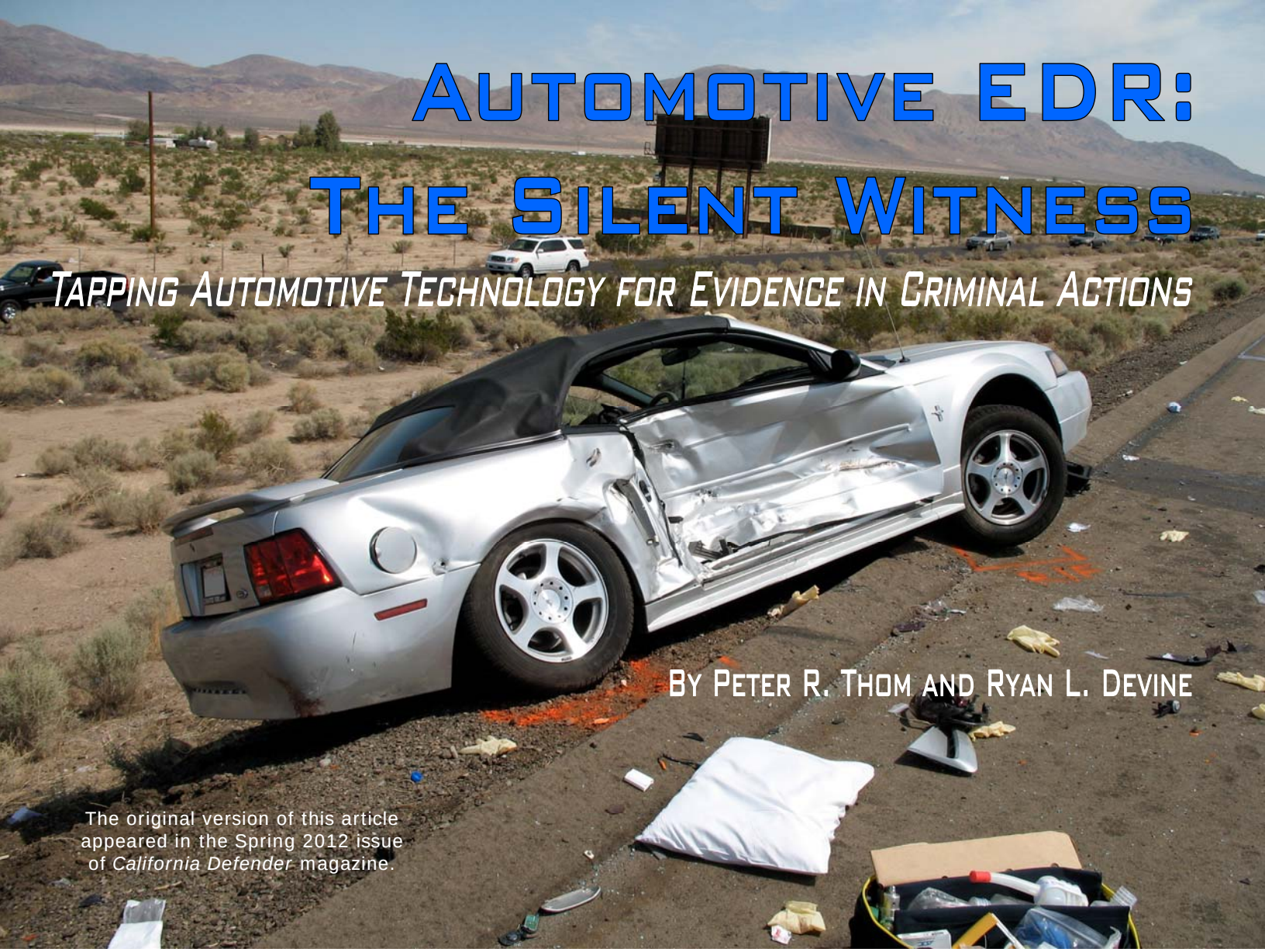
Automotive EDR: The Silent Witness

Tapping Automotive Technology for Evidence in Criminal Actions



By Peter R. Thom and Ryan L. Devine

The original version of this article appeared in the Spring 2012 issue of *California Defender* magazine.

In a realm where irrefutable evidence is priceless, data downloaded from an automotive event data recorder (EDR) might offer objective evidence for criminal actions involving vehicular accidents. The data downloaded from a technology sometimes described as an automotive "black box" can capture driver actions and decisions immediately prior to and succeeding an accident. Should a defendant's fate ride on an exact understanding of a poorly witnessed event, then EDR crash data potentially could fill a testimonial role.

Of course, there are caveats at play when using EDR data to build a defense in criminal cases. Even while the technology promises answers to automotive accidents, it is also triggering questions about judicial admissibility and privacy rights. Many of them can be answered with a better understanding of the technology and its implications, while others will be resolved over time as EDRs mature.

Who is Watching Whom with EDR?

The query references a misplaced fear that EDR technology is used to spy on drivers. An automotive EDR is simply a data-gathering module located in a car's airbag control system designed to collect very specific data in case of an airbag deployment. No microphones. No cameras. Nor does the module function like General Motor's OnStar® or related products, with in-vehicle communications, security, global positioning systems, and remote diagnostic capabilities. The real-time monitoring capability makes them more vulnerable to questions of privacy invasion than EDR. Issues like "Who, what, where, when and how?" might be retrievable from such systems, whereas EDR delivers only a limited data set.

Peter R. Thom *is President of Peter R. Thom and Associates Inc., a national firm of consulting automotive engineers.* ***Ryan L. Devine*** *is a managing engineer at the company.*

What is EDR's backstory?

EDR was developed by automakers to collect operational information about airbags. If the airbags do not function as designed then automakers become liable for the injuries sustained by drivers and passengers when they fail. It was a very short jump to then apply the technology to the needs of regulatory agencies like the National Highway Transportation Safety Administration (NHTSA) and transportation researchers that require real-world crash statistics for highway safety research and policy-making. Add accident investigators, attorneys, and insurance carriers who want access to accident data for their own purposes, and suddenly EDR becomes a child caught in a custody battle.

The result is that automakers who install EDRs now have to reengineer them to meet the operational and reporting needs of a broader audience—with voluntary compliance set for model year 2012 vehicles. To be clear, not all cars have EDR modules in their airbag control systems—the NHTSA estimates 64% of model year 2005 have some EDR capability, although that figure has grown in recent years.

Keep in mind that the newest vehicle models are replete with microprocessors, especially in performance-enhancing features like electronic stability control and antilock brakes. However, the most pertinent data-gathering module here is the one found in airbag safety systems because it is designed to collect, store, and report accident data to a NHTSA-regulated standard. Even if these other modules retain useful information for crash investigators—a distant possibility, at best—the data usually is wiped with each ignition cycle (turning the vehicle on/off), plus the modules remain outside the scope of current federal laws.

Many jurisdictions have law enforcement personnel who are certified to download crash data from EDR modules. Be sure to ask investigators if the affected vehicles had accessible EDRs and if they were able to download the crash data. However, accessing the data is one step in the investigation process, obtaining an accurate understanding of the data usually requires the input of someone, like an automotive engineer, who can interpret the significance of the results within the broader context of an accident reconstruction.

Plain and simple, how does EDR work?

EDR's mission is simple: passively monitor specific operational readings until a sudden velocity change like a rapid acceleration or deceleration triggers activation. At that point, the EDR will wake up and save the data it has been sampling in the seconds prior to the event. Then it will record the subsequent changes in vehicle speed that describe the behavior of the vehicle during a collision—engineers use the term *crash pulse*. If the accident results in airbag deployment, the data will be saved indefinitely, but if the crash is less severe, the data may be erased if another sudden deceleration occurs or if the vehicle goes through a large number of ignition cycles. Not every speed burst or sudden braking will signal an accident, but an event of sufficient magnitude to awaken the system will be documented until erased or overwritten.

The EDR data set may include: vehicle speed, engine speed, brake status, throttle position, seatbelt status, ignition cycles, Delta V's (velocity changes), passenger airbag status, and time from impact to airbag deployment.

How is EDR data collected?

A proprietary cable is the means for retrieving data from an EDR module. For now there is only one commercially available crash data retrieval (CDR) system and it is used primarily for vehicles manufactured by the Big Three U.S. automakers (Chrysler, Ford, and GM). Access to other automaker modules must be initiated through the manufacturer, although they will have to facilitate crash data retrieval access via a commercially available system by 2012.

The EDR data set may include: vehicle speed, engine speed, brake status, throttle position, seatbelt status, ignition cycles, Delta V's (velocity changes), passenger airbag status, and time from impact to airbag deployment.

Data extraction from an EDR is not for the hobbyist, as tampering with airbag sensors or attempting to remove the module can imperil airbag operation and related safety systems. Airbags are explosive devices that are dangerous to untrained personnel who may inadvertently trigger deployment. All EDR matters should be handled by trained personnel who understand the different components in these systems and are careful when accessing the EDR to avoid or minimize problems like data loss or evidence spoliation. In addition, they will need to document both the retrieval process and the chain of custody. These precautions ultimately will facilitate admissibility of the downloaded crash data in judicial proceedings.

Is There Anything Else About EDR That I Should Know?

Not every vehicle has an accessible EDR, and even if it does, there is no guarantee that the data downloaded from the module following an airbag deployment will be accurate or complete. The technology is still developing, plus current automotive EDRs are not as resilient or reliable as their aviation counterparts, which can withstand concussion, conflagration and submersion. At present there is no commonality in data collected, sample rate, recording period, communications protocol, or module connectors. Remember standardization is the goal of the NHTSA rule, but even as new models are compliant, that still leaves 250 million or more cars on U.S. roads whose EDRs are unaffected by federal oversight.

Consequently, the data retrieved from an EDR download is best used as an adjunct to a thorough accident investigation and not as standalone testimony. The data may refute or corroborate witness statements, but when issues are gray rather than black or white, it is crucial that the evidence be as indisputable as possible. The analysis and interpretation of the data is best left to skilled professionals who are aware of the technology's limitations and schooled in broader analytics.

How has EDR fared in court?

EDR evidence was first introduced in a Colorado criminal prosecution in 2002. Since then, EDR evidence has been accepted by the courts in most states as well as several Federal District Courts. In fact, *Frye* and *Daubert* hearings to assess admissibility have been supportive of the module's crash data in every instance. For criminal proceedings, the information gleaned from a download has been used primarily to prosecute drivers who were driving recklessly before fatal collisions. In contrast, the civil cases primarily concern airbag malfunction or vehicle defects like an alleged sticking gas pedal. In the few cases where the court has ruled against admitting EDR data, it determined that the recorded event was not relevant to the matters at issue.

What's all the talk about privacy issues and EDR?

Those who investigate vehicular accidents tend to shrug their shoulders about the fears of privacy invasion. To them, EDR data is akin to any other piece of objective evidence to be picked up at an accident scene. Law enforcement personnel usually check the brake lights, seatbelts, tire pressures, turn indicators, and more of the affected vehicles at the crash site. If they are trained in and equipped with CDR, and the vehicle has an accessible and undamaged system, then they will download the data, typically with the permission of the vehicle owner.

Things get a little more complicated for consumers because there is something uncomfortable about a technology that can reveal mistakes. Plus they wonder why they do not get a choice in the matter of EDR placement in their cars. Thus loss-of-control fears underlie the privacy invasion issue and have fueled legislative and regulatory actions addressing EDR data ownership.

To date thirteen states have EDR laws on the books, with California leading the way in 2003. All of them require owner consent to download the data. A number of other states have pending legislation. Common computer trespass laws criminalizing unauthorized access may be applicable to EDR data recovery as well.

Absent consent, can EDR data be retrieved without a search warrant? The Fourth Amendment says that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" U.S.Const., 4th Amend. In *Smith v. Maryland* (1979) 442 U.S. 735 (99 S.Ct.2577), the Supreme Court stated that " this court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."

In *People v. Xinos*, H034305 Sixth Dist. Feb. 8 2011, the California Sixth District Court of Appeal held that the defendant had a reasonable expectation of privacy in the data contained in his vehicle's EDR. As such, the data is protected by the Fourth Amendment and may not be searched/seized without a search warrant unless, at the time of the search/seizure, the officers have reasonable or probable cause to believe they will find the instrumentality of a crime or evidence pertaining to a crime before they begin their search/seizure. The *Xinos* court found that the officers lacked probable cause because at the time of the data download they did not think that they would find anything since the airbag had not deployed. They were merely doing the data download at the unexplained request of the District Attorney.

The Court distinguished cases where technology (e.g. radar guns, traffic cameras, etc.) is used to allow law enforcement to capture information that a person knowingly exposes to the public stating that in this case the government wasn't making observations of conduct exposed to public view; rather, the defendant's own vehicle was internally producing data for its safe operation and such data was not exposed to the public or conveyed to any other person.

The Court also distinguished *People v. Quackenbush* (1996) 88 N.Y.2nd 534, in which the New York Court of Appeals held that there is only a diminished expectation of privacy in the mechanical areas of the vehicle. The court stated that while the holding in *Quackenbush* may make sense in New York, due to that state's extensive regulation of vehicular safety equipment, this same reasoning doesn't extend to California, because California does not have similar laws requiring annual inspections and/or safety inspections following an accident as is true in New York.

In a subsequent case, *People v. Ferguson* (2011) 194 Cal.App.4th 1070, the Fourth District Court of Appeal upheld the trial court which denied defendant's motion to exclude evidence obtained from his EDR. The court discussed the *Xinos* court's recognition of an expectation of privacy in the data contained in the vehicle's EDR and the Fourth Amendment protections attaching thereto. *Ferguso*n, however, found defendant's reliance on *Xinos* misplaced stating, "Here, there is no Fourth Amendment issue. Ferguson concedes the data from his vehicle's EDR was lawfully obtained pursuant to a search warrant." (*Id.* at p. 1088.)

On May 19, 2011, the Califonria Supreme Court unanimously voted to depublish *Xinos.* Although *Xinos* cannot be cited as precedent, the *Xinos* and *Ferguson* cases are indicative of how California courts might rule when faced with this issue in the future.

Considering these rulings as well as the EDR-specific and computer trespass statutes, it is in the best interest of all parties to obtain written consent of the owner(s) before removing the EDR module and/or accessing the data. The consent should identify the vehicle (VIN #) and allow the retrieval of the EDR module as well as the recovery of the EDR data. It should also address the continuing utilization, release, and ultimate disposition of both the module and the data. Absent consent, a search warrant should be obtained, unless, at the time of the search, the officers have reasonable or probable cause to believe they will find the instrumentality of a crime or evidence pertaining to a crime before they begin their search.