As published in LAW360

Automobile Data Recording Is Not An Invasion Of Privacy

By Derek S. Whitefield, Dmitriy Kopelevich and Isabella C. Hsu, Dykema Gossett PLLC
June 19, 2014

Increasingly, vehicles are equipped with electronic sensing technologies, such as lane departure warning/assist, night vision, automatic braking, and driver drowsiness detection/alert. Various subscription services upload vehicle condition and location in the event of a crash. Within several years, vehicles may be communicating with control centers and each other to facilitate traffic flow and even help avoid collisions. Fully autonomous vehicles are being tested and have clocked hundreds of thousands of miles.[1]

How well do these technologies work? Will they reduce motor vehicle injuries and deaths? To answer questions like these, and to continuously improve new sensing technologies, many vehicles can record data about the operation and performance of these systems. This recorded data has the potential to improve vehicle reliability, service and, most importantly, motor vehicle safety. However, concerns have been raised about whether the benefits of automobile data recording have been properly balanced with individual privacy rights.

Though only recently standardized, crash event data recording has been going on for decades. While the popular press and even some courts colloquially refer to automobile event data recorders ("EDRs") as a "black box," this is a misnomer that likely contributes to misperceptions about the intrusion of data recording on privacy rights. Unlike the black boxes in airplanes, trains, and ships, which record data continuously throughout their operation, EDRs in automobiles only record data for a brief period of time, and usually only in the event of a crash or near crash event. Current EDRs do not record audio, video, driver identity or vehicle location.

The National Highway Traffic Safety Administration describes EDRs as "[A] device installed in a motor vehicle to record technical vehicle and occupant information for a brief period of time (seconds, not minutes) before, during and after a crash."[2] Pursuant to 49 CFR Part 563 et seq., the EDRs in vehicles built on or after Sept. 1, 2012, must comply with standardized requirements for data elements, data format, data capture, and disclosures in owner manuals. There are 15 required data elements and an additional 30 data elements that, if collected, must be captured at certain minimum intervals for specific periods.

The 15 required data elements can be roughly divided into pre-crash and post-crash elements. Pre-crash data elements include vehicle speed, accelerator pedal position/voltage, throttle position, engine throttle percent, engine speed (rpm), service brake status, steering angle, vehicle roll angle, ABS activity, stability control, safety belt status, frontal air bag warning lamp, and the number of times the ignition was turned on or off. Post-crash data elements include airbag trigger times, number of crash events, time from event 1 to 2 (if applicable), and longitudinal change in forward crash speed vs. time during the impact (delta-V).

While EDR data is typically only recorded during an actual vehicle crash or near crash, in some vehicles data recording may also be activated during certain abrupt driving maneuvers, such as sharp steering or sudden braking. In this situation, the vehicle may record similar data as if there had been an actual or near crash. Subscription services like OnStar or BMW Assist, portable GPS devices like those made by Garmin or TomTom, toll-road transponders, and auto insurance monitoring devices like the Progressive Snapshot may also record data about vehicle system performance.

---

[1] Google has already announced that it had begun building a fleet of 100 experimental driverless vehicles, road ready for the Google campus in 2015.

[2] http://www.nhtsa.gov/Research/Event+Data+Recorder+(EDR)/Welcome+to+the+NHTSA+Event+Data+Recorder+Research+Web+site

What expectations of privacy do people have in vehicle event data, and how are these privacy concerns protected? Privacy protections regarding event data generally fall into two categories: (1) requirements for disclosure of the existence of the recording device, and (2) requirements regarding permission/approval to access recorded data.

Disclosure of EDRs is required by 49 CFR Part 563.11, which requires each vehicle owner manual to include a specifically worded statement informing vehicle owners that their vehicle contains an EDR and of its recording capabilities. Currently, 14 states also require disclosure of EDRs.[3] These requirements provide a uniform and consistent message to consumers about event data recording. In short, no one should be surprised that their vehicle records crash and near crash event data. While EDRs preserve information that occurred during a split second event, the data itself is generally observable from the street (i.e., whether an occupant was wearing a seat belt, made a steering input, or applied their brakes), and so the EDR is really nothing more than an electronic, albeit more reliable witness of otherwise nonprivate information.

Access to EDR data is regulated primarily by state law. For those 14 states with EDR laws, owner consent is generally required to download EDR data. Even though the definition of ownership varies somewhat from state to state, most states consider the owner to be the "registered owner, a person entitled to the possession of a vehicle as the purchaser under a security, or a lessee of the vehicle for a period of over three months."[4] Most of the state laws also permit data to be accessed without owner consent pursuant to a court order, for vehicle safety research, and for vehicle diagnostic, service, or repair purposes.[5]

Other state laws make it unlikely that event data will be accessed without permission. In some states, computer trespass laws would likely be interpreted to prohibit access to EDR data without some form of consent. By way of example, California Penal Code Section 502 provides protection to individuals from unauthorized access to lawfully created computer data. Any person who "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network" can be punishable by a fine not exceeding $10,000.

Additional protections regarding access to event data may be legislated by Congress. The Senate passed S.B. 1813, which mandates EDRs for every car sold in the U.S. starting with model year 2015. The bill would revise 49 CFR Part 563 to establish requirements for preventing unauthorized access to event data. The bill provides exceptions when the data is obtained by court order, to facilitate emergency medical response, pursuant to a qualified investigation, or by owner consent for any purpose, including vehicle diagnostic, service, or repair purposes.

While access to EDR data is primarily regulated by the states, several federal privacy laws add additional protections. The Computer Fraud and Abuse Act makes it a crime to intentionally access a "protected computer" without authorization. The Federal Trade Commission is also empowered to prevent unfair or deceptive acts or practices affecting commerce and has included EDR data in their "Internet of Things — Privacy and Security in a Connected World" panel on "Connected Cars."[6] Finally, in the criminal context, the Fourth Amendment protects against unreasonable search and seizure.

There will be more cases decided in the criminal context, but recently the California Court of Appeal ruled in People v. Diaz, that no Fourth Amendment violation resulted when police seized the EDR from the defendant's truck, impounded it for evidence, and downloaded the data.[7] The court found the vehicle had been lawfully seized, the examination of the vehicle for evidentiary value did not constitute a "search" (as the term is used in both the California and federal constitutions), and the defendant had no reasonable expectation of privacy in the data from the device regarding the vehicle's speed and braking since both speed and brake lights can be readily observed from the street. Id.

---

[3] http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx

[4] Arkansas, Colorado, Maine, Nevada, New Hampshire, New York, Oregon, Texas, Utah, Virginia, and Washington.

[5] http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx

[6] http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

[7] People v. Diaz, 213 Cal. App. 4th 743 (2013).

Automobile data recording can aid in the understanding of what happens in crashes and how to prevent them. The data can help in the development of safer vehicles, thereby reducing the number of crashes, the severity of crashes, and the severity of injuries and deaths when crashes do occur. In our view, the value of automobile data recording far outweighs concerns expressed about invasion of privacy rights. The data is mostly collected on public roads, mostly of a technical nature, and as related to driver performance, primarily of actions that are observable from the street. Accordingly, the limited intrusion on privacy rights associated with collecting event and other automobile data is outweighed by the benefits of data recording.

Derek Whitefield is a member, Dmitriy Kopelevich is a staff attorney and Isabella Hsu is a summer associate in Dykema's Los Angeles office.