electronic traffic stop invitation (*e.g.*, by pressing a "decline" button on the UX of the operator's smartphone) or if the officer does not timely receive a response from the operator, the officer may proceed with a typical face-to-face traffic stop interaction with the operator.

After the operator accepts the electronic traffic stop invitation, the parties may exchange electronic messages. For example, the officer may send a request for Operator ID information to the operator, such as a request for images (*e.g.*, photographs) of the operator's driver's license, vehicle registration, and proof of insurance. Responsive to receiving the request for Operator ID information, the operator's smartphone may display a notification on the UX.

The operator may elect to share Operator ID information electronically with the officer. For example, the operator could utilize their smartphone to take photographs of their driver's license, vehicle registration, and insurance card, and attach the photograph(s) to a message sent to the officer. Alternatively, before the traffic stop, the operator may elect to save images of the Operator ID information on their smartphone as device data that could be attached to a message sent to an officer in the future.

Aspects of the interaction between the officer and the operator during the electronic traffic stop may be documented, recorded, and stored by one of the devices, for example, as one or more images, audio recordings, or video recordings. Such information may be automatically transferred to a remote server (*e.g.*, via a cellular network connection) during or after the traffic stop.

In the disclosed techniques, the operator and the officer (each a "user") may be provided with controls allowing the user to make an election as to both if and when systems, applications,

and/or features described herein may enable the collection of user information (*e.g.*, Operator ID information, a user's current location), and if the user is sent content and/or communications from a server. In addition, certain data may be treated in one or more ways before it is stored and/or used so that personally identifiable information is removed. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to another user.

Through such techniques, in-vehicle computing devices can be utilized in an electronic traffic stop process enabling the electronic exchange of information between a police officer and an operator that facilitates safer and less-stressful interactions during traffic stops.

References:

[1] Patent Publication: US20180338231A1. Method and system for managing temporary detention of civilians. Priority Date: May 22, 2017.

[2] Patent Publication: US20200097708A1. System and method for increasing safety during traffic stops. Priority Date: September 22, 2017.

[3] Jeffrey-Wilensky, Jaclyn, and David Freeman. "This Police Robot Could Make Traffic Stops Safer." NBCUniversal News Group. May 9, 2019. https://www.nbcnews.com/mach/science/police-robot-could-make-traffic-stops-safer-ncna1002501.