Draft paper to appear in *I/S: A Journal of Law and Policy for the Information Society*.

How Technology Drives Vehicular Privacy

ALEECIA M. MCDONALD[1] & LORRIE FAITH CRANOR[2]

ABSTRACT

Technological changes in the past twenty years have contributed to decreased privacy in privately owned vehicles in the United States. This paper presents six areas in which new technologies have privacy-invasive aspects that many people fail to fully appreciate: "black boxes" (EDRs) in cars, traffic cameras, OnStar, GPS transponders attached to cars, EZ-PASS (an RFID-based highway toll system), and proposals for new use taxes based on where and when people drive. This survey is useful in understanding the cumulative effect of new technologies, rather than just examining each in isolation.

I. INTRODUCTION

The public is largely unaware of the potential for privacy invasion that rides along with the newest gadgets in their cars. This paper provides information about how newer automotive technologies work, what they were originally designed to do, and the additional privacy-invasive purposes new technologies may be used for. These additional purposes often come as a surprise to car owners.

Many papers about threats to privacy tend to focus on one issue at a time, for example the risk of a ``black box'' in a car that tells police the driver's speed prior to a car crash. This paper catalogs a variety of different technologies and the threats they present. In addition to the convenience of one paper that summarizes several major threats to vehicular privacy, this approach also emphasizes just how much privacy we've lost — in many cases, with little or no public debate.

Cellular phones pose their own set of privacy concerns. Uncertain regulatory rules spawned industry guidelines on location-based services.[3] While people in cars can be tracked by their cell phones, we see this as an issue that happens to overlap with traveling in a car, rather than an issue specific to vehicular privacy. As such, we do not address cell phones specifically in this paper. That said, we would be remiss if we did not note that

---

[1] (aleecia @ aleecia . com), MS student, H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, Pittsburgh PA 15213

[2] lorrie @ acm . org), Associate Research Professor, Computer Science and Engineering & Public Policy, Carnegie Mellon University, Pittsburgh PA 15213

[3] Kupres, M., Ed. *Wireless Location Privacy: Law and Policy in the U.S., EU and Japan* (Reston, Virginia, 2003), ISOC, The Internet Society. http://www.isoc.org/briefings/015/index.shtml Accessed 16 October 2005.

cell phones can be used to track traffic congestion, which is a use of cellular technology specific to vehicular privacy. For example, the Missouri Department of Transportation plans to use cell phone location data to track traffic conditions on 5,500 miles of major roads.[4]

In this paper we first summarize the legal context for vehicular privacy in the United States. This is particularly relevant in understanding how law enforcement and government agencies can obtain and use information.

Next we turn to technology issues in six areas: black boxes in cars, traffic cameras, OnStar, GPS transponders attached to cars, EZ-PASS and other RFID-based highway toll systems, and highway use tax proposals. Again, these areas are specifically limited to implementations in the United States.

In conclusion, we look at the types of privacy threats posed by each of the six technologies, and we consider how those technologies can be combined to erode privacy even further.

II. AUTOMOTIVE PRIVACY IN THE UNITED STATES

A. Legal environment

While there is no right to privacy explicitly codified in the United States Constitution, the Fourth Amendment does provide some protection:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[5]

While one has some expectation of privacy in one's own home, courts have narrowed privacy rights with regard to cars since the Supreme Court ruled in Carroll v. U.S. in 1925[6] — only 17 years after the introduction of the Model T.[7]

FindLaw's annotated Fourth Amendment is a good overview of the legal context.[8] Reasoning for reduced privacy in cars includes:

---

[4] Lieb, D. A. Mo. may track cell phones for traffic data, October 2005. http://abcnews.go.com/Technology/wireStory?id=1214736 Accessed 16 October 2005.

[5] United States Constitution, Amendment IV, December 1791. http://www.usconstitution.net/const.html#Am4 Accessed 14 October 2005.

[6] Carroll v. U.S., March 1925. 267 U.S. 132 (1925). http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=267&invol=132 Accessed 14 October 2005.

[7] Ford motor company - history. http://www.ford.com/en/heritage/history/default.htm Accessed 14 October 2005.

[8] FindLaw. U.S. Constitution: Fourth Amendment annotations. http://caselaw.lp.findlaw.com/data/constitution/amendment04/03.html#f55. Accessed 15 October 2005.

- Because cars are mobile, it is unreasonable to expect a police officer to be able to get a warrant to search a car before it moves. Therefore, in some cases no warrant is required.[9]
- Because cars use "public thoroughfares where both its occupants and its contents are in plain view," there is a lower expectation of privacy for vehicles.[10]
- Because people riding in a car have no expectation of privacy, the contents of a car may not be private either[11] — police can search a closed suitcase or a glove compartment without a warrant after they have arrested the driver on unrelated charges.[12]

More recently, the Supreme Court upheld a ruling in Illinois v. Caballes that police can conduct a search based on a dog sniffing drugs in a car — even when there's no probable cause to bring the dog to the car to begin with. Justice Stevens' reasoning included his view that there is no expectation to privacy for illegal activities.[13] Further case law may determine if speeding is likewise an illegal activity that bars expectations of privacy.

In general, the Supreme Court has ruled in favor of law enforcement's interest to search cars over the car owner's privacy interests. Consequently, some privacy advocates have largely given up on the courts. Instead, they look to solutions from regulatory boards, new legislation, or new technologies.

B. Common Characteristics of Privacy Threats

Many specific vehicular privacy invasions are comparatively new, and have come about as a result of changes in technology. However, at a more general level, the backdrop for vehicular privacy threats looks much the same as other categories of privacy loss. There are two main concerns, mission creep and deliberate abuse.

Privacy advocates warn of "mission creep":[14] the government (or private corporations) collect data for one purpose, but once they have the data they find new

---

[9] Carroll v. U.S., March 1925. 267 U.S. 132 (1925). http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=267&invol=132 Accessed 14 October 2005.

[10] Cardwell v. Lewis, June 1974. 417 U.S. 583 (1974). http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=417&invol=583#590 Accessed 15 October 2005.

[11] Rakas v. Illinois, December 1978. 439 U.S. 128 (1978). http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=439&invol=128 Accessed 15 October 2005.

[12] Colorado v. Bertine, January 1987. 479 U.S. 367 (1987). http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=479&invol=367 Accessed 15 October 2005.

[13] Dorf, M. C. The Supreme Court upholds suspicionless dog sniffs. FindLaw's Writ (February 2005). http://writ.news.findlaw.com/dorf/20050201.html Accessed 8 December 2005.

[14] Lieb, D. A. Mo. may track cell phones for traffic data, October 2005. http://abcnews.go.com/Technology/wireStory?id=1214736 Accessed 16 October 2005.

ways to use it. For example, New York introduced Metrocards for the subway system to replace tokens and allow riders to use one payment method across transit types. Within a month of installing Metrocard stations in subways, the police used Metrocard data to track a suspect.[15, 16] More recently, the FBI told Congress that the PATRIOT Act is important in part because now the FBI can track people by their electronic highway toll payment system without waiting for Judicial oversight.[17]

Some technologies also have multiple primary purposes. For example, some cities have both red light cameras and cameras to measure traffic flow. These are different systems with different goals. This is not a case of cameras being used in secondary ways, but rather shows there are multiple primary purposes for cameras pointed at vehicular traffic.

In addition, there is the potential for deliberate abuse of the data collected. IRS employees comb through the tax files of famous people, prospective dates, and neighbors. The IRS has also looked at files of people critical of them — including people who did nothing more than write letters to the editor.[18] Even when it is illegal to browse files, as it is for IRS employees, abuse remains a risk. This risk increases when systems collect more personal information than they need, and when information is stored indefinitely.

It's human nature to use the tools we have. Sometimes that leads to new uses for existing data, and sometimes it leads to abuse. We recommend designing systems with mission creep and abuse in mind, and thinking about ways to mitigate risks prior to launching new systems.

III. Six Technologies Considered

We consider six technologies that may affect vehicular privacy. Five have already been deployed; highway use taxes are still in the proposal stage. After discussing each in turn, we summarize the privacy threats they pose.

---

[15] New York city transit - history and chronology. http://www.mta.nyc.ny.us/nyct/facts/ffhist.htm Accessed 15 February 2006.

[16] Peneberg, A. L. The surveillance society. Wired 9, 12 (December 2001). http://www.wired.com/wired/archive/9.12/surveillancepr.html.

[17] Caproni, V. Bill to reauthorize certain provisions of the USA PATRIOT Act and for other purposes, May 2005. Transcript of Ms. Caproni's testimony available from http://intelligence.senate.gov/0505hrg/050524/witness.htm Accessed 23 October, 2005. Testimony regarding toll systems was during question and answer. Information from author's notes.

[18] Oversight hearing on the Internal Revenue Service, September 1997. http://enzi.senate.gov/anon3.htm Accessed 23 October 2005.

A. Black boxes

Many people are familiar with the phrase "black box" in the context of airplanes — devices that record the conditions in the vehicle right before a crash.[19] Many cars have similar black boxes, also known as Event Data Recorders (EDRs).[20] As of May, 2005, about 25 million cars in the United States had EDRs.[21] Most people don't know if they have an EDR in their car. About two-thirds of Americans don't even know cars can have event recorders at all.[22]

i) How they work

EDRs sit under the front seat in a car and collect information from the car's systems.[23] EDRs are usually installed at the time cars are manufactured, but there are also after-market EDRs that can be installed.[24]

Cars moved from mechanical systems to electronic systems about 20 years ago. Electronic systems monitor different parts of a car with a set of sensors. An Electronic Control Unit (ECU) collects information from sensors, processes the information, and sends instructions to various subsystems. EDRs capture electronic information and store it for a brief span.[25]

Different EDRs capture different data. EDRs vary by automobile model, and newer EDRs generally capture more data than early EDRs. For instance, a 1995 Cadillac Deville EDR monitors four things: how long it took for the airbag to deploy, whether the driver was wearing a seat-belt, deceleration for the 300 milliseconds after the airbag deployed, and if the airbag was turned off. A 2001 Ford Crown Victoria EDR monitors

---

[19] Committee, N. S. Minutes of the Senate committee on transportation and homeland security, May 2005. http://64.233.161.104/search?q=cache:-HAq-zXb35YJ:www.leg.state.nv.us/73rd/Minutes/Senate/TRN/Final/4454.pdf+erd+%22black+box%22&hl=en&client=firefox-a Accessed 16 October 2005.

[20] Spooner, J. G. Rocky road for car 'black boxes', March 2005. http://news.com.com/Rocky+road+for+car+black+boxes/2009-1041 3-5604449.html Accessed 8 October 2005.

[21] Committee, N. S. Minutes of the Senate committee on transportation and homeland security, May 2005. http://64.233.161.104/search?q=cache:-HAq-zXb35YJ:www.leg.state.nv.us/73rd/Minutes/Senate/TRN/Final/4454.pdf+erd+%22black+box%22&hl=en&client=firefox-a Accessed 16 October 2005.

[22] Evidence from black boxes in cars turns up in courts. Fox News (2003). http://www.foxnews.com/story/0,2933,90673,00.html Accessed 15 October 2005.

[23] Volpe center highlights - March/April 2004, March/April 2004. http://www.volpe.dot.gov/infosrc/highlts/04/marapr/d papers.html Accessed 13 November 2005.

[24] Committee, N. S. Minutes of the Senate committee on transportation and homeland security, May 2005. http://64.233.161.104/search?q=cache:-HAq-zXb35YJ:www.leg.state.nv.us/73rd/Minutes/Senate/TRN/Final/4454.pdf+erd+%22black+box%22&hl=en&client=firefox-a Accessed 16 October 2005.

[25] Edgar, J. Logging your every driving moment, November 2003. http://www.siliconchip.com.au/cms/A 30802/article.html Accessed 13 November 2005.

twelve different things.[26] EDRs usually store less than 10 seconds of data, frequently far less.[27]

ii) Original use

United States car makers began to install primitive EDRs in the late 1970s, with more sophisticated versions in the last 1990s. Car makers used EDRs to collect data after crashes, and to improve car safety. They answered questions like: Did the airbag deploy as designed? Did someone step on the gas instead of the brake?[28] Car manufacturers were able to access data when people brought cars to the dealership for repairs.[29]

iii) New uses

Today EDRs are used in several ways:

- Understanding accidents. Data from EDRs can be used to make cars safer. For example, if people hit the gas when they meant to hit the brakes, it suggests an opportunity to redesign the car's layout.[30]
- Court cases, particularly to establish excessive speed. The star witness in many cases has been data from EDRs. In most cases it's been used to find a driver guilty, but in at least one case has been used to establish innocence.[31, 32, 33]
- Monitoring teens. A commercial product taps into EDRs to signal drivers that they are cornering too hard, driving too fast, or braking too aggressively. It emits a clicking tone that gets progressively louder if the driver's behavior doesn't change. It also logs data from EDRs, which

[26] Services, H. T. Motor vehicle event data recorders. http://www.harristechnical.com/downloads/cdrlist.pdf Accessed 16 October 2005.
[27] Edgar, J. Logging your every driving moment, November 2003. http://www.siliconchip.com.au/cms/A 30802/article.html Accessed 13 November 2005.
[28] Spooner, J. G. Rocky road for car 'black boxes', March 2005. http://news.com.com/Rocky+road+for+car+black+boxes/2009-1041 3-5604449.html Accessed 8 October 2005.
[29] Gritzinger, B. Under the hood, with big brother: Forget Orwell's 1984–20 years later it's our cars that are giving us up. *AutoWeek* (November 2004). http://www.autoweek.com/apps/pbcs.dll/article?AID=/20041108/FREE/411080714 Accessed 11 March 2006.
[30] NTSB wants black boxes in passenger vehicles. Fox News (2004). http://www.foxnews.com/story/0,2933,127945,00.html Accessed 15 October 2005.
[31] Hechier, D. Pandora's high-tech boxes hit the courts. *The National Law Journal* (2003). http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1066080441829 Accessed 15 October 2005.
[32] Evidence from black boxes in cars turns up in courts. Fox News (2003). http://www.foxnews.com/story/0,2933,90673,00.html Accessed 15 October 2005.
[33] EDR case law. Harris Technical Services . http://www.harristechnical.com/cdr5.htm Accessed 16 October 2005.

allows parents to find out if their teens have driven the family sedan in excess of the speed limit.[34]

- Insurance companies. Since most drivers have insurance, court cases often involve two companies fighting it out to determine liability.[35] In addition, Progressive Insurance had a pilot program that offered discounted rates to "good drivers" who turned over EDR data that they stored on a second chip that customers mailed back to Progressive. Discounts were offered for people who drove lower distances, drove at particular times, and drove under 75 miles per hour.[36]

Data on EDRs is particularly relevant in legal cases with fatal crashes. Excessive speed can be used to support a contention of negligence: a jury could find a speeding driver was not acting within the reasonable person standard. For speeds in excess of 20 miles per hour over the speed limit, some states apply a strict liability standard, which holds the driver at fault for whatever else occurs even if the driver would not otherwise be found to have intentionally or negligently committed a crime.[37]

Insurance is probably the second most important use of EDR data. As the LA Times reports, "...already there are private sector plans to collect a huge pool of accident data from the recorders with the aim of finding more cost-effective ways to service insurance claims and simplify litigation. That sounds good, too, on the face of it. But emerging technologies have a way of beginning as one thing and then oozing Blob-like into something else."[38]

iv) Legislation Around Black Box Data

The National Transportation Safety Board (NTSB) initially opted not to get involved in recommendations over EDRs in cars, saying it liked how industry was progressing without any new regulation. However, in 2004 the NTSB reversed its stance and called for mandatory EDRs, along with a standard set of data that must be collected.[39]

---

[34] Spooner, J. G. Rocky road for car 'black boxes', March 2005. http://news.com.com/Rocky+road+for+car+black+boxes/2009-1041 3-5604449.html Accessed 8 October 2005.

[35] Black box a reality big brother is here! - Progressive to use data-logging device. *The Auto Channel* (2004). http://www.theautochannel.com/news/2004/08/09/208150.html Accessed 15 October 2005.

[36] Love, D. Progressive's black box: Is big brother good for the industry. *Insurance Journal* (December 2004). http://www.insurancejournal.com/magazines/southeast/2004/12/06/features/50322.htm Accessed 10 December 2005.

[37] Steven, D. N. Negligence primer. *Publish Lawyer* (2001). http://www.publishlawyer.com/negligen.htm Accessed 8 December 2005.

[38] Shannon, S. Witness on board. *Los Angeles Times* (July 2005). http://www.latimes.com/classified/automotive/news/la-tm-blackbox29jul17,0,824755.story?coll=la-classifieds-autos-news Accessed 8 December 2005.

[39] NTSB wants black boxes in passenger vehicles. Fox News (2004). http://www.foxnews.com/story/0,2933,127945,00.html Accessed 15 October 2005.

Case law establishes that court use of EDR data is not barred by either Fourth Amendment or Fifth Amendment concerns. As a report for the National Cooperative Highway Research Program concludes, legal issues around rules of evidence are not a strong concern:

> *...although the data (and the recorder itself) may be "owned" by the automobile's owner or lessee, that data may almost certainly be used as evidence against that owner (or another driver) in either a civil or criminal case. Certainly nothing within the Federal Rules of Evidence (FRE) or the Fifth Amendment's protection against compelled self-incrimination would exclude the use of data recorded by the EDRs. ...the issue here is not one so much of legal authority to use EDR data in court, but instead what the public will accept. ...the problem is less a legal concern than it is a battle to mold public perception.*[40]

More specifically, EDR data is admissible in court under the *Daubert* test, since it "possesses the requisite scientific validity to establish evidentiary reliability".[41] In a privacy-friendly move, California passed a state law in 2004 to require car manufacturers to disclose black boxes by mentioning them in car manuals. Further, the law states that car owners also own the data on their EDRs.[42] California's law has become a model for legislation in other states.[43]

Arkansas, Nevada, North Dakota and Texas enacted similar legislation in 2005. Eleven other states also considered legislation in 2005, but failed to pass laws during the 2005 session.[44] As of February, 2006, 13 states are currently considering new legislation.[45]

There are minor variations between the state laws. All five carve out an exception that EDR data may be used without consent to perform medical research on crash reactions. North Dakota is unique in specifically barring insurance companies from using EDR data to set insurance rates. Arkansas' law is fairly typical in granting ownership of

---

[40] Gabler, H. C., Gabauer, D. J., Newell, H. L., and O'Neill, M. E. Use of event data recorder (EDR) technology for highway crash data analysis, December 2004. http://trb.org/publications/nchrp/nchrp w75.pdf.

[41] IBID.

[42] Hechier, D. Pandora's high-tech boxes hit the courts. The National Law Journal (2003). http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1066080441829 Accessed 15 October 2005.

[43] Committee, N. S. Minutes of the Senate committee on transportation and homeland security, May 2005. http://64.233.161.104/search?q=cache:-HAq-zXb35YJ:www.leg.state.nv.us/73rd/Minutes/Senate/TRN/Final/4454.pdf+erd+%22black+box%22&hl=en&client=firefox-a Accessed 16 October 2005.

[44] Greenberg, P. 2005 legislation related to event data recorders ("black boxes") in vehicles, December 2005. http://www.ncsl.org/programs/lis/privacy/blackbox05.htm Accessed 4 March 2006.

[45] Greenberg, P. 2006 legislation related to event data recorders ("black boxes") in vehicles, February 2006. http://www.ncsl.org/programs/lis/privacy/blackbox06.htm Accessed 4 March 2006.

the data to car owners, yet specifies the data can be used without the owner's consent in several ways — such as by a court, a police officer with probable cause, the Highway and Transportation Department to calculate fuel taxes or mileage, and EDR data may be entered into any civil or criminal court case if "relevant and reliable."[46]

Data ownership does not appear to curtail facing your car as the star witness in a court case against you. It remains to be seen in practice how these new state laws will change the legal landscape. We await case law.

Insurance companies are frustrated by the new laws, since they need either the owner's permission or a court case to gain access to data. In states with EDR laws, insurance companies cannot use data accessed during car repairs to deny a claim, or raise a customer's rates. At least one car repair center has provided EDR data directly to insurance companies.[47] New state laws also make it more difficult for insurance companies to charge rates based on mileage.[48] Researchers are looking at the economic implications of a system called pay-as-you-drive-and-you-save (PAYDAYS) to determine how to tie insurance rates to mileage.[49]

v) Privacy concerns

If consumers tamper with the EDRs in their cars, they will also interfere with the signals that tell air bags to deploy or car seat belts to adjust during a crash.[50] Because seat belts are mandatory, it may be illegal to attempt to disable EDRs. In Montana, New Hampshire and New Jersey, new bills would explicitly give owners permission to turn off EDR data collection, even though it means disabling the airbags in the process.[51]

Privacy advocates are frustrated that in most states, car owners don't know EDRs are in cars, consumers don't have the choice to turn off EDRs, and there are no guidelines limiting who can access EDR data or what it can be used for.[52] The major risks are

---

[46] Reddick, D. Regulating event data recorders: How should insurers react to new state laws?, July 2005. http://www.namic.org/insbriefs/050722BlackBox.pdf Accessed 4 March 2006.

[47] Baker, C. Black box FAQs, November 2005. http://www.collision-insight.com/news/archives/200511-feature.htm Accessed 3 March 2006.

[48] Reddick, D. Regulating event data recorders: How should insurers react to new state laws?, July 2005. http://www.namic.org/insbriefs/050722BlackBox.pdf Accessed 4 March 2006.

[49] Greenberg, A. Applying mental accounting concepts in designing pay-per-mile auto insurance products, December 2005. http://trb.org/am/ip/paper detail.asp?paperid=12324 Accessed 6 March 2006.

[50] Shannon, S. Witness on board. *Los Angeles Times* (July 2005). http://www.latimes.com/classified/automotive/news/la-tm-blackbox29jul17,0,824755.story?coll=la-classifieds-autos-news Accessed 8 December 2005.

[51] Baker, C. Black box FAQs, November 2005. http://www.collision-insight.com/news/archives/200511-feature.htm Accessed 3 March 2006.

[52] Vlahos, K. B. Privacy experts shun black boxes. Fox News (2004). http://www.foxnews.com/story/0,2933,132056,00.html Accessed 15 October 2005.

criminal and civil liability, since EDRs are seen as evidence rather than self-incrimination, and the risk of adverse insurance policy changes.

B. Traffic Cameras

Traffic cameras evolved from a system designed by race car driver Maurice Gatsonides. Frustrated by inaccuracies from stop watches, Gatsonides developed a series of automated ways to time cars.[53]

Red light cameras take photographs of cars that run red traffic lights. They catch both cars that continue through the intersection after a yellow signal, and cars that edge into the intersection before the light turns green. The cost and size of video cameras has plunged, which is a key factor in adoption. Red light cameras were introduced in the United States over 40 years ago, but it's been in the last 10 years that they have become pervasive.[54]

Traffic cameras are also used in a variety of contexts other than monitoring red lights. Traffic cameras are also used to measure speed and issue speeding tickets. Many cities use cameras to monitor traffic flow. This way they can find more efficient routes for emergency vehicles, and can adjust traffic signals to better handle congestion, for example, after a football game.[55]

i) How They Work

Systems vary widely. A typical red light camera system works with roadway sensors that communicate with traffic lights. When a car enters an intersection during a red light, the sensor sends a message to a camera. The camera captures an image of the car in the intersection. Cameras are usually mounted high above the road, and generally operate in pairs to confirm that the car crossed into the intersection. Cameras operate in the infrared frequency and bathe the intersection in infrared light so they can get images at night. Cameras send the images to a central computer for processing.[56]

Different systems capture different levels of detail. At minimum, systems capture the vehicle's license plate. In the early days of red light cameras, a clerk would look at the picture of the license plate, look up the registration information for the vehicle, and send a ticket to the owner. Today, the process is typically contracted out to a firm that uses image-processing software to automatically process the image and determine the license plate. The license plate number can then either be sent to the municipality to look up in a computer database, or municipalities can grant access directly to registration

---

[53] Finlay, R. Gatso and the cameras. ITV Motoring (May 2001). http://www.itv-motoring.com/columns/ross finlay/1510.asp Accessed 25 November 2005.

[54] Harris, T. How red-light cameras work. *howstuffworks* (2002). http://electronics.howstuffworks.com/red-light-camera6.htm Accessed 26 November 2005.

[55] Learmonth, M. Say cheese. *Metroactive* (1997). http://www.metroactive.com/papers/metro/02.06.97/traffic-camera-9706.html Accessed 25 November 2005.

[56] Harris, T. How red-light cameras work. *howstuffworks* (2002). http://electronics.howstuffworks.com/red-light-camera6.htm Accessed 26 November 2005.

databases.[57] Some systems still use film rather than digital cameras. In that case, a worker must go to each camera to collect the negatives and install new film.[58]

Most cameras show the make, model, and color of the car. Cameras record the time and date the image was taken. Because cameras are usually used in pairs, it is generally possible to calculate a vehicle's speed.[59]

Even though most cameras are infrared, it is usually possible to determine the race of the driver and any passengers. Less common, some systems also use image recognition software to identify drivers and passengers. Automated facial recognition is used in security systems to grant access to corporate parking lots.[60]

ii) Original uses

Traffic cameras were presented as a way to enhance safety. Some of the reasons given for installing cameras include:

- Red light cameras act as a deterrent for running red lights, thus preventing accidents.
- Speed trap cameras act as a deterrent against excessive speed, again preventing accidents.
- Video cameras in police cars document officers' conduct, which decreases police brutality.[61]
- Traffic cameras monitor the flow of traffic on highways and main roads to help emergency vehicles find the fastest route to an accident. They also help reduce congestion, because traffic signals can be adjusted to respond to conditions.[62]

iii) New uses

Red light cameras capture images of crashes. These images can be used to determine which driver was at fault.[63]

---

[57] Hofman, Y. License plate recognition - a tutorial, May 2004. http://www.licenseplaterecognition.com/ Accessed 26 November 2005.

[58] Labash, M. The yellow menace. *The Weekly Standard* (2002). http://www.weeklystandard.com/Content/Public/Articles/000/000/001/078ftoqz.asp Accessed 25 November 2005.

[59] Learmonth, M. Say cheese. *Metroactive* (1997). http://www.metroactive.com/papers/metro/02.06.97/traffic-camera-9706.html Accessed 25 November 2005.

[60] Hofman, Y. License plate recognition - a tutorial, May 2004. http://www.licenseplaterecognition.com/ Accessed 26 November 2005.

[61] Oakland cops may go to video; city wants cameras in police cars, March 2004. http://www.policeone.com/police-products/vehicle-equipment/in-car-video/articles/78478/ Accessed 26 November 2005.

[62] Learmonth, M. Say cheese. *Metroactive* (1997). http://www.metroactive.com/papers/metro/02.06.97/traffic-camera-9706.html Accessed 25 November 2005.

[63] The red light running crisis: Is it intentional?, May 2001. http://www.thenewspaper.com/rlc/reports/rlcreport6.asp Accessed 6 March 2006.

Red light cameras are a substantial revenue source for local governments. Washington, DC's red light camera system generated $18 million dollars in tickets from 1999 to 2002.[64] DC's photo radar system (automated fines for speeding) made $9 million in its first seven months of operation.[65] While raising funds from people who break the law isn't necessarily a bad thing, there are concerns that local governments are installing red light cameras strictly as a source of profit, rather than out of concern for citizens' well-being.

Red light cameras were supposed to reduce accidents because fewer people would run lights. Instead, there is evidence to show red light cameras cause accidents: drivers slam on their brakes to avoid tickets, which leads to an increase in rear-end collisions for the intersections that have red light cameras. In some cases, while rear-end collisions increase, more dangerous T-bone accidents decrease. However, the details appear to vary widely. For example:

- Fort Collins, Colorado had an 83% increase in accidents.[66]
- Portland, Oregon had a 140% increase in rear-end collisions.[67]
- The Washington, DC area had more than twice as many accidents and fatal crashes increased 81%.[68]

There is a simple way to decrease the number of people who run red lights: lengthen the time the light is yellow. The Institute of Transportation Engineers (ITE) decreased their recommended yellow light length by as much as a third since the 1970s recommendations. Yellow lights were once 4 to 6 seconds long, and are now typically 3 to 4 seconds. 80% of motorists who run red lights do so in the first second the light turns red — time when it would still be yellow, under the older guidelines. The ITE suggests that instead of longer yellows that allow drivers to react, thanks to traffic cameras, "enforcement can be used instead".[69]

While local governments vigorously deny they're motivated by money rather than safety, it does seem money factors into decisions. For example, Fort Collins increased the length of yellow lights and saw such a large decline in revenues that they decided to hold

---

[64] Mahoney, E., and Helperin, J. Caught! Big brother may be watching you with traffic cameras, October 2004. http://www.edmunds.com/ownership/driving/articles/42961/article.html Accessed 26 November 2005.

[65] Labash, M. The yellow menace. *The Weekly Standard* (2002). http://www.weeklystandard.com/Content/Public/Articles/000/000/001/078ftoqz.asp Accessed 25 November 2005.

[66] Benson, M. Accidents increase on camera's watch, October 2005. http://www.thenewspaper.com/news/07/740.asp Accessed 25 November 2005.

[67] Song, A. Do red light cameras pose safety problems? *KATU News* (November 2005). http://www.katu.com/team2/story.asp?ID=81073 Accessed 25 November 2005.

[68] Wilber, D. Q., and Willis, D. D.C. red-light cameras fail to reduce accidents. *The Washington Post* (October 2005). http://www.washingtonpost.com/wp-dyn/content/article/2005/10/03/AR2005100301844.html Accessed 25 November 2005.

[69] Labash, M. The yellow menace. *The Weekly Standard* (2002). http://www.weeklystandard.com/Content/Public/Articles/000/000/001/078ftoqz.asp Accessed 25 November 2005.

off installing new red light cameras, out of fear they might lose money.[70] In Washington, DC camera placement did not correlate to the intersections with the greatest number of accidents. Instead, contractors helped the city identify intersections likely to generate the greatest number of infractions — and profits. Similar placement trends have been documented in Charlotte, North Carolina and San Diego, California. Intersections at the bottom of hills with yellow lights of three seconds or less are particularly popular.[71]

iv) Privacy concerns

Perhaps the most alarming use of traffic cameras is illustrated in China. Cameras used to measure traffic congestion around Tiananmen Square provided images the Chinese government broadcast on TV, and helped them round up student leaders who had escaped the 1989 massacre. Today China is installing more cameras in the Tibet Autonomous Region. The stated reason is that cameras are used to track traffic congestion, even though several areas they're installing cameras in have only pedestrian traffic.[72]

In the United States, there is no law that mandates municipalities need a data retention policy. It's entirely possible that images could be archived for years, then sifted through with facial recognition software to retroactively determine the movements of a person of interest.

Because cameras send photos of the front seat occupants along with a ticket, there have been several reports of red light cameras leading to marital strife. The Cato institute commented on the story of a woman "who got in hot water when an intersection camera caught her joyriding in her husband's pet sports car — a car he'd forbidden her to drive."[73] Extramarital affairs may also be discovered by traffic photos enclosed with tickets.

Privacy concerns have been cited in decisions not to install cameras, or to remove them. Usually it's "privacy and" — for example, privacy and lack of revenues with longer yellow lights, or privacy and concern that police officers would lose jobs.[74]

---

[70] Benson, M. Accidents increase on camera's watch, October 2005. http://www.thenewspaper.com/news/07/740.asp Accessed 25 November 2005.

[71] Labash, M. The yellow menace. *The Weekly Standard* (2002). http://www.weeklystandard.com/Content/Public/Articles/000/000/001/078ftoqz.asp Accessed 25 November 2005.

[72] Walton, G. China's golden shield: Corporate complicity in the development of surveillance technology. Human Rights in China (June 2002). http://iso.hrichina.org/public/contents/article?revision id=2440&item id=2439 Accessed 25 November 2005.

[73] Balko, R. Not so candid camera. *CATO Institute* (February 2002). http://www.cato.org/research/articles/balko-020206.html Accessed 25 November 2005.

[74] Red light camera timeline 2002, 2001. http://www.hwysafety.com/nma_rlc_timeline4.htm Accessed 22 October 2005.

C. GPS transponders

Global Positioning System (GPS) transponders use a system of 24 satellites to calculate precise world-wide locations in three dimensions (latitude, longitude, and height).[75]

GPS itself just calculates position. However, GPS is frequently combined with transmitters that send the data to a receiver, or with media (like a hard drive, or a USB flash drive) to capture data for later retrieval.

i) How they work

GPS transponders can determine their precise location by bouncing signals off of satellites. The satellites have atomic clocks, and calculate time very accurately. GPS was conceived shortly after Sputnik's launch. Scientists realized that since they could track Sputnik's signal and figure out where it was in space, the converse must be true: they can use signals to satellites in space to determine location on earth. GPS transponders use multiple signals from satellites to triangulate position.[76]

ii) Original use

GPS is a military technology. It was used, and still is used, for troop deployments, supply drops, and bomb targeting.[77]

iii) New uses

The United States government allowed anyone to use the signal from GPS satellites, free of charge. A wide range of applications developed. Early uses were for ships' navigation. Some computer networks use the time from GPS satellites to ensure they keep time accurately and uniformly. Surveyors use GPS to determine the exact location of property lines.[78]

Specifically for cars, GPS systems are coupled with map services to show drivers where they are. These systems are advertised as enhancing safety, because lost drivers don't have to "struggle with a large map" or "ask a stranger for directions."[79] However, a study by Privilege Insurance found that GPS-based map systems are more distracting

---

[75] A guide to the global positioning system (GPS): A brief history of navigation and GPS, 2004. http://support.radioshack.com/support_tutorials/gps/gps hist.htm Accessed 2 March 2006.

[76] IBID.

[77] IBID.

[78] Page, S., Frost, G., Lachow, I., Frelinger, D., Fossum, D., Wassem, D. K., and Pinto, M. NATIONAL INTERESTS AND STAKEHOLDERS IN GPS POLICY. Rand, 1995, ch. 2, pp. 11– 44. http://www.rand.org/publications/MR/MR614/MR614.sec2.pdf Accessed 10 December 2005.

[79] Intellinav - drive with confidence, 2002. http://www.intellinav.com/product.html Accessed 1 March 2006.

than paper maps. Further, people who own GPS-based map systems are more likely to just start driving without looking for directions first.[80]

General Motors is testing a new system that uses both GPS and a communications system to allow all similarly equipped cars to communicate. The goal is to avoid car crashes. This system is seen as an improvement over existing radar systems, since it is not affected by fog, rain, and snow.[81]

iv) Privacy concerns

Law enforcement uses GPS to automatically track suspect's cars through one of two ways. Police can affix a GPS device to a car, usually hidden underneath and held to the car frame with a magnet, and then return later to retrieve the device and the data. Or, police can use a GPS transponder to broadcast location data in real time. The first GPS case led police to a 9-year-old's body in 2003.[82] National attention focused on this issue as part of the media coverage of the Peterson murder trial. Courts have upheld the legality of using GPS to track suspects.[83]

Courts have held that because GPS functions as an automated replacement for "tailing" a car, it comes under no more judicial oversight. Initially, probable cause was not required.[84] However, the Washington State Supreme Court has since ruled that a warrant is necessary, which in turn necessitates a determination of probable cause.[85]

As of February, 2006, the Los Angeles police department is currently testing a system that allows them to fire GPS darts at moving cars. "Each unit can fire two GPS tracking devices containing a battery and a radio transmitter embedded in an epoxy compound. The tag affixes to the suspect's vehicle and transmits its location via satellite to police headquarters. The system is approved by the National Security Agency".[86]

---

[80] Report: In-car navigation systems can be dangerous, February 2006. http://news.com.com/Report+In-car+navigation+systems+can+be+dangerous/2100-1041_3-6041393.html Accessed 1 March 2006.

[81] MATEJA, J. GM system lets cars talk to each other, February 2006. http://www.navigadget.com/index.php/2006/02/04/ Accessed 1 March 2006.

[82] Cops challenged on GPS use, May 2003. http://www.wired.com/news/privacy/0,1848,58948,00.html?tw=wn_story_related Accessed 10 December 2005.

[83] Dornin, R. Judge allows GPS evidence in Peterson case. CNN (February 2004). http://www.cnn.com/2004/LAW/02/17/peterson.trial/ Accessed 9 December 2005.

[84] Cops challenged on GPS use, May 2003. http://www.wired.com/news/privacy/0,1848,58948,00.html?tw=wn_story_related Accessed 10 December 2005.

[85] In landmark ruling, Washington Supreme Court says police need warrant for surveillance with global tracking devices, September 2003. http://www.aclu.org//privacy/spying/14888prs20030911.html Accessed 10 December 2005.

[86] Brandt, N. Los Angeles turns to GPS devices to end deadly police chases, February 2006. http://www.bloomberg.com/apps/news?pid=10000103&sid=aYPV2SPTS9.o&refer=us Accessed 1 March 2006.

GPS could be widely deployed on vehicles for an entire community, such as all members of a political or religious group. The records can be saved and matched against other people's data retroactively, for example as part of social network analysis.

GPS could also be used to alert a community about an individual's location. For example, GPS could be used to inform neighbors about a former sex offender's current location. Individuals can use GPS to spy upon each other. Divorce lawyers and private investigators advertise their use of GPS data to potential clients.[87]

D. OnStar

OnStar is a commercial service that alerts the police when cars are in accidents, and offers consumer convenience benefits for a monthly fee. Initially an optional service, since 2004 it has been pre-installed on most General Motors cars. It will be mandatory in all General Motors cars from 2007 forward.[88] Mercedes-Benzes, BMWs and Jaguars use a similar technology to perform the same functions.[89]

i) How it works

OnStar's strength is that it uses so many different technologies in combination. OnStar combines GPS transponders for vehicle tracking, a hands-free voice activated cell phone to talk to OnStar employees, and real-time monitoring of data from the car's EDR. OnStar employees can open doors, or turn off car engines without being physically present.[90]

ii) Original use

OnStar was promoted as a safety feature. OnStar can track when airbags deploy, call the cell phone in the car to check for false alarms, and notify the police if appropriate. OnStar was also advertised as a roadside assistance program. OnStar advertising frequently depicts the service saving people in peril.[91]

---

[87] Stevens, J. B. GPS trackers foil cheating spouses, August 2005. http://www.scfamilylaw.com/divorce-46-gps-trackers-foil-cheating-spouses.html Accessed 10 December 2005.

[88] OnStar — home. http://www.onstar.com/us_english/jsp/ovd/index.jsp Accessed 9 December 2005.

[89] Shannon, S. Witness on board. *Los Angeles Times* (July 2005). http://www.latimes.com/classified/automotive/news/la-tm-blackbox29jul17,0,824755.story?coll=la-classifieds-autos-news Accessed 8 December 2005.

[90] OnStar — home. http://www.onstar.com/us_english/jsp/ovd/index.jsp Accessed 9 December 2005.

[91] IBID

iii) New uses

Because OnStar is always on, OnStar data is valuable to law enforcement. OnStar does require a warrant before they grant access to their databases, and they explicitly state they maintain that policy out of fear they'll lose customers over privacy concerns.[92]

OnStar realized that with the data they already collect, they can tell how many passengers are in a car. They can also tell the passengers' weight from data they collect to suppress airbags in certain crashes. With this data, and data from which area of a car was hit during an accident, OnStar can calculate how likely it is that someone is badly injured. This lets them prioritize calls to emergency services. One of their engineers was quoted in the press saying, "This is a great secondary use".[93]

iv) Privacy concerns

Privacy experts from the EFF and EPIC voiced concerns that the tracking data OnStar collects could be used in unexpected ways. One example they offer: if OnStar records show you stopped at a bar for three hours, might that be entered into evidence in a court case, even if you never had a drink while you were there?[94]

OnStar has been used to catch drunk drivers. One driver pushed the OnStar button repeatedly, failed to respond to inquires, and was subsequently arrested after the OnStar employee called the police to report the vehicle's location. A state police sergeant summed up, "Sometimes, you get help that you didn't expect."[95]

Even law makers are surprised when they realize the scope of data collected by OnStar. A state Senator in North Dakota was quoted as saying "When I bought my car, I didn't realize that I was also buying a highway patrolman to sit in the back seat."[96]

The FBI realized that systems like OnStar can be turned on at any time, even if a consumer does not pay for the service. They used this feature to surreptitiously monitor all conversations in a car. The 9th Circuit Court of Appeals ruled against the FBI's use, not because it was privacy invasive, but because the FBI tap interfered with the basic functionality of the system.[97] If there had been an accident, the system would not have worked. Federal law enforcement can listen in via OnStar and related technologies without notice, even for people who are non-subscribers, so long as they structure the

---

[92] Block, R. In terrorism fight, government finds a surprising ally: FedEx. *Pittsburgh Post Gazette* (May 2005). http://www.post-gazette.com/pg/05146/510879.stm Accessed 15 October 2005.

[93] Konrad, R. Car-tracking system: Promises, potholes. ZDNet News (August 2002). http://news.zdnet.com/2100-9595 22-947519.html Accessed 8 December 2005.

[94] IBID.

[95] Field, S. OnStar leads police to drunken drivers. *The Morning Sun* (December 2005). http://www.themorningsun.com/stories/120205/loc_onstar001.shtml Accessed 9 December 2005.

[96] Shannon, S. Witness on board. *Los Angeles Times* (July 2005). http://www.latimes.com/classified/automotive/news/la-tm-blackbox29jul17,0,824755.story?coll=la-classifieds-autos-news Accessed 8 December 2005.

[97] It is believed the system in question was the Tele Aid system used in Mercedes vehicles, an OnStar competitor, but the court case does not name the system.

system so OnStar remains operative. It stands to reason they could listen in on non-subscribers at any time, since they won't disrupt the functionality of a system that is not in service.[98]

The website onstarprivacy.com details several privacy concerns including:

- Progressive Insurance has a pilot program to give "good driver" discounts based on OnStar data. The concern is car insurance companies will require data access as a condition of insurance.
- Data may be for sale or shared between the General Motors family of companies. Will dealerships decide you abused your car and it is now out of warranty?
- GMAC Insurance offers discounts to OnStar employees who allow GMAC Insurance access to OnStar data. They monitor the number of miles driven, and adjust insurance rates every six months based on mileage.[99] Again, the concern is eventually all insurance companies will demand data as a condition of insurance.
- OnStar launched a "Virtual Advisor" service. It was designed to announce where to find inexpensive gas when OnStar senses your fuel gauge is low. It can also push ads that match location based information with user profiles, for example, to tell an avid golfer that she's three blocks away from a sale on golf clubs.[100] Not everyone is comfortable with the idea of merchants purchasing location data for advertising. For instance, imagine driving with a child in the back seat as an ice cream shop offers a discount – or what magazines might arrive in the mail based on which shop you parked in front of.

E. E-ZPass

E-ZPass and several similar systems are used to pay highway tolls automatically. Drivers put a small transmitter in their car, and funds are automatically deducted each time they drive through a toll both.

i) How E-ZPass works

The underlying technology is Radio Frequency Identification (RFID), which sends a radio signal to a receiver.[101]

---

[98] Poulsen, K. Court limits in-car FBI spying. The Register (November 2003). http://www.theregister.co.uk/2003/11/20/court_limits_incar_fbi_spying/ Accessed 6 March 2006.

[99] Gabler, H. C., Gabauer, D. J., Newell, H. L., and O'Neill, M. E. Use of event data recorder (EDR) technology for highway crash data analysis, December 2004. http://trb.org/publications/nchrp/nchrp_w75.pdf.

[100] Konrad, R. General Motors to "push" ads to drivers. *CNET* (2001). http://news.com.com/2100-1023-250696.html?legacy=cnet Accessed 9 December 2005.

[101] Shermach, K. Legoland RFID tracks lost kids, collects data. CRM News (October 2004). http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html Accessed 9 December 2005.

E-ZPass uses a semi-passive RFID tag. All E-ZPass tags have a non- replaceable lithium battery, which limits the life of the tag to two to five years.[102] E-ZPass communicates by taking an incoming radio signal from an RFID reader, and bouncing back a modified signal that contains the ID number for the device. As a result, E-ZPass can only "speak when spoken to" — it can't broadcast information unless a reader requests it. This differs from GPS devices, which often contain transmitters that send real-time updates of location.

ii) Stated purpose

E-ZPass bills itself as a convenient, easy, and fast way to pay tolls. Some highways have special lanes reserved just for motorists with E-ZPass. Because cars pass through toll booths more quickly, E-ZPass may also reduce pollution and save fuel.[103]

iii) New uses

E-ZPass is primarily used for paying tolls on highways, though the data does find its way into other uses. The customer agreement foresees a time when the pass itself may be used in other ways: "Nor are we liable for any third party act taken by reason of your use or display of the E-ZPasstag."[104]

E-ZPass is used to pay for airport parking in Pittsburgh, New York, New Jersey, Texas, Chicago, and Delaware. Drivers take parking tickets when they enter, and at exit have a choice of paying with cash, credit, or debit from their E-ZPass account.[105]

While a few McDonald's on Long Island allow drive-thru customers to pay with E-ZPass, it hasn't proven economically successful to the point of justifying installing E-ZPass hardware in more McDonald's.[106]

Transcom uses E-ZPass to assess traffic conditions in New York, New Jersey, and Connecticut. Transcom installed roadside readers along the I-95 corridor to read E-ZPass tags. They can measure how many cars go past. If the number of cars passing a reader suddenly drops, there must be congestion before the reader. Transcom scrambles the E-ZPass ID code so they are able to get data without tracking individuals.[107]

---

[102] E-ZPass information - frequently asked questions. http://www.ezpassmaineturnpike.com/info/faqs.html#q21 Accessed 11 March 2006.

[103] Excellence in highway design - E-Z Pass electronic toll collection program, April 2003. http://www.fhwa.dot.gov/eihd/ezpass.htm Accessed 10 December 2005.

[104] E-ZPass customer agreement terms and conditions, January 2003. http://www.ezpass.com/static/terms/i_terms.pdf Accessed 10 December 2005.

[105] Samuel, P. Non-toll transponder use E-ZPass Plus flies at New York area airports. *TOLLROADSnews* (May 2004). http://www.tollroadsnews.com/cgi-bin/a.cgi/Nxop4qUAEdiRW6r2jfFwDw Accessed 11 March 2006.

[106] IBID.

[107] Konheim, C. S. Intelligent transportation systems in the New York region: An overview. *ITS-NY Winter 1998/1999* (1999). http://transport-link.com/region/ITSOverview.htm Accessed 11 March 2006.

iv) Privacy concerns

Because E-ZPass transponders only give information when they're scanned, they're less privacy invasive than GPS, which captures location information all the time. Still, E-ZPass data has shown up in surprising contexts. For example, E-ZPass data has been used in divorce cases to support allegations of infidelity.[108]

Additional E-ZPass scanners could be placed along local roads to track traffic off highways as well as on them. Further, because RFID technology broadcasts a signal to anyone with a scanner, it would be fairly easy for a stalker to track every time his target left home or work.

The FBI cited E-ZPass data as one example of data they can obtain without judicial oversight, and used it as an argument in favor of keeping all USA PATRIOT Act provisions.[109] Law enforcement is also interested in E-ZPass data to track suspects and missing persons.

Drivers are concerned that E-ZPass will eventually be used to issue speeding tickets. It is easy to calculate an average speed over the distance between two tollbooths. While stories abound of "a friend of a friend" getting a ticket in this way, it does not appear that E-ZPass is currently being used to issue speeding tickets.

F. Highway Use Tax Proposals

Several states, most notably Oregon[110, 111, 112] and California, are investigating "use tax" to replace gasoline taxes. The idea is that as people buy more hybrids, gasoline taxes will decrease, which leaves states short on funds to maintain roads.[113] Instead,

---

[108] Shermach, K. Legoland RFID tracks lost kids, collects data. CRM News (October 2004). http://www.crmbuyer.com/story/Legoland-RFID-Tracks-Lost-Kids-Collects-Data-37694.html Accessed 9 December 2005.

[109] Caproni, V. Bill to reauthorize certain provisions of the USA PATRIOT Act and for other purposes, May 2005. Transcript of Ms. Caproni's testimony available from http://intelligence.senate.gov/0505hrg/050524/witness.htm Accessed 23 October, 2005. Testimony regarding toll systems was during question and answer. Information from author's notes.

[110] Whitty, J. M. Report to the 72nd Oregon legislative assembly on the possible alternatives to the current system of taxing highway use through motor vehicle fuel taxes. Final report, Road User Fee Task Force, Salem, OR, 2003. http://www.oregon.gov/ODOT/HWY/OIPP/docs/FinalReport2003march.pdf Accessed 8 October 2005.

[111] Whitty, J. M., and Imholt, B. Oregon's mileage fee concept and road user fee pilot program. Final report, Oregon Department of Transportation, Salem, OR, 2005. http://www.oregon.gov/ODOT/HWY/OIPP/docs/2005LegislativeReport.pdf Accessed 8 October 2005.

[112] Road User Fee Task Force. Office of innovative partnerships and alternative funding. http://www.oregon.gov/ODOT/HWY/OIPP/ruftf.shtml Accessed 8 October 2005.

[113] Salladay, R. DMV chief backs tax by mile. LA Times (November 2004). http://forums.fingerlakes1.com/showflat.php?Cat=&Number=55289&Main=54730 Accessed 8 October 2005.

proponents suggest a new tax based on miles driven and time of travel (rush hour might cost more than 3 am, for example.)

i) How it could work

The most complete proposal involves a government-mandated GPS transponder that tracks everywhere a car travels, then sends a bill to the owner. A less invasive proposal is to add a device to the odometer. Every time a driver pulls into a gas station, the device broadcasts the mileage, and the gas tax is collected at the pump.[114]

ii) Privacy concerns

Even without any systems in use today, privacy experts fear secondary uses for the data and privacy invasions. As we have seen with other technologies, it seems likely that law enforcement, spurned spouses, insurance companies, and possibly marketing companies will all work to find ways to use the data for their own purposes.

IV. DISCUSSION

As we have shown, along with benefits from increasing technological sophistication in the automotive sphere, there are also privacy threats. When combined together, threats to privacy are even worse than just the individual concerns. For example, an insurance company with access to data from a system like OnStar will know when there has been an accident, and will be in a better position to request data from EDRs from mechanics. The combined data may lead to dropping a customer's insurance policy. Government surveillance can combine information from red light cameras' license plate recognition on local roads with E-ZPass highway data to track a person of interest very closely.

Most people don't consider privacy when they get into a car. Yet taken in aggregate, these technologies can report where you are, where you have traveled, who you have seen, and with whom you have traveled.

A. Privacy threats associated with each technology

The table below summarizes the privacy threats associated with each technology discussed. Note that for Use Taxes this information is speculative, since the technology is still in the planning stage.

---

[114] Salladay, R. DMV chief backs tax by mile. LA Times (November 2004). http://forums.fingerlakes1.com/showflat.php?Cat=&Number=55289&Main=54730 Accessed 8 October 2005.

Risk	*EDRs*	*Cameras*	*OnStar*	*GPS*	*E-ZPass*	*Use Tax*
Technology can reduce safety		X	X	X		
Insurance company raises rates	X	X	X	X	X	X
Insurance company drops coverage	X	X	X	X		
Location data sold to marketing company			X			
Increased risk of criminal charges	X	X	X	X	X	X
Increased risk of tickets or fines		X		X	X	X
Data used in divorce proceedings		X	X	X	X	X
Parental surveillance of teens	X			X		
Govt. surveillance and data mining	X	X	X	X	X	X

i) Technology can reduce safety

While most of the technologies listed are advertised as improving safety, in some cases they actually may decrease safety. As discussed in section 3.2.3, red light cameras may increase traffic accidents, particularly rear-end collisions due to drivers slamming on the brakes. As discussed in section 3.3.3, map systems that use GPS or OnStar may contribute to accidents by distracting drivers.

ii) Insurance company raises rates

Insurance companies are very interested in using new technologies to gain competitive advantage in the way they set rates. As discussed in sections 3.1.3 and 3.1.4,

insurance companies are exploring ways to charge rates based on mileage. EDRs that save speed and braking data for later retrieval, license plate recognition coupled with traffic cameras, OnStar data, GPS data, E-ZPass data, and highway use tax data are all useful in calculating mileage. Insurance companies might be willing to purchase such data from state governments, or obtain the data from an affiliated partner company like OnStar. As discussed in section 3.1.3, insurance companies are also trying to amass a large database of EDR data to try to better predict which customers will have accidents.

iii) Insurance company drops coverage

Similarly, insurance companies may drop coverage for customers they believe to be high risk. For consumers, one advantage to insurance is to pool risk. For insurance companies, being able to exclude the most expensive customers allows greater profits or lower prices and thus greater market share. Insurance will probably not be dropped just for driving more miles than average, so E-ZPass and use tax data are not relevant. But as with setting insurance rates, data that show drivers are aggressive in cornering (ERDs, OnStar,) run red lights (traffic cameras,) or even park in bad neighborhoods on a regular basis (GPS) are all potential flags for a higher risk policy. If insurance companies could combine data from these sources, they would have the ability to create better statistical models of which customers are likely to cost the most, and drop their coverage.

iv) Location data sold to marketing company

So far, the threat of marketing companies purchasing location based data is comparatively low. While marketing companies might love to know which stores people visit even if they don't make a purchase, how long they visit any given store, and then to tie that data to point of sale information to determine what they purchased, right now marketing companies don't have easy access to data. We include OnStar as a threat since, as discussed in section 3.4.4, OnStar did offer a "virtual advisor" service that allowed real-time advertising for nearby products. EDRs don't record useful information for marketers. Marketers don't have access to affix GPS devices and transponders to hundreds of thousands of cars. At present, E-ZPass data only establishes which toll roads a customer takes. Marketers could install RFID readers in parking garages in order to track how frequently specific shoppers visit a given store, but that's a lot of expense — and much of that data can be established by looking at credit card receipts. Use tax data and traffic camera data might be interesting to marketers. That data is retained by various governments (both state and local,) and some may be willing to sell it. So far, the threat of sales to marketing companies is largely theoretical, but this is an area worth watching in the future.

v) Increased risk of criminal charges

Increased risk of criminal charges is a major risk posed by new technologies. In particular, as discussed in section 3.1.3, data can be used in court rooms to establish negligence, strict liability, or that the defendant did not adhere to the reasonable person standard. EDRs have been used to determine speed and braking prior to a crash (section 3.1.3). Red light cameras have captured accidents and photos have been submitted as evidence (section 3.2.3). OnStar reported a drunk driver to the police (section 3.4.4). GPS was used in the Peterson murder trial (section 3.3.4). The FBI cited availability of E-

ZPass data as a reason to renew PATRIOT Act sunset provisions (section 3.5.4). We assume the FBI would utilize use tax data similarly, since it provides even more information than E-ZPass. Note that these are examples of things that have already happened, rather than prospective threats. Law enforcement and the court system take full use of new technologies.

vi) Increased risk of tickets or fines

Similarly, drivers are at increased risk of traffic tickets or fines. ERDs have no way to tell what the speed limit is and it would be difficult to re-architect them for speeding tickets. Red light and speeding cameras are used to issue tickets — that is their primary purpose (section 3.2.2). The risk from other technologies is low and largely theoretical. OnStar or GPS data could establish a driver's speed and location, then combine it with speed limit data to determine speeding. However, OnStar is unlikely to offer their data to law enforcement for speeding, since it would dramatically reduce their subscription base. Similarly, GPS is usually installed by vehicle owners, who are unlikely to purchase a system that reports them for speeding. (Parents may want to catch their children, but won't want to pay higher insurance and speeding tickets by sharing that data with law enforcement.) E-ZPass and use tax proposals could very easily determine if a driver's average speed exceeded the limit. However, that doesn't appear to be happening currently.

vii) Data used in divorce proceedings

Divorces can get bitter, especially with large estates or child custody at stake. Private investigators attach concealed GPS devices to help establish infidelity (section 3.3.4). Traffic cameras may capture unexpected passengers in photographs sent home to document running a red light or speeding, again giving rise to infidelity claims (section 3.2.4). E-ZPass sends information home about times a car went through a tolls booth, which may lead to suspicions. OnStar data is not readily available during a divorce, but may be subpoenaed from the company. We expect use tax data would be sent home like E-ZPass, but with the fine detail of OnStar. While these threats to privacy do exist today, the majority of divorces do not involve suspicious spouses using covert means to spy on each other.

viii) Parental surveillance of teens

Parents watch not just each other, but their children. A commercial system warns teens not to brake too aggressively and logs the speeds recorded by the car's EDR (section 3.1.3). Traffic cameras may show teens driving at times they weren't allowed to, or in a car they weren't supposed to drive (section 3.2.4). OnStar is not a likely source of data for parents. Some parents may elect to add GPS tracking to their cars, either with or without their child's knowledge, and use that data to verify a child's location. As mentioned above for divorces, E-ZPass sends data home, and use tax would likely do the same. These technologies could also be used to determine where a child traveled.

ix) Government surveillance and data mining

Government surveillance, in particular, gets a large boost from these new vehicular technologies. Now that it's economically and legally feasible to monitor large

groups of people, law enforcement can track the movements of entire communities. Databases can be stored indefinitely, allowing retroactive analysis. Data can be cross-checked to see which people gather together — who was in the parking lot for the ACLU meeting two years ago? Social networks can be studied — list everyone who parked within a three block range of John Smith's house on June 23rd. EDRs don't store data that's useful for government surveillance. Traffic cameras, OnStar data, GPS de- vices attached by law enforcement, E-ZPass records, and use tax data are all available to the government. This is another area where combining records allows a far more detailed picture than isolated data from one technology.

B. Fair Information Practice Principles

Automotive privacy is not substantially different from other realms where privacy guidelines have been developed, and in some cases codified into law. The Organization for Economic Co-operation and Development (OECD) Guide- lines on the Protection of Privacy and Transborder Data Flows of Personal Data are a useful framework for evaluating privacy.

The following table, which mirrors the analysis in Cranor's *I Didn't Buy It For Myself*[115], gives an example of good behavior as well as how each of the eight OECD principles can be violated with automotive technologies.

OECD principles	*Good behavior*	*Potential violation*
Collection limitation	Don't collect more data than needed for the primary purpose	Retaining use tax data with not just cumulative mileage, but also destination and travel path.
Data quality	Be clear on what level of accuracy to expect from tools	A faulty EDR reading could result in an erroneous manslaughter conviction.
Purpose specification	State what data is used for	Data from red light cameras was not supposed to be used to facilitate social network analysis.
Use limitation	Don't use data for new purposes without consent	Mechanics give ERD data to insurance companies.
Security safeguards	Keep data safe and secure	If hackers understand OnStar data, they can broadcast signals to open doors and start the ignition.
Openness	Tell people when data is collected and what it's used for	Not all states require notice for EDR systems.

[115] Cranor, L. F. 'I didn't buy it for myself ': Privacy and Ecommerce personalization, 2004. http://lorrie.cranor.org/pubs/personalization-privacy.pdf Accessed 14 September 2005.

Individual participation	Let people correct faulty data	If a red light camera misidentifies a license plate number, it can be a nightmare to resolve.
Accountability	Be proactive in supporting these principles	Lack of data retention policies make these datasets targets for new uses and abuses.

We are particularly concerned by the lack of use limitations, which give rise to so many secondary uses. While security has not yet been a major issue, we anticipate it's just a matter of time before we read of a massive data breach. These dangers could be mitigated by following a policy of collection limitation.

C. Potential for Change

We believe that the potential for surprise uses of data, as well as possible abuses of data, warrant changes to policies and practices at all levels. Who can create changes?

Actor	*Ability to influence change*
Insurance companies	While they have the power to simply not acquire data, the market will reward companies that exploit information advantages.
Car manufactures	Auto makers are in a position of power since they largely determine what goes into their cars at the factory. However, we don't anticipate benefits to car manufactures for a privacy protective stance, which makes it unlikely they will be concerned.
Consumers	Individuals can educate themselves and buy privacy friendly products. Yet in many cases, consumers have no real choices. EDRs and traffic cameras are ubiquitous. The only way to opt out of those privacy risks is to forgo driving, which is not a practical alternative in many areas.
Advocacy groups	Education and public awareness often precede changes. In many cases educating legislative members about their personal privacy risks foster the enactment of better privacy protections for all citizens. We see an on-going role for advocacy.
Policy makers	New laws that curtail data use are the most likely path to increased privacy. At the Federal level, Congress can legislate the reach of the FBI and the PATRIOT Act to ensure new powers are used to fight terrorism, rather than as an expansive new set of surveillance powers used in a more indiscriminate way. At the state level, E-ZPass and use tax data can be restricted for just the purpose of raising revenues. At the local level, traffic cameras can be deployed in ways that don't increase accidents, and the data can again be limited for use in traffic enforcement.

These are powerful tools and technologies. Used with care and restraint, they may prove beneficial. However, ubiquitous use is likely to create a chilling effect. They cut to the core of the right to assembly, and the ability to dissent in a democracy.

We hope that moving forward, policy makers will turn their attention to privacy issues and act in ways that protect their constituents. It's often easier to enact legislation prior to new systems (for example, prior to use taxes going into effect), and to "build in" privacy. However, it's not too late to add privacy protections after technology is widely deployed, as we see with new laws around EDR data. In this way we can gain the benefits of new technologies without also incurring unfortunate side effects.