Privacy at Speed

Alexander Valys
Massachusetts Institute of Technology

December 12, 2007

paper completed for MIT course 6.805/STS085
Ethics and Law on the Electronic Frontier,
Fall 2007

Contents

1 An Unknown, Growing Threat

Most people do not think of the fact that, by stepping into a modern automobile and driving it somewhere, we are entering an environment that is unique even in our technological society - an environment in which we are surrounded by countless computers and monitoring devices, which we have absolutely no control over.

A technically-knowledgeable individual is capable of maintaining control over their computer - keeping it free of spyware that might record their webcam or microphone inputs, browsing history, keystrokes, and so forth. But even the most adept hacker is unlikely to have any success in maintaining a similar level of authority over the devices integrated in or attached to his car.

When talking about issues of privacy in the modern world, one tends to gravitate towards discussing the internet and personal computing. After all, it is the rapid pace of change in technology that is in some sense causing most of today's privacy issues, and the most prominent feature of advancing technology in most people's lives has been the personal computer and the internet, and all the issues accompanying them. Little attention is paid to the automobile industry, even though it affects significantly more people than the internet and personal computing

And for quite a while, this indifference has been justified. Major auto manufacturers tend take a very conservative approach to adopting new technology, and have very long product development cycles to begin with. This means that the level of technology in even the most exclusive car available to the public lags well behind the state-of-the-art.

Even as technology dramatically changed our everyday lives during the dawn of the personal computer era, our automobiles remained relatively unaffected by this digital revolution. The use of electronic systems grew, but they remained mostly out of sight in the bowels of our car - there is little privacy risk inherent in a digital emissions control system with a few kilobits of memory and a 1 MHz processor.

However, over the past few years, things have begun to change. Automakers have been developing a variety of electronic systems that take advantage of our newly-discovered technological ability to improve the safety, comfort, convenience, and efficiency of their vehicles, by monitoring and controlling the actions of the driver and passengers. Some of these systems have already been implemented in models available to the public, and others will appear over the next few years.

At the same time, governments and insurance companies have begun to develop technological monitoring systems of their own, more to serve their own interests than out of a desire to improve the driving experience for their citizens and customers. Government agencies see the opportunity to increase their revenue by automating traffic enforcement, toll collection, registration verification, and so on, and insurance companies are eager to gain access to more information about their customers' driving habits in order to maximize the accuracy of their risk models, and thus, their profits.

Regardless of their stated goals and potentially significant benefits, I argue that many of these systems pose a substantial, unrealized threat to a personal privacy, one that most people remain unaware of and which is poorly handled by the legal system, and that without strong reforms on the part of Congress and the judiciary, the future of technological development in the automotive industry will be greatly impeded.

This paper is intended as a survey of the various technologies with privacy implications that have emerged in the transportation industry over the past few years, as well as some that are still in the conceptual phase. In discussing each technology, we will look at both actual cases of abuse of the information they collect (where such cases exist), as well as speculate on the potential for abuse. Following this analysis, we will consider steps that could be taken to minimize the potential for abuse of this data, without compromising the effectiveness of the systems themselves.

2 Prelude - Electronic Data Recorders in Aviation

The first technology we will consider is the so-called "black box", or electronic data recorder. The most visible of these today are the flight data recorders and cockpit voice recorders ubiquitous in the commercial aviation industry, where they are used with great success for post-crash analysis and reconstruction.

However, since the 1970's, major auto manufacturers such as General Motors have included "black box"-style devices in their vehicles' airbag systems, initially as a diagnostic tool. [34] While these devices collect a small amount of data, the limited information they do store has been admitted as evidence in criminal and civil cases.

Discussing the origin and legal framework surrounding aviation black boxes will give us a good starting point to begin talking about the corresponding systems in automobiles.

2.1 History

The idea of a black box was first conceived by a research scientist named David Warren in the 1950's, while working at the Aeronautical Research Laboratories in Melbourne, Australia. This was the age of the first jet-powered airliner, the British-made Comet. In 1953 the Comet was plagued by a series of unexplained crashes that gave rise to serious doubts about it's safety, and threatened the fledgling commercial aviation industry. [39]

The severity of the crashes meant that there was little evidence to be found among the wreckage, and investigators had no idea where to even begin looking for a possible cause. Dr. Warren, a chemist specializing in aviation fuel whose own father was killed in an aviation accident, was tasked with determining whether a fuel explosion could be responsible, but his attention wandered elsewhere. Warren theorized that, while the cause of the accidents was unknown to the investigators, the Comets' crews must have had some idea of what was wrong with the aircraft, and that it would be useful to have a log of the conversation on the flight deck. He wrote up a report outlining this proposal, but it generated little effect. [39]

By 1958, long after the cause of the Comet's crashes had been identified through other means, Warren had developed a prototype device that stored a looping record of the last four hours of cockpit conversation and instrument readings. It recorded information in analog form by embossing readings onto a single-use piece of metal foil. [17] Presenting this device to various Australian aviation industry organizations, reaction was decidedly poor. The Royal Australian Air Force dryly concluded that the device would "yield more expletives than explanations", and the Federation of Air Pilots stated that "no plane would take off in Australia with Big Brother listening". [39]

However, on a trip to Australia, a British official (the Secretary of the United Kingdom Air Registration Board) by the name of Sir Robert Hardingham caught wind of the device during a visit to Warren's Aeronautical Research Laboratory, and was impressed enough to convince Warren to return to England with him to conduct demonstrations. This was not the result of any pressing safety issues in British aviation, but merely a product of Hardingham's excitement over the new technology. [41]

British authorities in general apparently shared his enthusiasm, as they gave Warren money and personnel to continue the development of his device and prepare it for production use. He did so, increasing the accuracy and data capture rate of the device, as well as improving its crash resistance and fire protection. A British company approached Warren, and purchased the production rights to the device. It began to be sold commercially, both in Britain and abroad. [39]

British authorities began to move towards making the device mandatory on all civil aircraft almost as soon as Warren's team began work, but ironically, the first government to do so was Australia's, despite their initial dismissal of the concept. The first steps in this direction occurred when the team investigating the cause of a crash of a Fokker F27 in Queensland, Australia was unable to reach any definite conclusion as to the cause of the accident. The judge overseeing the investigation, upon being informed of Warren's device, "made a judicial order" requiring that all airliners in Australia be equipped with flight data recorders and cockpit voice recorders by 1963. The crash of another airliner shortly thereafter, and subsequent difficulties in investigating its cause, drove home the point. After some bureaucratic and logistical delays, Australia became the first nation worldwide to mandate the installation of FDRs and CVRs. This was the heyday of the Jet Age, and as their investigative benefits and safety benefits were realized, the required installation of data recorders became a worldwide trend. The Federal Aviation Administration in the United States made FDRs mandatory in 1964. [39, 41]

2.2 Privacy and Legal Issues

Privacy concerns are generally not raised about flight data recorders. Even the modern units in use today store only control inputs, sensor values, and instrument readings. It is hard to argue that the pilot of a commercial aircraft has a privacy interest in this information - and indeed, no one has done so in any serious manner.

However, significant concerns have arisen about cockpit voice recorders. Unlike FDRs, which store only impersonal information directly related to the operation of the aircraft, CVRs are capable of storing every second of conversation in the cockpit, between the pilots and other crew - most of which is personal conversation, unrelated to the flight, and certainly irrelevant to crash investigation. [3]

It took until 1978 for the FAA to make CVR's mandatory in the US, mostly because of resistance from the US Airline Pilots Association (ALPA). Pilots, who spend the majority of their professional working hours in the cockpit, were extremely reticent to "let Big Brother into their cockpits", even though they accepted the potential benefit to industry safety. [3]

A compromise was reached. Pilots agreed to willingly give up the privacy of what is essentially their workplace in order to assist investigators in improving safety, in exchange for certain restrictions:

1. The CVRs would be limited to recording just the past 30 minutes of cockpit conversation immediately preceding an accident.
2. The pilots would have the ability to erase the CVR recording once the plane was on the ground.
3. The CVR data would be used only for accident investigation.

Shortly after the requirement became active, however, the ALPA and other aviation organizations were unhappy to realize that the National Transportation Safety Board, responsible for accident investigations and custodian of the event recorder data, could not keep the FAA's promises. The recently-enacted Freedom of Information Act made it easy for news organizations to get their hands on data recorder logs, sometimes before the relevant NTSB investigation had even begun, and soon the previously-private conversations of airline pilots involved in incidents were being broadcast throughout the media. Often the segments that were shown on the nightly news bore little relevance to the cause of the accident, but instead consisted of particularly scandalous or off-color remarks made by the pilots prior to any trouble occurring. [40]

In response to pressure from pilots, Congress reacted in 1982 by passing legislation that attempted to limit misuse of flight data recorder logs, while still ensuring that the public had access to relevant portions of them. The new law allowed the NTSB to keep the data private for 60 days after the retrieval of the voice recorder, after which it was required to release the "relevant and pertinent" portions of the transcript - not the original, raw audio data itself. [40]

However, even this attempt still proved insufficient. As the legal industry began to realize the potential for using cockpit voice recorder data, obtained via discovery proceedings, in civil cases, the news media continued to obtain voice recorder tapes through courtroom leaks and other mishaps.

For instance: shortly after the new legislation was passed, at least two state courts accidentally ordered the release of CVR information through discovery proceedings without placing a protective order controlling its use, thus allowing the tapes to find their way to the local media, and eventually be aired nationally on the evening news. Additionally, in 1987, the New York Times published excerpts of data from the CVR retrieved out of a downed Northwest Airlines plane in Detroit, obtained through unknown means. [40]

Pilots' concerns continued to grow about the potential for their private conversations, and potentially their last words, to be used in sensationalistic courtroom demonstrations and TV news programs. [40] As Van Stewart, a retired airline captain, states:

> "There is no doubt that...many attorneys would relish the chance to have actual CVR audio and even video available for their own use. Airline pilots, however, are disturbed by such possibilities. It is potentially their dying words that would be broadcast in the courtroom for their families and, shockingly, their local television affiliates to hear. That was not the original intent of pilots' acquiescence to the introduction of CVRs into their cockpits."

The ALPA continued their lobbying efforts, pushing Congress to strengthen restrictions on the use of CVR recordings. In 1990, Congress made a final attempt to resolve the issue, by passing legislation that altered the discovery rules governing crash recorder data. The law limited the use of cockpit voice recorder tapes and transcripts in legal proceedings to only those cases where "a fair judicial proceeding cannot be had without them", and specified that a protective order limiting their distribution be issued even in those circumstances. [40]

And that is how things stand today. Yet despite this long history of attempts to limit the unauthorized and improper use of cockpit voice recorder tapes outside accident investigations, they are still regularly leaked to the media, and regularly used in the ways that the pilots of the 1960's, who agreed to give up their workplace privacy in exchange for a chance of improving public safety, feared.

Many websites now offer CVR tapes and transcripts for download. One of these, `airdisaster.net`, prefaces their archive of actual audio recordings with the following disclaimer:

> It is illegal for the National Transportation Safety Board, who regulates these recordings, to release them to the public. The recordings presented here were obtained from other legitimate sources. The airlines, who own the original recording, are legally allowed to release it if they so choose. Several others come from lawsuit settlements in which release was mandated by a court order, and yet others come from various independent investigators who chose to release the information.

Many of the audio files available on that website and others are perfect examples of what pilots were concerned about being made public. One chilling recording of the crash of Air Florida Flight 90 contains the final two minutes of cockpit conversation during the flight, just before it crashed due to ice covering a critical engine sensor:

> Pilot: Come on forward...forward, just barely climb.
> Pilot: Stalling, we're falling!
> Copilot: Larry, we're going down, Larry!
> Pilot: I KNOW!
> (sound of crash)

Both pilots died in this incident, as well as 76 other people. While the cockpit voice recorder was instrumental in determining the cause of the accident (among other things, it revealed that the pilot chose not to activate the airplane's anti-icing system, after stating to the copilot that he believed it was ineffective and "gives you a false feeling of security"), there is certainly no reason to make such a grisly recording of the two men's final moments available for the entire world to listen to.

It is clear that, despite the passage of almost 40 years since cockpit voice recorders were first mandated by the FAA, and significant efforts on the part of Congress, the information they collect is still regularly used in unauthorized and improper ways. This has had a detrimental effect on the use of this data for its intended purpose - safety investigations. The failure of the government to limit the distribution of this data has delayed the deployment of improvements to both FDRs and CVRs, under pressure from the now ever-wary ALPA.

It has even limited the ability of the government to use the information gathered for safety purposes. For instance: a potentially beneficially program proposed in 1980 that would allow the FAA to use CVR and FDR information to conduct "human factors research" was blocked by the ALPA, which was so concerned about the government's ability to safeguard the data used in this program that it authorized a "suspension of service" (e.g. an airline pilots' strike) if the program were put in place. [3]

As another example - with video recording technology continuously getting cheaper and improving in quality, the FAA and NTSB are pushing for the installation of what are termed Cockpit *Image* Recorders in airliners. These would provide investigators with a video record of the cockpit up to the moment of the crash, providing additional information on what happened. It is thought that these would prove especially useful in crashes resulting from a disagreement between the pilot and copilot. In one circumstance where such a video would have been useful, EgyptAir Flight 990, which dove into the Atlantic ocean off Nantucket

without obvious reason, there existed evidence suggesting that the copilot intended to commit suicide and fought control of the plane away from the pilot, but not enough for the NTSB to determine this as the cause, or even mention in the final report. [40]

However, the ALPA is strenuously opposed to such a requirement, fearing the appearance of even more gruesome videos on Youtube and the nightly news. In a policy statement on their website, ALPA states: ([1])

> [The CIR] represents a major invasion of privacy for pilots. Having your every move recorded by video cameras is bad enough. Despite strong U.S. laws protecting CVR and CIR tapes from public access, they can be played in court in some circumstances. Tort lawyers will find video recordings to be an irresistible gimmick to increase damage claims for pain and suffering and for alleged negligence... ...Once out in the open, a video recording can be made available on the Web from anywhere in the world, 24 hours a day, forever. As one pilot bluntly stated, "I dont want my spouse and children and grandchildren and a million strangers to be able to watch me die."

If the government had been able to exercise better control over the distribution of CVR recordings, one wonders if the ALPA and airline industry in general would be so cautious and resistant. The inability to control the purposes for which this data is used has undoubtedly harmed airline safety, by forcing airlines and pilots to reject many promising and potentially beneficial safety improvements because of the risk to their privacy.

These events set the stage for our discussion of data recording in automobiles, which has heretofore been mostly ignored by Congress and state legislatures, yet ultimately has the potential to impact the privacy of every American who drives a car - not merely commercial airline pilots.

3 Black boxes in Automobiles

3.1 The Sensing and Diagnostic Module

Let us now turn our attention to black boxes in the automobile industry. Since 1974, General Motors has shipped devices within the airbag control systems of their vehicles that are capable of recording rudimentary information about the deployment of the airbag during a crash, but in 1999 GM introduced a more advanced system that they call the "Sensing & Diagnostic Module" (SDM). [34] This system stores a wide variety of information about the 5-second period leading up to a crash, including whether the driver's seatbelt was buckled, the vehicle's speed, the engine speed, the position of the brake pedal, and the position of the throttle pedal. [34]

While initially deployed only in certain models, this device is now present in essentially all cars GM sells. GM claims that the purpose of the SDM is to enable their engineers to improve the performance of the car's airbag system, and the safety of their cars in general, ([38]) but obviously the data itself is not limited to that particular use. The information collected by the SDM could be used to show, for instance, that a driver involved in an accident on a residential street was operating his vehicle at 65 mph in 3rd gear without his seatbelt buckled, and didn't even take his foot off the throttle when a vehicle pulled out in front of him, thus triggering the deployment of the airbag.

In 1998, prior to the release of the SDM system, GM provided the module's interface specifications to Vetronix Corporation, who proceeded to use this information to produce their "Crash Data Retrieval" product. This is a hardware device that simply plugs into the ODBII diagnostic port in the dashboard of all GM (and some Ford) vehicles, and can download the information stored in the SDM module directly onto a Windows-based laptop, without requiring any help from GM, or essentially any technical expertise whatsoever. [16]

Vetronix was purchased by ETAS Group in 2003, which as of November 2007 still offered the CDR device for sale to anyone, for approximately $2,500. The device is capable of downloading data from ap-

proximately 20% of vehicles on the road in the US, and Vetronix is conducting discussions with additional manufacturers to add support for their vehicles as well. [16]

As of 2003, the NHTSA was operating a program providing federal grant money for law enforcement agencies to purchase the CDR system, and reported in that year that it was in use by at least 30 such agencies nationwide, as well as numerous insurance companies and private crash investigation agencies. [37] The website of a traffic accident reconstruction specialist lists 56 private consulting firms in the US that specialize in recovering data from EDR devices. [2]

NHTSA estimated in 2004 that between 65% and 90% of all "light vehicles" sold in that year contained EDRs. While GM remains the most prominent user of the technology, several other auto manufacturers have implemented similar devices: a NHTSA study indicated that Toyota, Daimler, Honda, and Ford all have event data recorders with capabilities equivalent to GM's SDM module, although the tools for retrieving data from them are not yet available beyond proprietary technology available only to the manufacturers themselves. [37] This, however, will soon change.

3.2 Future Developments

Event data recorder devices are still in their infancy in the automobile industry. The NHTSA, in a "Notice of Proposed Rulemaking" issued in 2004, announced their intents as to how the technology should move forward. Stopping short of requiring that the devices be included on all new cars, the NHTSA instead will propose a standardized specification for communication with EDRs that all manufacturers employing the devices must comply with. The proposed standards define a universal set of information that the devices must log, as well as standardized physical and electronic interfaces for crash investigators to download information from them. [31]

The NHTSA's new rules will go into effect in 2008. The net effect of these rules will be to allow anyone with the necessary technical expertise and/or sufficient resources to construct or buy a single device capable of downloading the data from all EDRs shipped on vehicles manufactured in that year or later, simply by plugging into a port under the dashboard. [31]

Future data recorders will also store even more information than current devices do. GM's SDM module originally recorded 5 seconds of information prior to each "crash event" - the NHTSA's proposed rules require that all EDRs be capable of storing eight seconds of data prior to a crash, as well as six seconds of data following the impact. [31] Given the ever-decreasing cost of computer-memory, it is not unreasonable to expect that many of these devices introduced in the future will be capable of recording even more information. Some devices already present on the market are capable of recording up to 45 seconds of information in total. [37]

A document prepared for NHTSA by the National Academy of Engineering lists data elements that are expected to be present in the next several generations of EDRs. Among them are:

- Wiper and headlight switch positions.
- Turn signal switch position.
- Cruise control system status.
- Status of any integrated or paired Bluetooth cellphone (e.g., on a call).
- Video image of the driver, as well as the driver's eye in particular(see section 4.1)
- Cellphone microphone input, similar to a cockpit voice recorder in an aircraft

Devices known as "Automatic Crash Notification" (ACN) systems are also in development, which immediately broadcast the contents of the EDR log over the cellular network when a crash occurs, making them available to emergency personnel. GM's Onstar system (see section 5) is one such technology that is already on the market. Standards are also in development that would allow first-responders (or anyone else equipped with the necessary receiver) to download information from the EDR wirelessly, immediately upon arriving at the crash site, without having to even touch the vehicle.

3.3 Use of Data

The NHTSA's motivation for supporting this technology is clear - they would like to be able to use the information gathered by EDR's to further their goal of improving highway safety.

NHTSA currently collects EDR data through three programs: ([15])

1. NASS-CDS, a "national statistically-sampled database, currently collecting data on about 4-5,000 crashes each year at 27 locations around the U.S."
2. SCI, a collection of targeted crash investigations looking at emerging safety issues.
3. CIREN, a system of crash investigations conducted at hospitals, involving about 400 cases per year.

It is hard to argue that these uses of anonymous, aggregated crash report information constitute a violation of privacy. Indeed, NHTSA has adopted a policy of asking for permission from the vehicle owner before downloading EDR data for use in one of these programs. [15] But the NHTSA is just one of the many organizations that gather EDR data, and will therefore benefit from their proposed, soon-to-be-effective rules standardizing data collection and retrieval. And it is one of the only such organizations that asks for permission.

For one, law enforcement agencies routinely use information gathered from these devices for accident reconstruction, and in bringing charges against the driver responsible. The legalities of the this practice are discussed in section 3.4 - but for now, suffice it to say that EDR information has been used against drivers in criminal proceedings at least 100 times, in at least 25 different states. An incomplete list of such cases is available from [14].

In many of these examples, EDR evidence was used to disprove the defendant's claim that they were obeying the speed limit. In one case, the EDR provided evidence indicating the defendant was moving at a speed of 57 mph in 35 mph zone. In another, 80 mph in a 45 mph zone. In others, the EDR's record of driver inputs was used to prove that the driver was being inattentive or otherwise incompetent. For example - in 2002, Michael Baybado's 2001 Chevrolet S-10 crossed the center line of a highway and hit a van head-on in the opposite lane, killing its driver, and injuring two passengers. The EDR indicated his speed was 45 mph, and showed no effort at braking prior to the impact. Baybado was convicted of second-degree negligent homicide. In another case, a 77-year-old woman in Texas drove her Cadillac through the wall of a post office, killing someone on the other side. The driver claimed that her vehicle accelerated on its own, but with the aid of data from the car's EDR indicating that the accelerator pedal had been depressed immediately before the crash, the victim's family was able to win a wrongful death judgement against her. [14]

Insurance companies also make use of EDR data in order to assign responsibility in claims investigations, and the ensuing civil suits. In fact, many insurance policies are worded in such a way that requires the driver to allow the insurance company access to data stored within their vehicle's EDR. EDR data is used in these situations the same way it is in criminal cases - to prove speeding, driver inattention, and so forth. Some consumer groups expect that insurance policies will one day *require* the installation of an EDR device, and the industry has already begin taking steps in this direction - see section 7.

Auto manufacturers have also used EDR logs in product liability cases to demonstrate that their vehicles did not malfunction in the manner that plaintiffs claimed. Here, the information gathered by EDRs has been primarily used by manufacturers to prove the correct operation of the airbag system. If you recall, GM's stated primary purpose for starting their EDR program in the first place was airbag system diagnostics. [36]

As an example - the plaintiff in Batiste v. General Motors claimed that he suffered severe injuries because the airbags in his 1996 Oldsmobile failed to deploy upon his collision with a guardrail and tanker truck. GM presented testimony from its own experts stating that the EDR showed no malfunction codes, and that the angle of the collision recorded in the EDR was too shallow to trigger the airbag activation. Batiste was unprepared to defend against these allegations, and lost the case via summary judgement. [36]

In another case, Bachman v. General Motors, the plaintiff claimed that the airbag in her 1996 Chevrolet Cavalier deployed for no reason, causing her to crash into a van. Her car was actually the subject of a

recall for inadvertent deployment of the airbags at slow speeds, one to three miles per hour. However, GM experts used EDR data to show that she was traveling at 16 mph when the accident occurred, well above the threshold of the recall, and consistent with the pattern of damage to the van. Experts additionally testified that the model of EDR within her Cavalier was capable of storing multiple separate "events", but had only recorded one - indicating there was no significant time separation between the airbag deployment and collision with the van.

In fact, some motorist organizations and advocates have questioned GM's claim that these devices are used for genuine product safety investigations at all, and theorized that their sole purpose is to assist GM in discrediting liability claims related to the airbag and other systems. The National Motorists Association has noted that there is no evidence that GM has ever sought to collect information from the black box of a vehicle that was not in some way connected to a product liability concern. [**?**] They have also questioned why, if the program was intended for safety purposes, GM has gone through the expense, engineering effort, and public-relations difficulty of fitting EDRs to every one of their automobiles, rather than a randomly-selected subset of willingly-participating customers. [5]

3.4 Legal Protections

EDR information enjoys very little protection in the legal system. Courts have repeatedly ruled that there is no constitutional protection of EDR data [36], given that individuals are considered to have diminished expectation of privacy when it concerns their automobile.

3.4.1 Civil Litigation

In civil litigation, EDR data is accessible through simple discovery proceedings. The primary obstacle to its use in such cases is its admissibility as evidence, for which there are two tests.

The Frye standard, established by *Frye v. United States*in 1923, requires "general acceptance in the particular field in which [the expert testimony] belongs." [38] A three-prong test emerged from this standard, requiring that the use of a scientific device be admitted into evidence if:

1. The device was built according to accepted scientific principles.
2. It was accurately constructed and in good working condition.
3. Testimony is being provided by a user qualified in using the apparatus by training and experience.

Expert testimony is normally required to prove these elements, however the court may also take "judicial notice" of such facts if they are especially well-known. [38]

The newer Daubert standard, established in 1993 in *Daubert v. Merrell Dow Pharmaceuticals*, provides a different test for admissibility of expert testimony. It requires a two-part test: that the testimony introduced be relevant to the facts of the case, and that the evidence given in the testimony be backed up by sound scientific principles. [38]

Both tests have been applied to EDR data in civil cases, and in general, it has been found to be admissible in trial courts. There have been relatively fewer decisions about the admissibility of EDR data in appeals courts, but some exist.

The US District Court for the Northern District of Texas decided that EDR data was admissible under the Daubert test, stating in its opinion that the "Hard Brake 1 Report" from a Detroit Diesel Electronic Control Unit was accurate and reliable, and mentioning evidence that "measurements from [such reports] are often used in accident reconstruction." [38]

The Frye Test was upheld by the Appellate Court of Illinois in the previously-mentioned case of *Bachman v. General Motors*, which found that the process of gathering and recording data through EDRs was not particularly new or novel, and held that the design and implementation of the EDR device met the standards required by the test. [38]

The US District Court of Connecticut, in the case of *Brill-Edwards v. Ryder Truck Rental*, issued an opinion that exempt EDR data from both the Frye and Dauber tests. The reasoning here was that the software developed by Vetronix and other manufacturers has reduced EDR information to the level of so-called "raw data": charts and graphs requiring no expert opinion or analysis. [38]

3.4.2 Criminal Cases

In criminal cases, the limitations on introducing data from EDR devices are primarily constitutional. The first question to be answered is who "owns" the data contained with an EDR, as this determines whose constitutional rights may be violated when the information is seized. NHTSA, the NTSB, and the Federal Highway Administration (FHA) all agree that ownership of EDR data lies with the owner of the vehicle, and I have found no attempts to challenge this view in a court of law.

With ownership established, we can look for constitutional protection of EDR data in two places: the 4th and 5th amendments.

The 4th amendment requires a warrant based on probable cause before a search is conducted. Obviously, the most direct way for a police officer or criminal investigator to bypass this protection is to simply obtain a warrant. In any accident investigation but the most trivial, knowledge that an EDR is installed in an involved vehicle should be more than sufficient to establish probable cause that it will contain information relevant to the investigation.

However, there are many options open to police officers looking to collect data from EDRs without a warrant. These come from the so-called "automobile exception" to warrant law, which is a very complex field. However, the components relevant to this situation can be traced back to just one case: *Carroll v. United States*. Here, the Supreme Court established that the presence of probable cause leading an officer to believe that evidence is contained within a car justified a warrantless search. In the case of EDRs, therefore, a police officer's knowledge of the presence of an EDR in a certain vehicle, combined with the knowledge that said vehicle was involved in an accident, should be sufficient probable cause to perform a warrantless search of the car, and download the EDR data. [38]

An additional point mentioned in Carroll is the exigency requirement - unlike other forms of evidence, a vehicle is mobile, and if evidence from the car (EDR logs or otherwise) is not collected as soon as possible at the scene of the (potential) crime, there is a significant risk that the owner of the vehicle will drive away and destroy it. [38]

A closely related argument, thought not tested in any court of law, would be that EDR data is simply a piece of evidence local to the crime scene that must be gathered during the course of a normal police investigation, like eyewitness testimony, skid marks on the road, debris patterns, the final resting position of the cars involved, and so forth.

Conversely, the 5th amendment provides protection against self-incrimination. However, there is fewer law applicable to the case of EDRs than existed for the 4th amendment. I will quote from a legal analysis on the issue: ([38]

> Courts should the Fifth Amendment completely inapplicable to EDRs because EDRs are "real" or "physical" evidence rather than "testimonial." As components of automobiles, EDRs record data independently of any act by the driver, save for turning the key; EDRs are therefore free of any "compulsion to extort communication," let alone any "communications" in the first instance. Even if an officer demanded that a driver permit the officer to download the automobile's EDR data, that data came into existence long before and completely independently of the officer's demands.

Essentially, the argument is that EDR data, collected by a physical device inside an automobile, is no different from other physical evidence present on an automobile - like tire marks, paint transfer, etc.

Two criminal cases provided early tests of the admissibility of EDR data in such proceedings. In the first, *People v. Christmann*, decided by the California Court of Appeals, the defendant was prosecuted for speeding and causing the death of a pedestrian. An accident reconstructionist working for the California

Highway Patrol arrived, and used a Vetronix CDR to download data from the defendant's EDR. This information was analyzed and presented at trial as evidence proving the defendant's speed at the time of the impact.

The defendant challenged the warrantless retrieval of the EDR data, but the court rejected this claim, finding that "[there is] only a diminished expectation of privacy in the mechanical areas of the vehicle which must yield to the overwhelming state interest in investigating fatal accidents." The court also recognized the exigency of this situation, mentioned above, and dismissed the defendant's claim that the EDR data was inadmissible under Frye, finding it to be reliable. [38]

In another case, *People v. Hopkins*, decided in a New York Trial Court, a warrant was actually issued for the retrieval of information from the EDR of a car believed to have left the scene of an accident. The defendant in this case challenged the probable cause that underlay the warrant, but the court found that the description of the crash and eyewitness accounts of the vehicle were sufficient to provide it. Additionally, the defendant challenged the admissibility of the EDR data, citing it to be unreliable - but the court cited numerous documents from the NHTSA and other organizations describing the widespread use of EDR data as general evidence of reliability, and stated that specific questions of reliability were only relevant to the weight of the EDR evidence, not its admissibility. [38]

3.4.3 Explicit Legal Protection

A number of states have passed laws controlling access to EDR data, but none of these statutes provide anything more than basic protection. They are all essentially based on the first statute of this type, passed in California in 2004, and now comprising section 9951 of the California Vehicle Code. It states:

1. Manufacturers must disclose the presence of an EDR in the owner's manual of all vehicles sold in California.
2. Data collected by an EDR may be downloaded without consent of the vehicle's owner:
   (a) If a court with jurisdiction to do so issues an order to retrieve the information.
   (b) For the purpose of motor vehicle safety, including medical research regarding the human body's reaction to motor vehicle accidents.
   (c) If the data is retrieved by a licensed automotive dealer or technician for the purpose of diagnosing or servicing the vehicle.

Needless to say, this statute and others like it do nothing to prevent the use of EDR data against vehicle owners - they simply make it slightly more inconvenient for law enforcement agencies and private organizations to gain access to the data.

3.5 Reaching an Opinion

Reaching a conclusion on the merits of electronic data recorders is difficult. On one hand, the use of information that recorders collect has the potential to improve driver safety, through improvements to both automobile and highway design. Clay Gabler, a professor of mechanical engineering at Virginia Tech's Center for Injury Biomechanics, has a concrete example of such an improvement - he says data from EDR records has already helped roadway engineers redesign highway guardrails to better protect people who crash into them. [10]

On the other hand, every other use of EDR data is clearly detrimental to consumer privacy - in criminal investigations, civil lawsuits, insurance claim settlements, and so forth.

The decision balancing these two factors is one that will have to be made by individual consumers, in deciding what car to purchase. They will have to make the choice between the potential safety improvements present in cars that employ EDRs, and the potential privacy concerns. They will also have to weigh their privacy against the potential safety improvements that will benefit society at large, and may be gained

from EDR data in a crash that they are personally involved in. Disabling the EDR system is not an option, as current EDR devices are highly integrated with the airbag and other safety systems, and attempting to disable them manually will often compromise their operation. An article on the subject states: "The data recording function is so thoroughly integrated into a car's electronics that there is no way to completely disable it without also disabling safety features in a way that would violate federal law." [10]

GM and other manufacturers have born a great deal of criticism about these devices. There have been countless articles published in mass-media newspapers and magazines about EDRs and their potential privacy implications, and interest groups like the American Automobile Association and National Motorists Assocation Manufacturers have lobbied manufacturers to stop including them, or at least give consumers the ability to disable them. Yet despite great public pressure, no manufacturer has been willing to give consumers the option to disable these devices, much less remove them from use entirely. Without such an ability, customers have no way to guarantee that their own vehicle will not be used by the government, or their insurance company, or any other third party, to "testify" against them.

4 Data Recorders on Steroids

The Event Data Recorders, or so-called "black boxes" that were pioneered by GM, and will soon be standardized by NHTSA, store a very limited set of information - information that, as one court decision noted, does not go beyond what a bystander at the side of the road would observe if they witnessed a crash. [36] These devices have historically been tied to the airbag system, and thus have access to only the limited set of information that the airbag system uses to evaluate whether it should deploy.

However, with the increased use of sophisticated electronic systems in modern automobiles, controlling everything from the climate control to the radio to the fuel mixture, automobiles are gaining access to far more information about their driver's actions than the comparatively ancient "black boxes". Many luxury automobiles now have full-blown embedded computers controlling everything that goes on in the cockpit. For example, the initial version of BMW's iDrive control system used Windows CE, and now uses VxWorks from Wind River. [20]

Automakers are taking advantage of the significant computing power at their disposal to implement systems that improve safety - and also systems whose benefit is merely driver convenience. But with all of these computerized control systems comes once again the potential for monitoring, and use of the data stored in these systems against the vehicle's owner. However, these new systems are capable of delivering far more explicit testimony than any black box could.

4.1 Lane Departure Warning

The first system we will look at is the idea of a lane-departure warning system. Many implementations of these systems are already on the market. They attempt to detect if a vehicle is drifting out of its current lane without the driver's activation of a turn signal, and if so, provide some kind of audio/visual/physical warning to the driver. Some systems subtly wiggle the steering wheel, others play the sound of a rumblestrip over the audio system, and others vibrate the driver's seat. [21]

The implementation of these systems vary as well - some use a camera mounted inside the vehicle, while others use infrared sensors mounted under the bumpers. Companies currently offering this technology on some or all of their vehicles are Mercedes-Benz, BMW, Infiniti, GM, Volvo, and Lexus. Some advanced versions of the system, in addition to providing alerts, are capable of dynamically adjusting the steering ratio or selectively applying the brakes to keep the vehicle in the lane, if the vibrating seat isn't annoying enough to prompt the driver to do so on their own.

The safety benefits of these systems are obvious. But what of the privacy issue? Consider the following scenario.

4.1.1 A Cautionary Tale

Jessica Smith buys a brand-new Infiniti M45 sedan. She has a one-month-old baby to take care of, and she wants a car with an excellent safety record. Entranced by the salesman's description of the lane-departure-warning system, she makes sure that the car she buys has that option.

A few weeks later, her baby is cranky, upset, and apparently sick. She puts him in the car seat and sets off for the doctor's office, 20 miles away. On the way, her baby grows increasingly more upset, and starts bawling and squirming around in the seat. Jessica twists in her seat and picks up some baby toys from the floor, and tries to placate her baby. She feels his head to make sure he hasn't developed a fever. All this while, she is not paying that much attention to the road, and relying on the lane departure warning system (which, after two months of ownership, she has grown to trust completely) to tell her when she is drifting out of her lane.

Suddenly, out of the corner of her eye, Jessica sees something in the road. She slams on the brakes, but can't stop quickly enough, and at 40 mph, slams into a pedestrian crossing at a crosswalk, killing them.

Jessica is sued by the pedestrian's family, and the police are looking to press charges of negligent homicide. Jessica argues strenuously that the pedestrian jumped out in front of her, and she had no time to react. However, the plaintiff's lawyers subpoena the contents of her car's lane departure warning computer, and download an event log indicating that the system activated itself 96 times in the 20-mile drive preceding the accident. Faced with this damning evidence, Jessica is convicted, and does not live happily ever after.

4.1.2 Manufacturer Responses

The situation described above could easily occur, if the lane departure warning system stored a history of its activations. This might be done for diagnostic or debugging purposes, as was GM's stated intent in developing the first airbag EDR's ([34]), or it might be done for liability reasons, to prove that the system was working properly in the event of a lawsuit - which, as mentioned earlier, is what some people consider to have been the actual reason driving the development of GM's systems.

Attempts to elicit additional information on this topic from manufacturers proved fruitless. The manufacturer representatives that deigned to speak to me were either unwilling to reveal the logging capabilities of their lane-departure warning systems, or uninformed about such details.

Thinking that a less direct approach might yield better results, I decided to call the service department at several dealers selling cars equipped with these systems.

The general question I posed to them was the following:

> I own a 2008 [model], with the lane-departure warning system option. I recently loaned the car to my son, who managed to bang it up a bit. I don't fully believe his story that he lost control on a patch of ice. I was wondering if the lane-departure system stored any diagnostic or logging information that could tell me, for example, that he drifted out of his lane 45 times in the 15 minutes prior to the accident.

After screwing up several of the early calls ("Now, where did you say you had the car towed?" "Errrr...*click*"), I got some answers. I called 3 BMW dealers, 3 Infiniti dealers, and 3 Lexus dealers. 1 BMW dealer and 2 Lexus dealers stated that they could not be sure about what information the car had stored without being able to physically access it, and invited me to bring it into their shop. 2 BMW dealers and all 3 Infiniti dealers stated that, while their car had a black box similar to GM's that could tell me the speed of the car at the time of the accident and other pertinent factors, they were not aware of any location where lane-departure warning logs were stored. The remaining 1 Lexus dealer denied the presence of any data recorders in the vehicle at all.

Notably, one of the BMW dealers I spoke to made the following comment: "I don't think we store any kind of logs from the lane-departure warning system...but it would be great if we did!"

Especially given the completely inaccurate response of that last Lexus dealer, I am not sure of the reliability of these results. It is quite possible that the dealers are simply unaware of the full technical capabilities of these cars - certainly, the technicians in the service department are not the same people who wrote the

software and designed the hardware that operates the lane-departure warning system, and it is possible that their diagnostic equipment is simply not designed to retrieve this sort of information.

Of course, it is equally possible that this information is just not logged at all. However, this does not eliminate the potential privacy concerns - it simply means that automakers have not currently seen the need to implement such logging. Certainly, the technical capabilities are there. I would imagine that, in time, liability concerns will drive them to add logging functionality to their lane-departure warning systems, just as GM did to their airbag system.

4.2 Collision Avoidance

A similar technology is that of collision avoidance systems. Many high-end cars now have so-called "active cruise control" systems, consisting of a radar or infrared emitter mounted on the front bumper, an associated sensor, and computer logic that automatically maintains a fixed distance to the car in front. The systems are capable of accelerating and braking in order to maintain this distance.

Recent iterations of this system operate even when cruise control is turned off, constantly monitoring the distance to the car in front, and providing an alert to the driver if he is approaching too fast. Some will even apply full braking power if they detect that the driver is not doing anything.

As is the case for lane departure warning systems, the logs from this system could be introduced as evidence to show that the driver involved in an accident was being inattentive, or even drunk (by recording, for example, moving averages of his reaction time over different timescales - e.g. the past month and the past trip). They could also be used to show that a driver had a habit of following too close on the highway, of cutting people off, and so forth.

4.2.1 Manufacturer Responses

As with lane-departure warning systems, getting solid information from manufacturers on the actual specifications of these systems was difficult, and made more so by the fact that most of them are still under development. The manufacturer's PR representatives were unwilling to reveal information that might be considered "trade secrets."

Even so, it is reasonable to hold the same expectations mentioned above - that these systems may contain some form of data logging for both troubleshooting and liability reasons. And even if current systems do not do so, the capability is clearly present, and it is easy to imagine the threat of lawsuits over crashes induced by supposedly "malfunctioning" collision avoidance systems driving a need for some kind of EDR-like capability for these systems as well.

4.3 Driver Monitoring

Another class of systems is one that I will characterize as "driver monitoring" systems. Some of these consist of cameras, infrared sensors, or similar devices pointed at the driver, use control units that employ facial recognition algorithms to monitor the driver's expression and movements - one such system calculates the frequency at which the driver's eyelids flutter, and uses this to infer his state of wakefulness ([30]). Others monitor the pattern of movement of the wheel and throttle and brake pedals ([19]), presumably watching for slow, abrupt or otherwise sloppy control inputs. Still others monitor the dilation of the driver's pupils, hoping to infer whether the driver has consumed any mind-altering substances. [23]

Volkswagen is current developing such a system [30], as are Daimler [19], Nissan [23], Volvo [9], and Toyota. [28]

At this point, the privacy implications of these systems in general should be obvious, but some deserve special mention. Volvo's system in particular is especially interesting. Here are some excerpts from an article ([9]) on the system's development:

> "The system also warns if the driver loses concentration for a reason other than fatigue. The system can detect if the driver is focusing too much on the navigation or audio systems or

children in the vehicle, issuing an audible and visual alert before control is lost"..."the driver can retrieve a safety rating about their driving style, based on consistency of performance. Included in the vehicle's trip computer, a display will provide the driver a rating, based on five stars. The less consistent the driving, the fewer stars illuminate."

One does not have to think too hard to come up with situations in which this system could work against the driver. Imagine a police officer arriving at an accident scene involving two identical, 2011 Volvo S80's. He glances inside the cockpit of the first car, and sees a glowing, green "5-star" attentiveness rating displayed on the navigation screen. He turns his head, looks into the other, and sees a flashing red "1-star" rating illuminated there. In the absence of significant other evidence, it is easy to imagine how his report of this accident will read.

Nissan has also developed a prototype of a driver-monitoring system that bears mention. In addition to the lane-departure warning capabilities already mentioned, this system integrates contact alcohol sensors into the gearshift, as well as airborne alcohol sensors throughout the cabin. If the system detects that the driver is attempting to drive drunk, it will warn the driver audibly and visually. [23]

Again, imagine the logs of this system being used against someone being prosecuted, this time for drunk driving. The defendant could claim that this was his first time ever driving drunk and he is terribly sorry, and the prosecution could produce evidence from Nissan's system that he gets hammered and drives 15 miles home in that condition every Friday.

Even Nissan admits that this system (unveiled in a concept car) is taking the idea a little too far, stating that "It is unlikely anyone would ever buy such an intrusive automobile." [23] However, it appears that Nissan's colleagues at Toyota do not agree: a recent AP report suggests that Toyota is developing such a system with the intent of using it in production automobiles by 2009, though it is unclear whether the technology will find its way to the US immediately, if at all. [28]

4.4 Electronic Control Systems

Aside from specialized systems that are purpose-built to monitor the driver's activities, other seemingly innocuous computer-control systems may pose a privacy threat as well. The Audi A8, Mercedes S-Class, and BMW 7-series all use an entirely computerized system controlled by a joystick-like knob (and some peripheral buttons) to control the operation of the radio, climate control, seat positions, and essentially all other cockpit functions. These systems have been criticized as hard to use and distracting by many reviewers and owners.

As with other systems discussed, it is certainly possible that these store a log of the driver's interactions with them, one that could be accessed by third-parties looking for evidence of the driver's wrongdoing. For instance, a defendant might be faced with the following accusation in court: "Your vehicle's computer indicates you were in the process of tuning the radio when you ran into the 87-year-old woman crossing the street."

4.5 Legalities

From a legal perspective, it is difficult to imagine any way to distinguish between this type of information, and the information stored in EDRs. All the legal precedents and arguments cited in our discussion about EDRs are relevant here - any logging functionality associated with these systems is simply an EDR that stores a different type of data.

Indeed, many of the data elements that these systems could conceivably store are part of the NHTSA's projections for what future EDRs will record.

4.6 If not Today, then Tomorrow

More than any other section in this paper, the issues raised by these technologies may not become widespread for many years. The limited evidence that I've gathered indicates that manufacturers have not implemented

EDR-like logging functionality into these next-generation, so-called "active safety" systems. This evidence may not be accurate. Even if it is, however, the absence of such functionality today does not imply the absence of such functionality tomorrow - especially given that no manufacturer has issued an official statement or policy outlining their stance on this topic.

And as I mentioned earlier, I think it is clear that manufacturers will eventually be compelled to include such logging functionality for liability reasons. Witness the success GM has had using EDR data to defend themselves against lawsuits claiming fault with their airbag system.

Imagine BMW being sued because the driver of a 2008 550i plowed into the car ahead of him, claiming that the active cruise-control feature failed. It would certainly be easier for BMW to defend themselves if they had a log indicating the ACC feature was disabled.

Or imagine Lexus being sued, because the driver of an 2011 LS600h hybrid, which has a lane-control system capable of adjusting the steering ratio to keep the car in the lane, claims it drove itself off the road and into a tree. It would be nice for Lexus if they could show that this system only corrected the steering angle by 2 degrees prior to the impact, and that it was the driver's sudden, unskilled swerving to avoid a pothole that caused the impact.

It is worth referring back to the National Academy of Sciences' report to NHTSA on electronic data recorders, which included the data elements collected by many of these next-generation systems among the potential information that may be included in next-generation EDRs - among them, video images of the cockpit, driver, and driver's eyes - easy pickings for an active driver monitoring system. See section 3.2.

If the data collected by these technologies does become a standard part of EDR systems, then it is likely that it will fall under future NHTSA rules standardizing EDR data formats and collection mechanisms - potentially meaning that anyone with access to a Vetronix CDR or similar system will be able to download all of the information described in the above sections just by plugging in a laptop under our dashboard.

4.7 Implications

Assuming that my predictions in the previous section become reality, then reaching a conclusion on the merits of these systems is much harder than considering black boxes, because unlike those crude and simplistic devices, these systems have very obvious, real, and quantifiable safety benefits. Many of them have been on the market too briefly for good data to be generated, but there are some statistics available.

Various studies cited by manufacturers in promoting their systems have concluded that drowsiness is the primary contributing factor in between 10 and 20 percent of "serious" traffic accidents. [19] In absolute figures, Volvo cites a NHTSA study that indicates approximately 100,000 collisions are caused each year by drivers who fall asleep at the wheel. [9] Volkswagen mentions a study conducted by a German traffic safety agency that blames 24% of fatal accidents on so-called "microsleep" events [30] - to say nothing of the amount of damage done by drunk drivers every year. Another NHTSA study indicates that simple "driver inattention" is responsible for as much as 80% of all crashes. [8]

While I have found no studies looking into the impact of the technologies described above on real-world crash rates (many of them are still in the prototype stage), I am willing to accept that, once widely deployed, they will have a significant effect. But are these safety improvements worth the inevitable harmful privacy consequences?

Once again, the decision between safety and convenience on the one hand, and privacy on the other hand, must be made by individual consumers. Ideally manufacturers would fully disclose the data logging capabilities of their vehicles, and allow their customers to completely disable any systems or features that are subject to logging, if they so desire. This would allow the customer to choose the tradeoff between their safety and their privacy that they are comfortable with.

5 Remote Assistance Systems - GM's OnStar

Another class of systems are the so-called "Remote Assistance Systems", of which GM's OnStar is the standard example. Other manufacturers have similar products: Mercedes' TeleAid, BMW's "BMW Assist",

and so forth.

These systems are integrated into the car's electrical system and the cellular and GPS networks, and provide various services to the driver: directions, emergency hotel reservations, summoning of tow trucks if necessary, and so forth. Usually a microphone and button are mounted in car's headliner, allowing the driver to access some of these features via a connection to a live operator. [24]

An often-touted feature of these systems is their ability to automatically summon emergency vehicles if a vehicle is involved in an accident - upon deployment of the airbags, the system automatically transmits details of the accident to the OnStar service center, and an OnStar representative is automatically connected to the vehicle's cellular telephone, allowing them to converse with people in the car and determine the severity of the accident. [24]

Newer versions of these systems have more advanced capabilities: they can unlock the car remotely if the owner is locked out, send diagnostic and service information to dealers automatically (even automatically scheduling service appointments when they are needed), remote tracking of the car if it is stolen, and even the remote disabling of the engine. [24]

The latter two features, referred to as "Stolen Vehicle Location" and "Stolen Vehicle Slowdown", allow police to locate and remotely slow your vehicle if it is stolen and being chased by police (or if the police are after you personally). They were announced on October 10, 2007. The press release GM issued describes the procedure like this: ([25])

1. Once the vehicle has been reported stolen to law enforcement, the subscriber can call OnStar and request Stolen Vehicle Location Assistance.
2. OnStar will use real-time GPS technology to attempt to pinpoint the exact location of the stolen vehicle and provide this information to law enforcement to help them recover the vehicle.
3. When law enforcement has established a clear line of sight of the stolen vehicle, law enforcement may request OnStar to slow it down remotely.
4. Safeguards will be in place to ensure that the correct vehicle is slowed down.
5. OnStar then sends a remote signal to the vehicle that interacts with the Powertrain system to reduce engine power which will slow the vehicle down gradually.

5.1 Law Enforcement

As you might expect, these systems have been used by law enforcement agencies in various ways. While they are subscription services, the systems are always on regardless of whether the subscription has been paid for or not, [24], which means that the location of the vehicle is always available to the OnStar operators. GM has stated that, because of privacy concerns, they will only release OnStar information when presented with a warrant [35] - however, it is unclear how this statement meshes with some of their advertised functionality, like the Stolen Vehicle Location process mentioned above.

In any case, this policy did not help the case of Brent Farmer and Denis Grant in 2005, when the OnStar system led to them being arrested for drunk driving in a Cadillac Escalade. Apparently both men, drunk, got into the car and started "messing around" with the OnStar emergency button. When an OnStar operator came on the line, they did not say anything to her, leading the operator to "fear for [their] safety". She contacted emergency dispatchers in the county where the men were driving, and was able to provide police with the exact location and direction of travel of their car. A State Trooper pulled them over, and both were arrested on a variety of charges. [26]

A more interesting use of the system was devised by the FBI in 2003, when they realized that the OnStar system was technically capable of using the microphone to eavesdrop on the conversation occurring inside the car, and transmitting the contents of the conversation over the cellular network. This could be done without the knowledge of anyone inside the car. They obtained a series of court orders requiring GM to

configure the OnStar system in certain suspect's automobiles in this manner. GM complied, but simultaneously challenged the FBI's authority to do so. The case made it to the Ninth Circuit Court of Appeals, who ruled that the FBI's wiretapping was illegal, but only because the use of the OnStar system in this manner disabled its other functions. The system's cellular transceiver was constantly occupied with relaying the microphone feed to the FBI - if the vehicle was in an accident, or an occupant pushed the emergency call button, nothing would happen (unless the FBI agent listening in took action himself).[33]

By Federal law, a "provider of wire or electronic communication service" is obligated to assist the FBI in conducting wiretaps, as long as such assistance is conducted "unobtrusively and with a minimum of interference with the services provided." The Court ruled that the FBI's request ran afoul of this statute, since it prevented the OnStar system from operating in the manner that the target of the eavesdropping was paying for. To quote the decision: ([33])

> Pressing the emergency button and activation of the car's airbags, instead of automatically contacting [OnStar], would simply emit a tone over the already open phone line. The FBI, however well-intentioned, is not in the business of providing emergency road services, and might well have better things to do when listening in than respond with such services... The result was that [OnStar] could no longer supply any of the various services it had promised its customer, including assurance of response in an emergency.

Presumably, if the system were technically capable of eavesdropping without compromising the performance of its other functions, the Court would not have taken issue with it - though this was not stated explicitly in their opinion.[33] And for this reason, the privacy issue in this case is not as clear-cut as in others - if the OnStar system were not available, surely the FBI would have placed a bug through other means. Since the individuals here were the subjects of a targeted investigation, not ordinary citizens un-accused of any crime, the FBI's attempt to use the OnStar system in this way simply provided them with a more cost-effective way to accomplish what they would have done otherwise. While it is unsettling that it is now so technically easy for the FBI to bug our cars, and that it would require very few resources massively abuse of this functionality, the situation is still not the same as the case of electronic data recorders, which record information on all drivers, targets of an investigation or not. The FBI does have the resources to place a bug on a few drug dealers' cars - but the police do not have the resources to place an EDR in all our cars, if the auto manufacturers had not taken care of this for them already.

5.2 Civil Cases

A source I initially consulted reported that OnStar records have been used in divorce proceedings - however, I was unable to find any primary-source evidence of this occurring.

Still, it is certainly not beyond the realm of imaginable possibilities - an OnStar representative confirmed to me that, if served with a court order requesting the location of a vehicle at a certain point in time, they could provide this. A GM dealer also told me, "off the record", that depending on which representative you talk to, it may be possible to simply call up the OnStar customer service line and request that they tell you the location of a vehicle, if you can prove ownership of it.

5.3 Implications

While OnStar is a subscription service, most of its privacy-violating functionality can be accessed by law enforcement agencies even without a subscription being paid, thus forcing especially privacy-conscious drivers to avoid GM cars entirely, as well as many models from other brands. All GM cars have been equipped with OnStar as a standard, unremovable option since the 2007 model year [24], and as stated earlier, similar technologies (some of then simple rebrandings of OnStar) are included on automobiles from other brands as well. [35]

A number of consumers and consumer-advocacy groups have spoken against OnStar. A 2004 editorial in Autoweek magazine, dating from near the introduction of a new iteration of the system, criticized the

system over privacy concerns. [**?**] Despite GM's claims that the system is only activated by accidents, Autoweek stated that the OnStar system triggered while their team was road-testing a car on a slalom course. Without warning, they heard a voice saying "Collision detected. Calling OnStar.", and were soon assuring an OnStar representative that they were not injured, and in fact, had not even come close to hitting anything.

The same article brings up additional possible abuses of the system - for instance, if you are racing your car on an autocross track, and the OnStar system falsely detects an accident and provides GM with your location, can they then deny your warranty claim if your engine dies two days later?

A similar article in Road & Track expresses negative sentiments about the system, telling the story of a man who crashed his car into the scenery on a deserted country road, and, not wanting to involve the police, chose to continue driving. The police, notified of the accident automatically by OnStar, followed a trail of coolant into a nearby orchard and arrested him (the exact charges were not described).

A humorous account of the introduction of the OnStar system's remote unlocking feature at the 1998 New York Auto Show is quoted below: ([22])

> OnStar also offers remote door locking: if you lock yourself out of your car - or walk away and leave it unlocked - you can call an toll-free number and they will hit the button for you at the OnStar Control Center in Troy, Michigan. At the auto show's Cadillac exhibit, there was universal shock when a spokesmodel described this locking feature. A nervous crowd peppered her with questions: Couldn't the signal go out accidentally and unlock every car in the country? An OnStar rep responded to this negative reaction, the first she'd heard: "Y'all are just paranoid. It doesn't bother me. I'm from Texas."

One man has created an entire website advocating the boycott of GM vehicles due to the OnStar system - `onstarprivacy.com`. He lists several actions that GM could take to satisfy him, and those who share his objections to the system:

1. Make OnStar an optional feature available for an additional cost, not standard equipment that all GM customers must pay for.
2. Include an informational plaque somewhere conspicuous on the vehicle informing purchasers that it has OnStar installed.
3. Provide simple instructions and/or an inexpensive kit allowing consumers to locate, disable and/or remove the OnStar module.
4. Buy back any vehicle that has been equipped with OnStar unbeknownst to the purchaser, or take whatever steps are necessary to remove the device at no cost upon presentation of ownership of the vehicle.
5. "Make freely available a full, complete and detailed summary of exactly what information the OnStar service and any devices may compile about a customer, their vehicle's location, driving habits or other information as well as how and the conditions under which this information is collected."

The OnStar system has undeniable benefits. GM reports that the system responds to 700 airbag deployments per month, by automatically dispatching emergency personnel to the scene of the accident, and informing them of the severity of injuries to expect. [**?**] But the privacy implications are undeniable as well.

Yet again, consumers are forced to make a very difficult choice: between the convenience and safety benefits of vehicles equipped with OnStar and systems like it, and the value they place on their personal privacy.

6 Electronic Toll Collection Systems

Let us now turn our attention to a technology very different from those that we have discussed so far.

A study prepared for the Federal Highway Administration determined that there are currently 4,630 miles of toll roads in the United States, and that the rate at which new toll roads are constructed will soon approach 150 miles per year. Most of these toll roads exist in heavily-traveled regions, with a high volume of commuter traffic - cities like Boston, Los Angeles, San Francisco, and New York. [7]

A trend in recent years has been the deployment of Electronic Toll Collection systems on many of these roads. The most widely-deployed of these systems (in terms of subscriber numbers) is the E-ZPass system used in New York, Connecticut, Rhode Island, Massachusetts, Pennsylvania, Maryland, Delaware and several other states (though it is referred to by other names in some of them, e.g. in Massachusetts as "Fast Lane"). [12] Additional systems are SunPass in Florida, FAST-TRACK in California, PikePass in Oklahoma, TxTag in Texas, MnPass in Minnesota, and I-Pass in Illinois.

These systems are beneficial both for the agencies collecting the tolls (they save a significant amount of money, compared to having to maintain and staff manned booths), and for the drivers, who enjoy a significantly quicker transit through the toll gates, as well as often a slight discount on the toll fees over cash payers.

Most of these systems are implemented using an RFID transponder mounted somewhere on the vehicle (windshield, front bumper, etc.), which is read by equipment mounted on the toll booths as the vehicle passes by. The data on the RFID tag is tied to an account in an administration system, which records the date and time the toll was paid, and the amount of the toll. Customers may either receive a bill at some regularly period, or have tolls deducted from a balance that is automatically refilled as necessary. [**?**]

But, as with the other technologies we've discussed, most drivers are not aware of (or do not think of) the potential privacy implications of using an electronic toll transponder. The convenience of the system tends to make us overlook the fact that every time we pay a toll using one of these tags, we are allowing our location at that time to be logged into a centralized database somewhere, and possibly stored there indefinitely.

And the privacy concern here is not just idle speculation. These records are frequently used against vehicle owners in both criminal and civil cases. [32] All that's required to gain access to them is a court order. To use a particularly amusing example from an article on this subject: in arguing over the custody agreement for children during a divorce proceeding, the husband could claim that he is home from work every day at 5:00 PM, only to be presented with evidence from his Fast-Lane account that he really only gets on the MassPike at 8:00 PM every day. [32]

A lawyer specializing in divorce cases had this to say about E-ZPass: "E-ZPass is an E-ZPass to go directly to divorce court, because it's an easy way to show you took the off-ramp to adultery." [13]

Reportedly, the E-ZPass system in New York received 251 court orders for toll records in 2003. [32] John Goodwin, a spokesman for the FAST-TRACK system in the San Francisco Bay Area (with a smaller number of subscribers) told me that his understanding was that the system received approximately one request each month for such records, with those requests equally split between criminal and civil cases.

Some electronic toll systems have established policies stating that they will only respond to subpoenas in criminal cases, not civil ones. The New Jersey E-ZPass system reportedly turns down approximately 30 civil subpoenas each year. [13]. Interestingly, the FBI has cited E-ZPass data as an example of data that they can currently obtain without judicial oversight, in arguing for a renewal of PATRIOT Act provisions. [35]

Data retention policies vary between these systems as well. The Illinois system explicitly states that records are maintained for only two years. [32] I was unable to get any information from the Massachusetts FAST-LANE program or the New York E-ZPass system regarding their retention policy, but Mr. Goodwin had this to say about California's FAST-TRACK system: "Records with regard to the toll transaction history on a given account are retained for as long as an account is open, and really, for all intents and purposes, retained in perpetuity."

6.1 Uses Beyond Tolls

But, the privacy issues do not end with toll collection. The transponders used in these systems are often used for other purposes as well.

For instance, looking at my FAST-LANE account logs right now, I can see that on the morning of September 3, 2007, I got onto I-90 E from I-84 E at 2:03 AM. I then exited I-90 E at exit 18 in Cambridge at 2:41 AM, 38 minutes later. Traveling 52 miles in 38 minutes, my average speed was 83 mph, well above the speed limit of 65 mph on I-90 E. Fortunately, the Massachusetts Turnpike Authority does not issue tickets based on FAST-LANE records ([18]), perhaps knowing that this would all but kill the program - but all the equipment is there to do so if they changed their minds in the future.

John Goodwin informed me of the "511" system in the San Francisco Bay Area, which uses toll tag readers spaced every quarter mile on the highways to determine the average speed of traffic flow - the time that a tag takes to traverse the space between the readers indicates how fast it is moving. He stated that this information is somehow encrypted in order to prevent it from being traceable back to a specific tag, as well as erased within 24 hours, and that it is the "absolute official policy" of the Bay Area Transit Authority to "never" use FAST TRACK information for speed enforcement. But promises aside, the technical capability is there - and with the technical capability, is the potential for abuse.

The New York E-ZPass system is used in a similar way - tag readers have been deployed along more than 150 miles of road leading into and out of New York, in an attempt to track and predict travel times for commuters. [11] The same guarantees are made about the use of this data, and the same possibility for abuse still exists. It is only the discretion and judgement of the administrators of these programs that holds it at bay.

6.2 Electronic Vehicle Registration Systems and Pay-As-You-Go Driving

An even more invasive technology than electronic toll collection systems is that of electronic vehicle registration systems. While no U.S. State seems to be considering deploying these at this point, several companies are developing and marketing them, and the tiny island nation of Bermuda is currently in the midst of an implementation. [29]

A company by the name of the TransCore claims to be the leader in these systems. Their product page covering EVR [29] describes how they work. Like electronic toll transponders, they consist of RFID chips mounted somewhere on the vehicle. But rather than read these chips only at toll booths or on highways, TransCore describes a system in which these chips are read *constantly* - at intersections, by police officers patrolling the streets, and as you drive through suburban streets. The following quote is taken directly from their website:

> "Deploying an Electronic Vehicle Registration system can help Motor Vehicle Administrators achieve increases in vehicle compliance and associated revenues by eliminating the need to rely on inefficient, manual, visual-based compliance monitoring techniques. New technology can enable automated monitor of vehicle compliance with all roadway usage regulations not just vehicle registration."

The site goes on to brag about "an automated means to screen vehicle compliance 24/7", "Improved use of law enforcement personnel via automated regulation compliance monitoring", and how their system can automatically "determine if the vehicle is stolen, non-compliant with governmental requirements, or if there are unpaid offenses. Additionally, incident reports or tickets can be generated automatically through a violation processing center." A box in the corner talks about the hazards of "non-compliance": "Did you know? Law-abiding citizens pay for those who are non-compliant with higher insurance premiums."

6.2.1 Direct from the Source

I spoke to Steven Baumhardt, Vice-President of Electronic Vehicle Registration Systems for TransCore. TransCore's system replaces ordinary vehicle registration stickers with an RFID tag attached to the wind-

shield by tamper-proof glue. The tag, in the system's standard configuration, contains only a unique number identifying the tag and allowing it to be linked to a vehicle registration record. However, the tag is capable of storing far more than this - several kilobytes of information, in fact - and Baumhardt stated that several of their customers are using this extra capacity to store additional data such as emissions test records, insurance information, and so forth.

Beyond the RFID tags, a TransCore EVR installation consists of three types of RFID readers. The first type are the fixed readers, which are permanently installed at highly-trafficked locations like highways and major intersections. These are capable of very fast scan rates, allowing them to accurately identify all cars even when traffic is moving at high speed.

The second type are "mobile" devices, which are identical to the fixed readers in capability, but are mounted on some kind of mobile platform, allowing them to be towed and temporarily installed somewhere, to augment the capacity of the network of fixed readers.

The third type are handheld devices, which have a limited range and operate on only one tag at a time, and are intended for use by meter maids and foot-patrol officers scanning parked cars.

All three of these devices are connected to a central monitoring station, where they transmit records of all cars that pass by. Here, the unique identifier on each tag is linked with the vehicle registration database, and violation reports are generated for cars operating without a valid registration, with an expired inspection, no insurance, and so forth.

The materials on the TransCore website are not explicit about many of these details. From them, I originally presumed that the "mobile" device could actually be mounted in a police car, to constantly scan the tags of nearby vehicles while an officer is driving. Surprisingly, Baumhardt stated that they do not manufacture any devices with that capability. I suggested this as a possible improvement.

While the systems are technically perfectly capable of speed enforcement, and Baumhardt acknowledges that there has been some level of interest on that front, their principal goal is to allow countries to verify that all vehicles operating on their roads have paid their registration fees, are up-to-date on their inspection requirements, are adequately insured, and so forth. As such, Baumhardt says the primary market for these systems is in "developing countries", which have very high numbers of unregistered vehicles (up to 40% in some places).

While the system does have some safety and environmental benefits, in talking to Mr. Baumhardt, it seemed clear that the primary motivation behind most deployments of this system is that it allows governments to collect millions of dollars in vehicle registration fees that their populations have heretofore been relatively successful in evading.

A secondary benefit that Baumhardt acknowledged, and one that is heavily promoted on the TransCore website, is the system's ability to track and identify vehicles that are reported as stolen, or that belong to "persons of interest" in a criminal investigation. A blurb on the site states: "Did you know? EVR can greatly aid law enforcement in the rapid identification and apprehension of vehicles reported as stolen." As an example of a case where the system would be beneficial, Baumhardt stated that it could be used to track down the subject of an "Amber Alert".

The system has already been deployed in several countries, and is under consideration (among several competing systems) in many others. Baumhardt told me that Brazil has passed a law mandating that its motor vehicle departments deploy electronic vehicle registration systems by 2009, and Mexico has passed similar legislation as well. He conducted our conversation from the airport lounge in Sao Paulo, Brazil.

6.2.2 Bermuda

TransCore's first EVR deployment was in the small, 21-square mile island nation of Bermuda. With the highest per-capita GDP of any nation in the world as of 2005 [6], this does not fit neatly into the category of "developing nation". Here, in addition to the standard benefits expressed above, the system also enforces time-based access control to certain roads - for instance, commercial vehicles are not allowed in congested areas during the day. Bermuda began the transition to EVR in April 2007, and it will be completed by June 2008. The Government of Bermuda estimates that the system will generate $11 million dollars of revenue over the next 5 years. **[?]**

The Bermuda Transportation Control Department posted a Frequently-Asked Questions document about the EVR system deployment, which has since been taken down, but lives on in the Google cache (see [**?**]). It recognizes and attempts to the address the privacy concerns surrounding the EVR system.

The document uses similar language as TransCore's marketing materials in justifying and explaining the system. It says that the EVR system will make verifying motor vehicle registration more efficient for the goernment, as well "more equitable for Bermudians" because it is "less random". It also says that the system will free up the Bermudian police to focus on "higher-priority community goals".

A question in the document reads "Will Electronic Vehicle Registration allow law enforcement agents to track the whereabouts of Bermuda citizens?", and it answers a definite "No". It also states that "Electronic Vehicle Registration is simply not practical for real-time surveillance of vehicles." Both of these claims are in direct contradiction to what is described on TransCore's website about it's law-enforcement benefits, as well as Baumhardt's personal statements to me about Bermuda's EVR installation. Another question in the document is "Are EVR tags on automobiles just one more sign that citizens are losing their right to privacy", to which the given answer begins: "The issue here is not really about privacy."

When queried about the use of the system in the United States, Baumhardt said that TransCore was not actively marketing it here, for two reasons. The first was that the rate of non-compliance with vehicle registration is much lower in the United States, and thus there is less profit motive for state motor vehicle departments to install the system. Curiously however, another of the many "Did you know?" blurbs on the TransCore website reads "As a result of registration non-compliance, states [in the US] lose an estimated $720 million to $1.44 billion in annual revenue." [29]

The second factor Baumhardt cited was the "perception" of privacy issues inherent to the system, acknowledging that any attempt to deploy a system like this in the US would face stiff opposition. He opined that this was primarily a matter of education - that the TransCore EVR system was no more invasive to personal privacy than a cell phone or electronic toll transponders. Of course, cell phones can be turned off, and electronic toll transponders are attached with velcro, not tamper-proof glue.

Obviously, the use of a system such as this in U.S. state would be even more worrisome than any of the other systems we've discussed, as there would be no way to opt-out of it - even if you bought a cheap car with no electronics, and paid for your tolls in cash, you'd still be subject to constant monitoring for "compliance".

6.3 Legality of Use

As with other issues relating to automobiles, the courts do not recognize an inherent right to privacy in electronic toll or registration information, reasoning that drivers do not have an expectation of privacy in where their vehicles go on public roads. [32]

7 The Insurance Industry

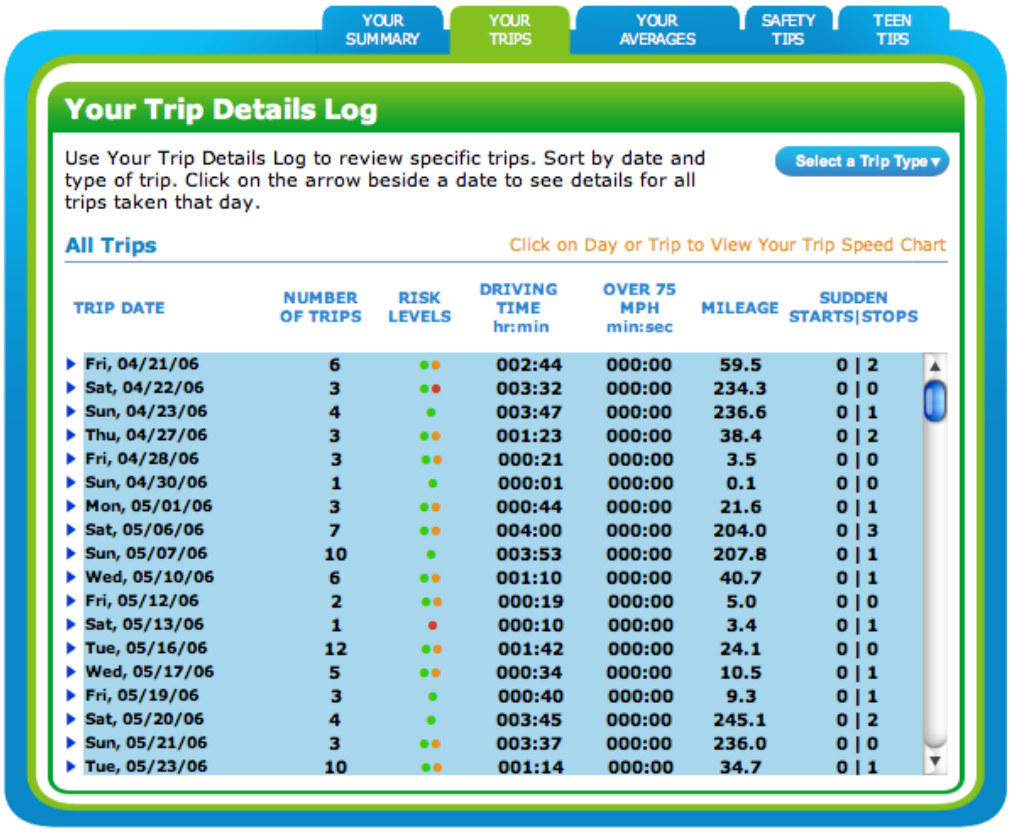
Law enforcement is one of the primary users of the technologies we have discussed. But one of the most eager users of the data gathered by these systems is the insurance industry.

Insurance companies are already making good use of event-data recorder ("black box") data, with claim investigators routinely downloading the information from these devices. The information logged within them can help in assigning blame in accidents, identifying fraudulent claims, and adjust injury compensation amounts - for example, many policies contain language that reduces the amount of compensation if the vehicle occupants were not wearing seatbelts, or if the driver was speeding excessively [36], both pieces of information that event data recorders can provide.

Insurance companies often include language in their policies that specifies drivers must consent to allowing the company to inspect the contents of their vehicle's data recorders, getting around the requirements passed by some state legislatures that such data be only accessible with the driver's permission. Additionally, the rules of discovery in litigation proceedings allow companies to retrieve data recorder logs from the vehicles of other involved parties as well. [36]

While my conversations with insurance company representatives indicate that companies are not yet aware of the potential for data harvesting from the more advanced automotive systems discussed in section 4, their behavior up to the present indicates that they will not let this opportunity to gather more information on their customers pass by.

7.1 GPS Tracking in Insurance



TRIP DATE	NUMBER OF TRIPS	RISK LEVELS	DRIVING TIME hr:min	OVER 75 MPH min:sec	MILEAGE	SUDDEN STARTS|STOPS
Fri, 04/21/06	6		002:44	000:00	59.5	0 | 2
Sat, 04/22/06	3		003:32	000:00	234.3	0 | 0
Sun, 04/23/06	4		003:47	000:00	236.6	0 | 1
Thu, 04/27/06	3		001:23	000:00	38.4	0 | 2
Fri, 04/28/06	3		000:21	000:00	3.5	0 | 0
Sun, 04/30/06	1		000:01	000:00	0.1	0 | 0
Mon, 05/01/06	3		000:44	000:00	21.6	0 | 1
Sat, 05/06/06	7		004:00	000:00	204.0	0 | 3
Sun, 05/07/06	10		003:53	000:00	207.8	0 | 1
Wed, 05/10/06	6		001:10	000:00	40.7	0 | 1
Fri, 05/12/06	2		000:19	000:00	5.0	0 | 0
Sat, 05/13/06	1		000:10	000:00	3.4	0 | 1
Tue, 05/16/06	12		001:42	000:00	24.1	0 | 0
Wed, 05/17/06	5		000:34	000:00	10.5	0 | 1
Fri, 05/19/06	3		000:40	000:00	9.3	0 | 1
Sat, 05/20/06	4		003:45	000:00	245.1	0 | 2
Sun, 05/21/06	3		003:37	000:00	236.0	0 | 0
Tue, 05/23/06	10		001:14	000:00	34.7	0 | 1

Figure 1: Progressive TripSense system trip overview report.

The worry here is that insurance companies will begin to enjoy having access to the additional information that event data recorders provide, and possibly make their use mandatory for all policyholders - thus making this information available to law enforcement. A large number of companies offer substantial "discounts" (up to 33%) if the policyholder is willing to install GPS-based anti-theft system in their car, capable of locating it remotely if it is stolen (or, if law enforcement is curious as to the whereabouts of its owner).

Some companies have begun taking steps down an even more worrisome path, by initiating pilot programs that offer premium "discounts" for customers who are willing to submit to having devices installed in their cars that monitor not just their location but their driving habits, through GPS or other means.

Dan Jacobs of MobileTeenGPS, the company behind the GPS technology underlying a number of these programs, told me in a phone interview that the insurance industry as a whole is moving towards the increasing use of telematics in private automobiles to provide premium discounts. He said that this has been common practice in the commercial trucking industry for years, with essentially all insurers offering significant discounts for trucks with GPS devices installed.

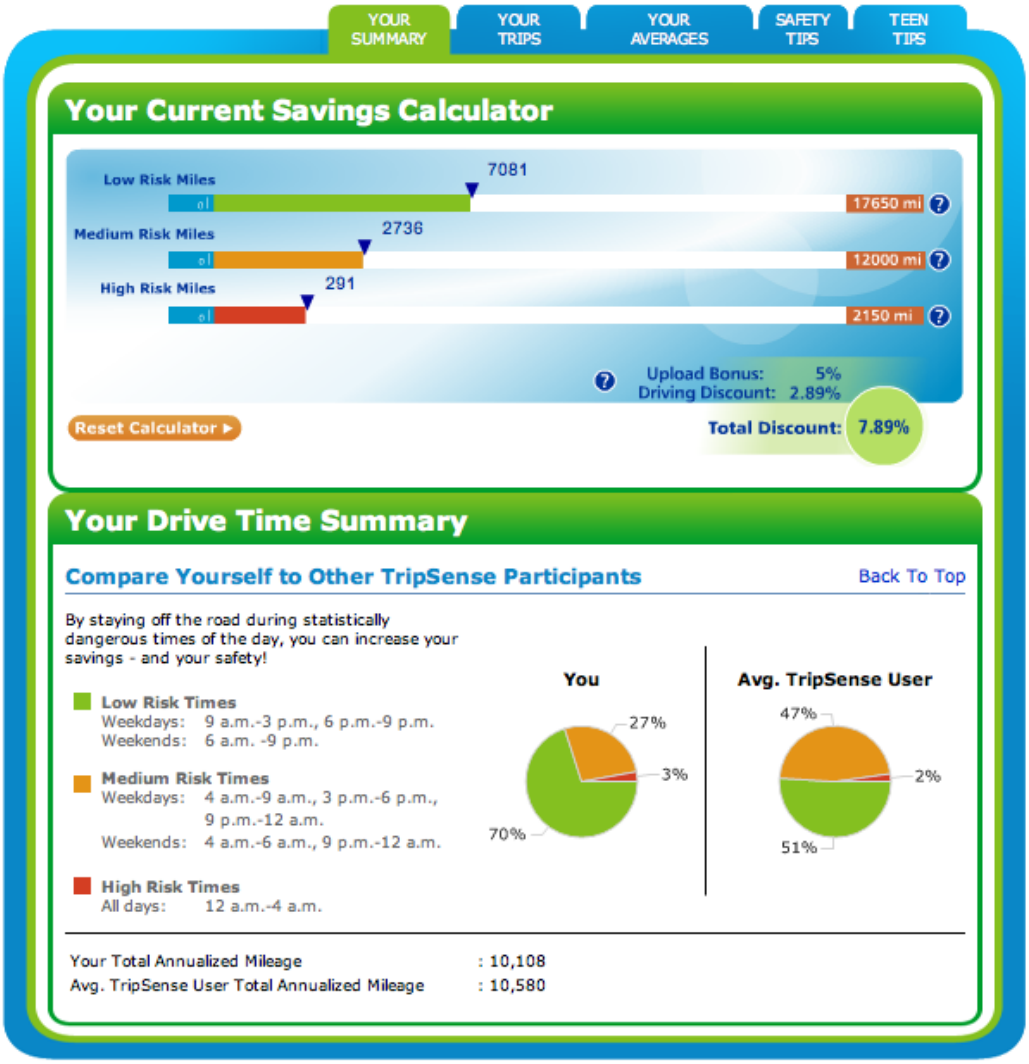


Figure 2: Progressive TripSense system summary report.

7.1.1 Progressive's TripSense

One such program in the private auto industry is Progressive's "TripSense". [27] This program, available to the company's customers in Michigan, Oregon and Minnesota, consists of a device (the "TripSensor") that plugs into a car's engine diagnostics port. It records the following information about each trip the car takes:

1. The trip's starting time
2. The trip's ending time
3. The number of miles driven during the trip
4. The duration of the trip
5. The number of "sudden starts" occurring during the trip

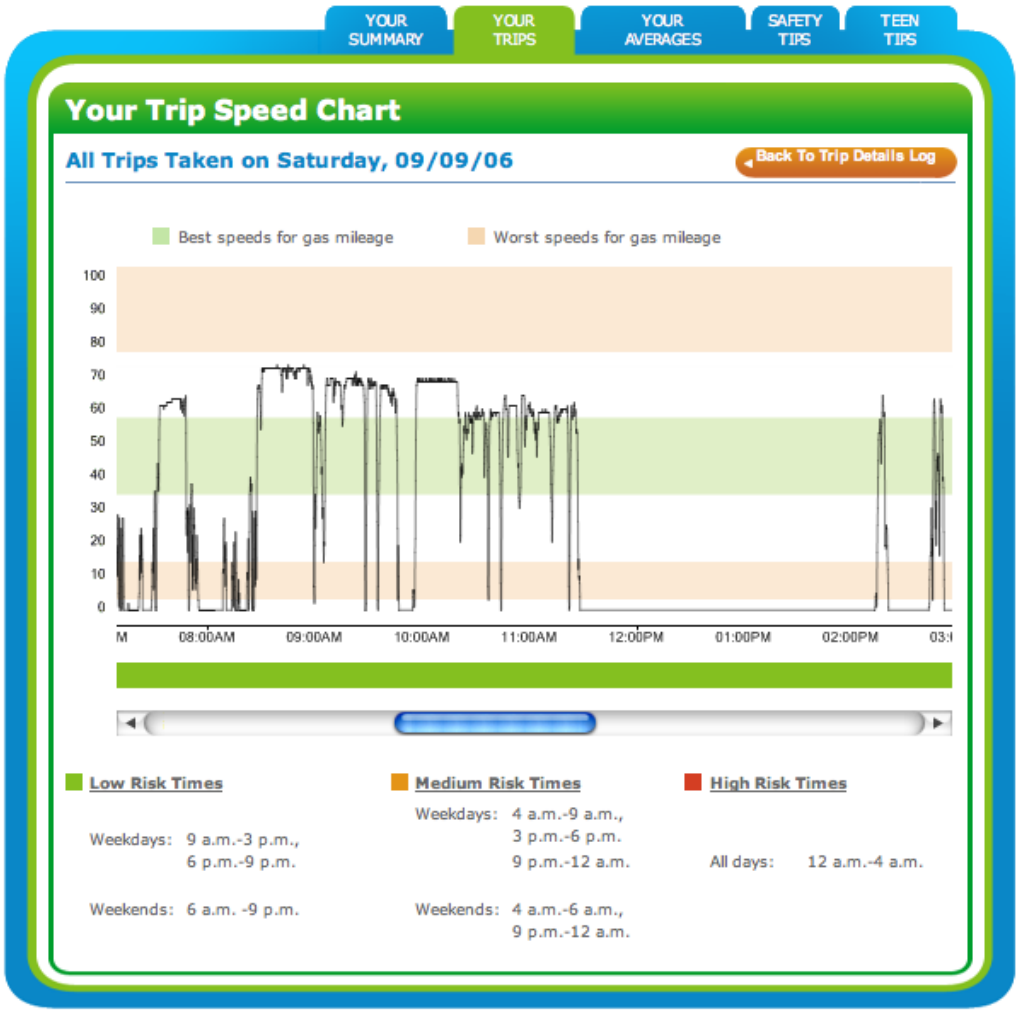


Figure 3: Progressive TripSense system trip detail report.

6. The number of "sudden stops" occurring during the trip
7. The duration the vehicle spend traveling over 75 mph during the trip
8. The time and date of each time the device is disconnected (too many disconnections will disqualify the driver).

The driver is periodically reminded to disconnect the TripSense device from his car and connect it to his computer, where the data gathered is analyzed, and the potential discount he can collect is calculated. If the driver so chooses, he can upload the TripSense logs to Prudential, who will then apply the discount to his policy.

The discount is calculated based on driving habits - it classifies your driving as "high risk", "medium risk", or "low risk", based on the number of miles you drive during certain parts of the day, how much time you spend above 75 mph, and how aggressively you accelerate and decelerate. Some examples of the reports generated by the system are included in figures 1, 2, and 3.

This data collected by the TripSensor device amounts to an enormously extended version of that collected by GM's event data recorders. Rather than just a few seconds worth of information, it can capture

a vehicle's driving history over an entire month or more. And the data within the "TripSensor" device is subject to the same access by law enforcement as the data within an EDR.

7.1.2 AIG and Safeco

Other companies have introduced similar programs involving GPS technology. Both AIG and SafeCo insurance have introduced GPS-tracking systems aimed at teenage drivers, called "MobileTeenGPS" [**?**] and "Teensurance" [**?**], respectively. These systems allow parents to keep track of the speed and velocity of their children's car at all times, as well as receive emails or text messages when it exceeds a certain speed, passes a predefined boundary, or is started up outside of a specified time window.

SafeCo charges extra for the privilege of using their Teensurance program, while AIG is offering it as a free service to select customers in certain states. Unlike Progressive, neither company offers a discount on insurance rates for participating in their pilots, instead using the "parental supervision" features to motivate people to participate. The SafeCo Teensurance website (`http://teensurance.com`) is filled with marketing material along those lines:

- "24/7 Roadside Assistance - There when you can't be."
- "Know your teen is driving responsibly. Know immediately if he isn't."
- "Seeing where she is helps you know she's safe."
- "Its all about providing parents peace of mind while teens earn their freedom."
- "A professionally installed GPS monitoring device that enables curfew reminders."
- "Your teen was heading to a friend's house across town; how can you be sure he made it there all right? With the Safety Beacon, you can know your teen arrived safely, even when they forget to check in."

All three companies have stated that their goal in these conducting these programs is to evaluate the effectiveness of the data collected by these types of devices in predicting accident rates.

When I asked an AIG representative about the potential privacy implications of their monitoring system, inquiring about what data was stored, for how long, and whether it could be tied back to the original driver if subpoenaed in a criminal investigation, she declined to answer directly, instead directing me to AIG's press release announcing the program. However, the press release [4] does not specify anything about what practices are being taken to protect this information, merely that it will not be used to affect the rates or renewal eligibility of the policyholder.

Dan Jacobs of MobileTeenGPS, while stating that his ability to answer was limited by a non-disclosure agreement in place between his company and AIG, stated that he was not aware of AIG taking any steps to secure the information it collects against from being used against their customers in criminal investigations, and suggested that a lawyer who knew of the existence of this information would be able to obtain it.

7.2 Implications

The privacy implications of these technologies and insurance industry practices are worrisome. While the insurance companies carefully refer to these programs as offering "discounts", putting them into widespread use would be equivalent to issuing a surcharge to customers who are unwilling to compromise their privacy by granting their insurance company (and thus, indirectly, the government) access to information about their driving habits and destinations. Again, consumers would be forced to make a choice, balancing their privacy against, this time, their wallet.

8 Conclusion

The slew of new systems deployed and soon-to-be deployed on the automotive market today provide an enormous potential for privacy abuses, one that remains mostly unrealized by law enforcement, insurance companies, the government, and the legal system in general. The fact that most people remain ignorant of the potential privacy implications of these systems makes them ever more dangerous, as no significant efforts have been taken to protect the information they collect. These systems, while mostly in the conceptual and planning stages now, will soon become ubiquitous, as the electronics underlying them become ever cheaper - and it is important that we take action now to limit their impact on personal privacy, before they become so widely deployed that this impact is enormous, and impossible to control.

The facts are simple. Society will soon have the technology to monitor every action that we take in our cars, not through government systems intended to do so directly, but primarily through the safety, convenience and economic systems meant simply to improve our lives. Through the technologies I've discussed, law enforcement will be able to determine the origin and destination of every trip we make, how fast we drive getting there, what drugs we had in our systems while doing so, how rested we were when we started, how long we spent with our eyes off the road adjusting the radio, how many times we performed a "rolling stop" at a stop sign, how many times we broke the speed limit (and for how long, and by what degree) - and countless other facts about our behavior.

The legal system currently provides only limited protection in these matters. Courts have repeatedly ruled that we have an extremely limited expectation of privacy in our automobiles and where we go with them, and that there is no issue with the use of information gathered by these technologies by law enforcement.

So, the easy solution to propose is that of consumer notification and informed choice. Auto manufacturers should inform their customers about what data-monitoring technologies are installed in their cars, give their customers the ability to completely disable event data recorders, lane departure warning systems, and remote-assistance monitoring systems, insurance companies should allow customers who don't wish to subject themselves to GPS tracking to abstain from such programs (possibly putting up with a surcharge), electronic toll collections and registration systems should never be made mandatory, and so forth.

And that, certainly, is a reasonable position to take, at first glance. After all, we're a free society, all about choice. But is this really an optimal outcome? Such a scheme forces consumers to choose between protecting their own privacy, and participating in technological progress - and all the associated advantages that such progress brings to their safety, their budget, and their convenience. This is not a fair choice to force people to make. One might even argue that it is unethical to force people to make such a choice.

Instead, what is needed is a fundamental re-evaluation of how we think about privacy in the automobile. The mere fact that we operate our automobiles in public should not mean that we have no expectation of privacy in the information contained in their computer systems - or that we do not expect privacy in what we do at 2:00 AM on a deserted, backcountry road.

An opposing argument might say that the systems discussed do nothing but merely "enhance the senses" of the police, collecting no more information than they might be able to gather from eyewitnesses at the scene. But this argument is misleading. With the increasingly widespread deployment of systems capable of recording data in automobiles, allowing law enforcement to have access to this information does not merely "enhance" their senses - it magnifies their sensitivity a million times, and makes the government and police nearly omniscient when it comes to what we do in our cars. This provides the government with several orders of magnitude more information and control over us than it has ever had, with precious little we can do about it.

We do not want to live in a police state, where the government is capable of monitoring our every move, and taking action against every minor infraction we commit. Congress and state legislatures should act to *create*, in law, an expectation of privacy in the contents of our automobile's computer systems, and allow all Americans to enjoy the benefits that automotive technology will bring us in the coming years, without the worry of having to decide whether these benefits are worth the loss of privacy they would otherwise surely entail.

References

[1]

[2] http://www.harristechnical.com/cdr4.htm.

[3] Access to data; privacy, proprietary and union issues. http://www.ntsb.gov/events/symp_rec/proceedings/authors/fenwick.htm.

[4] Aig auto insurance launches gps based teen driver pilot program. http://ir.aigcorporate.com/phoenix.zhtml?c=76115&p=irol-newsArticle&ID=982756&highlight=.

[5] Black boxes (event data recorders). http://www.motorists.org/edr/.

[6] Cia world factbook - bermuda. https://www.cia.gov/library/publications/the-world-factbook/geos/bd.html.

[7] Curren toll road activity in the u.s. http://www.fhwa.dot.gov/ppp/toll_survey_0906.pdf.

[8] Distracted driving, cell phone use, and motor vehicle crashes. http://www.teamster.org/resources/sh/factsheets/cellphones.pdf.

[9] Driver's sleep alarm from volvo. http://www.theautochannel.com/news/2005/11/30/151705.html.

[10] Driving big brother. http://www.wired.com/politics/security/news/2005/06/67952.

[11] E-z does it. http://nymag.com/nymetro/travel/features/2182/.

[12] E-zpass facilities information. http://www.ezpass.com/static/info/facilities.shtml.

[13] E-zpass records out cheaters in divorce court. http://www.msnbc.msn.com/id/20216302/.

[14] Edr case law. http://www.harristechnical.com/cdr5.htm.

[15] Edr: Developments and challenges - government perspective. http://www-nrd.nhtsa.dot.gov/pdf/nrd-01/SAE/SAE2004/EDR-GovtPerspective_Brophy.pdf.

[16] Etas edr product page. http://www.etas.com/en/products/1295.php.

[17] History of flight recorders. http://www.l-3ar.com/html/history.html.

[18] How fast lane works. http://masspike.com/travel/fastlane/works.html.

[19] Mercedes-benz developing warning system for motorists. http://www.cruisecontrolradio.com/MBwarningsystem.cfm.

[20] Microsoft technology hits the road in bmw 7 series. http://www.microsoft.com/presspass/press/2002/mar02/03-04BMWpr.mspx.

[21] Mobileye product page. http://www.mobileye-vision.com/default.asp?PageID=221.

[22] New york auto show. http://www.bffthing.demon.co.uk/html/t8/NYautoshow.htm.

[23] Nissan concept car to showcase anti drunk-driving technology. http://www.theautochannel.com/news/2007/08/03/057160.html.

[24] Onstar by gm homepage (various subpages). http://www.onstar.com.

[25] Onstar debuts stolen vehicle slowdown service. http://www.autoblog.com/2007/10/09/onstar-debuts-stolen-vehicle-slowdown-service/.

[26] Onstar leads police to drunken drivers. http://www.themorningsun.com/stories/120205/loc_onstar001.shtml.

[27] Progressive tripsense program description. https://tripsense.progressive.com/.

[28] Toyota developing drunken driving system. http://www.breitbart.com/article.php?id=D8MDILP82&show_article=1.

[29] Transcore evr overview. http://www.transcore.com/I&A/evr/default.html.

[30] Volkswagen provides a preview of a new driver assistance system. http://www.automotoportal.com/article/volkswagen-provides-a-preview-of-a-new-driver-assistance-system.

[31] National Highway Traffic Safety Administration. Notice of proposed rulemaking (49 cfr part 563). 69(113).

[32] Benjamin Burnham. Hitching a ride: Every time you take a drive, the government is riding with you. *John Marshall Law Review*, 1499(39), 2006.

[33] UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT. The company vs. united states of america, December 2002.

[34] International Symposium on Transportation Recorders. *Recording Automotive Crash Event Data*, May 1999.

[35] Aleecia M. McDonald and Lorrie Faith Cranor. How technology drives vehicular privacy, 2006.

[36] Patrick R. Mueller. Protecting driver privacy in event data recorder information. *Wisconsin Law Review*, (135), 2006.

[37] National Highway Traffic Safety Agency. *Event Data Recorders - Summary of Findings - Final Report*, August 2001.

[38] Kevin J. Powers. Automotive black boxes in criminal law. *Suffolk University Law Review*, 39(289), 2005.

[39] Defense Science and Technology Organization. The history of the black box. Technical report.

[40] Van Stewart. The bright line rule in the use of cockpit voice recorder tapes. *CommLaw Conspectus*, 389(11), 2003.

[41] David Uris. Big brother and a little black box: The effect of scientific evidence on privacy rights. *Santa Clara Law Review*, 42, 2002.