Testimony of Jim Harper
Director of Information Policy Studies
The Cato Institute
to the House Energy and Commerce Committee's
Subcommittee on Commerce, Trade, and Consumer Protection
at a legislative hearing on
"H.R. ____, the Motor Vehicle Safety Act"

May 6, 2010

Chairman Rush, Ranking Member Whitfield, and members of the subcommittee, thank you for inviting me to address this hearing on H.R. ____, the Motor Vehicle Safety Act of 2010.

My name is Jim Harper, and I am director of information policy studies at the Cato Institute. In that role, I study and write about the difficult problems of adapting law and policy to the challenges of the information age. I have maintained a web site called Privacilla.org since 2000, cataloguing many dimensions of the privacy issue, and I also maintain an online federal legislative resource called WashingtonWatch.com. It had over 1.6 million visitors in 2009.

Cato is a market liberal, or libertarian, think-tank, and I pay special attention to preserving and restoring our nation's founding, constitutional traditions of individual liberty, limited government, free markets, peace, and the rule of law.

I serve as an advisor to the Department of Homeland Security on its Data Integrity and Privacy Advisory Committee, and my primary focus in general is on privacy and civil liberties. I am not a technologist, but a lawyer familiar with technology issues. As a former committee counsel in both the House and Senate, I understand lawmaking and regulatory processes related to technology and privacy.

After sharing two prefatory observations about the constitution and risk management, I will turn to the privacy issues involved with the mandate for event data recorders authorized by section 107 of the legislation. My conclusions are that most of the Motor Vehicle Safety Act exceed the proper role of the federal government, that collective over-spending on collection of accident data may undermine the goal of preserving drivers' lives, and that mandatory EDRs are another move toward constructing surveillance infrastructure that threatens the privacy and liberty of the American citizen.

What's a Constitution When Lives Are at Stake?

My analysis of federal legislation always begins with the Constitution. Which grant of power in the Constitution allows Congress to act? And what impediments on federal power may limit Congress' action?

The Motor Vehicle Safety Act shares a constitutional infirmity with much of the legislation Congress considers today. There is no source of authority for it in the Constitution.

Likely, if your committee advances this legislation, your report will cite the commerce clause (article I, section 8, clause 3) as the specific power granted to Congress in the Constitution to enact it as law. That clause gives Congress power "To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."

The preface to the Cato Institute's pocket constitution—more than three million copies in print—discusses the meaning of this provision. Since the New Deal,[1] the Supreme Court has abandoned the meaning and purpose of the commerce clause, allowing Congress to regulate based merely on activity having effects on interstate commerce.[2]

You may regard the constitution's limited, enumerated grants of power, as quaint. But they are not. You swore an oath to bear true faith and allegiance to the constitution at the beginning of this Congress, as the Constitution requires you to do.

This is not just ceremony, and the Constitution is not just a symbol. The results of continuing nonchalance about the Constitution's limits are plain to many observers.

With reason, many people regard the federal government as overly large, remote, and imperious. Your good intentions notwithstanding, many view Congress negatively, as a body that cannot hew to any principle.

It is not just principle. There are consequences to disregarding the Constitution. Campaign finance law "reformers" believe that too much money is spent on politics and influence at the federal level. But people and organizations will always try to influence the government's influence over them. Money follows power. Huge expenditures on political influence follow directly from the hugeness of federal power.

As you press the federal government into involvement in every segment of the economy—including auto safety, automobile design, and auto safety research—you

[1] *E.g.* Wickard v. Filburn, 317 U.S. 111 (1942) (approving the regulation of wheat grown for personal use and not for sale under the Commerce Clause).
[2] The Court discovered the commerce power's present outer limits in United States v. Lopez, 514 U.S. 549 (1995), which found that gun possession near a school was too attenuated from effects on commerce to be within the commerce power.

should not be surprised to find that every segment of the economy spends money on lobbying and campaigning to push for its interests. If you want campaign finance reform, follow the Constitution and move authority back to the states and people where it belongs.

The good intentions that animate your auto safety efforts do not overcome constitutional limits on the government.

Is Auto Safety for Rich People?

Everybody shares the goal of maximizing the welfare of Americans, including by making auto travel safe. Better data about the operation of cars in the moments before collisions would almost certainly improve knowledge of how to make auto travel safer. Important questions remain about using event data recorders to generate statistical research that would improve the design of the nation's cars, however.

Risk management and benefit-cost analysis can enlighten efforts to maximize welfare by improving auto safety. As a member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, I helped design a framework for analyzing programs that generalizes to the problem of auto safety. In fact, we used the "security" of cars against common threats to illustrate risk management.

In the DHS Privacy Committee's "framework document,"[3] we defined the risk management problem as determining how, and how well, a program addresses threats to the public. With benefit information in hand, the costs of the program can be compared to determine whether it cost-effectively lowers risk. (Making auto travel safer for people is easier than securing against terrorism. Both the threats to car occupants and the costs of steps to counter such threats are easier to measure.)

Responses to health threats like automobile collisions can be categorized four ways:

- Acceptance—a rational alternative that is often chosen when the threat has low probability, low consequence, or both. Low-speed "fender benders" occur often, but are acceptable in terms of human safety because they have only the rarest impacts on life and health.

- Prevention—alteration of the target or its circumstances to diminish the risk of the bad thing happening. This is the main goal of data collection, to learn how cars might be altered to protect life in the event of serious collisions.

[3] Report of the Data Privacy and Integrity Advisory Committee, No. 2006-01 (March 29, 2006) http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf.

- Interdiction—confrontation with, or influence exerted on, an attacker to eliminate or limit its movement toward causing harm. The Privacy Committee report cited "flashing your lights to warn another car about the fact that you are passing" as a "mild interdiction." Discovering new interdiction techniques may be a goal of data collection.

- Mitigation—preparation so that, in the event of the bad thing happening, its consequences are reduced. It is unlikely, but the inclusion of first aid materials, for example, may be a mitigation of the effects of collisions on human health.

More data might contribute to each type of response to threats to human health from auto collisions. Continuing with the risk management framework:

> The final step in analyzing the program's efficacy is to be aware of new risks created by the prevention, mitigation, or interdiction of the threats under consideration. Installing heavy iron siding to a car may mitigate the risk to the car from accidents. At the same time, the reinforced car may pose new risks to other cars and pedestrians.

I do not worry that NHTSA will propose iron siding that sends cars careening into bike paths and playgrounds. But the costs of the data collection program may have risk transfer effects that are important to consider.

According to the Research and Innovative Technology Administration's Bureau of Transportation Statistics there were 6,813,369 new retail sales of passenger cars in the United States in 2008.[4] This is the lowest number of new car sales since at least 1990, given economic conditions 2009 was probably not a good year, and the only year for which BTS reports lower sales is 1960. The number of vehicles on American roads, meanwhile, continues to rise, to a whopping 254,403,082 as of 2007.[5]

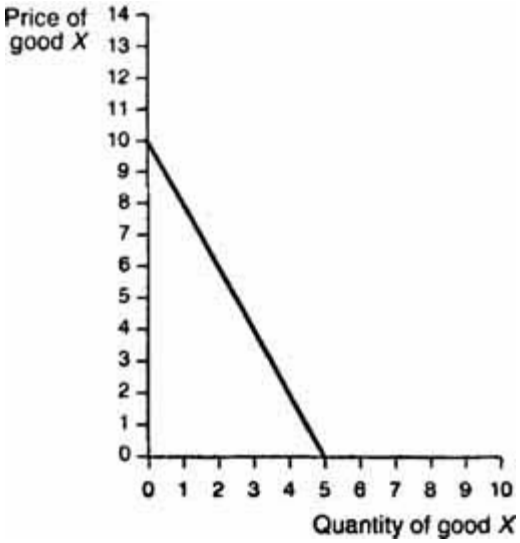
A demand curve is a graph illustrating the willingness of consumers to buy at a certain price. A downward sloping demand curve reflects the common circumstance in most markets: people buy less of things that cost more. In the demand curve pictured on the next page, an increase in price of two units will cause sales to drop by one unit.

---

[4] U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, Table 1-12: U.S. Sales or Deliveries of New Aircraft, Vehicles, Vessels, and Other Conveyances
http://www.bts.gov/publications/national_transportation_statistics/html/table_01_12.html

[5] U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, Table 1-11: Number of U.S. Aircraft, Vehicles, Vessels, and Other Conveyances
http://www.bts.gov/publications/national_transportation_statistics/html/table_01_11.html

This is not the demand curve for automobiles in the United States, but the U.S. automobile demand curve almost certainly slopes the same direction. When automobiles are more expensive, people buy fewer automobiles.



I do not know how steep the U.S. demand curve for automobiles is, and I do not know the cost of installing electronic data recorders in cars. But it is a near certainty that putting EDRs in cars raises their costs and lowers sales.[6] It lowers sales more for poor people than for rich people. New car sales affect the availability of used cars, of course, and the cost of trading up from an older used car to a newer used car.

This has negative effects for the automobile industry, of course, and unemployment has negative effects on the health and well-being of people. But lower auto sales probably also have negative effects on the safety of drivers and passengers.

When people forgo new car purchases or trade-ups to newer used cars, they remain in older cars that are likely to be involved in more collisions due to wear and tear and design problems that have been rectified in newer models. When they are in collisions, occupants of older cars may suffer more injury and death than they would in newer cars which are better designed to protect them.

Because the poor are in older cars, the bulk of these effects—greater numbers of collisions and greater morbidity and mortality in collisions—will fall on poor people.

I do not have the cost data or the economic training to determine the amount of injury and death produced by including EDRs in automobiles, but it is almost certainly above zero, and it probably falls more heavily on the poor.

It would be a mistake to conclude that EDRs should not be put in automobiles. The data they collect can improve auto safety so that the dynamic I have described—newer cars being safer—will continue.

[6] I focus here on the policy of putting EDRs in all cars as a whole, not the incremental advance of that policy in this bill. By requiring all makes to build EDRs into their cars, the bill would prevent any one manufacturer from gaining a cost advantage by not doing so.

The idea of trade-offs merely sharpens the auto safety risk management question to: *How much data do you need to make cars safer?*

It seems plain that statistically relevant evidence about auto safety could be produced using sampling, by drawing on a cross-section of collisions from which EDR data is available. Putting EDR functionality in every car is overkill that has costs.

Perhaps 50% of the cars produced should have EDRs. Maybe it's 30%, or 60%. If there is to be a mandate, why not place it on more expensive models?[7] If EDRs were offered as a public safety option, perhaps the wealthier cohort of auto consumers would choose them, avoiding cost impositions that endanger the poor.

Analyzing EDR data from 100% of accidents is not required to produce valid auto safety research. An across-the-board mandate serves some other end, which I speculate about below. The auto industry's general "voluntary" inclusion of EDRs in automobiles is not strong evidence to the contrary. The industry may not have considered these trade-offs, or it may be pursuing ends beyond or distinct from safety.

EDRs and Privacy

Privacy is a complex and vexing issue, and the interaction between EDRs and privacy is a challenge to describe or calculate. But the installation of EDRs in U.S.-sold vehicles to date has been a challenge to privacy. Making EDRs mandatory in new U.S. vehicles will erode privacy further, the privacy protections in the Motor Vehicle Safety Act notwithstanding.

The word "privacy" is used casually to describe many concerns in the modern world, including fairness, personal security, seclusion, and autonomy or liberty. Few concepts have been discussed so much without ever being solidly defined.

The strongest sense of the word "privacy" is its control sense: having control over personal information about oneself. In his seminal 1967 book *Privacy and Freedom*, Alan Westin characterized privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

I use and promote a more precise, legalistic definition of privacy: as the subjective condition people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and

[7] That rule could be adjusted where less expensive models do not share all the relevant design characteristics with the more expensive models.

values.[8] The "control" dimension of privacy alone has many nuances, and I will parse them here briefly.

A Personal, Subjective Condition

Importantly, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be.

To illustrate this, one has only to make a few comparisons: Some Americans are very reluctant to share their political beliefs, refusing to divulge any of their leanings or the votes they have cast. They keep their politics private. Their neighbors may post yard signs, wear brightly colored pins, and go door-to-door to show affiliation with a political party or candidate. The latter have a sense of privacy that does not require withholding information about their politics.

Health information is often deemed intensely private. Many people closely guard it, sharing it only with doctors, close relatives, and loved ones. Others consent to have their conditions, surgeries, and treatments broadcast on national television and the Internet to help others in the same situation. More commonly, they relish the attention, flowers, and cards they receive when an illness or injury is publicized. Privacy varies in thousands of ways from individual to individual and from circumstance to circumstance.

An important conclusion flows from the observation that privacy is subjective: government regulation in the name of privacy is based only on politicians' and bureaucrats' guesses about what "privacy" should look like. Such rules can only ape the privacy-protecting decisions that millions of consumers make in billions of daily actions, inactions, transactions, and refusals. Americans make their highly individual privacy judgments based on culture, upbringing, experience, and the individualized costs and benefits of interacting and sharing information.

The best way to protect true privacy is to leave decisions about how personal information is used to the people affected. Political approaches take privacy decision-making power away from the people. At its heart, privacy is a product of autonomy and personal responsibility. Only empowered, knowledgeable citizens can formulate and protect true privacy for themselves, just as they individually pursue other subjective conditions, like happiness, piety, or success.

---

[8] *See generally*, Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Policy Analysis No. 520 (Aug. 4, 2004) http://www.cato.org/pub_display.php?pub_id=1652

The Role of Law

The legal environment determines whether people have the power to control information about themselves. Law has dual, conflicting effects on privacy: Much law protects the privacy-enhancing decisions people make. Other laws undermine individuals' power to control information.

Various laws foster privacy by enforcing individuals' privacy-protecting decisions. Contract law, for example, allows consumers to enter into enforceable agreements that restrict the sharing of information involved in, or derived from, transactions. Thanks to contract, one person may buy foot powder from another and elicit as part of the deal an enforceable promise never to tell another soul about the purchase. In addition to explicit terms, privacy-protecting confidentiality has long been an implied term in many contracts for professional and fiduciary services, like law, medicine, and financial services. Alas, legislation and regulation of recent vintage have undermined those protections.[9]

Many laws protect privacy in other areas. Real property law and the law of trespass mean that people have legal backing when they retreat into their homes, close their doors, and pull their curtains to prevent others from seeing what goes on within. The law of battery means that people may put on clothes and have all the assurance law can give that others will not remove their clothing and reveal the appearance of their bodies without permission.

Whereas most laws protect privacy indirectly, a body of U.S. state law protects privacy directly. The privacy torts provide baseline protection for privacy by giving a cause of action to anyone whose privacy is invaded in any of four ways.[10] The four privacy causes of action, available in nearly every state, are:

- Intrusion upon seclusion or solitude, or into private affairs;
- Public disclosure of embarrassing private facts;
- Publicity that places a person in a false light in the public eye; and
- Appropriation of one's name or likeness.

While those torts do not mesh cleanly with privacy as defined here, they are established, baseline, privacy-protecting law.

---

[9] The Gramm-Leach-Bliley Act and federal regulations under the Health Insurance Portability and Accountability Act institutionalized sharing of personal information with government authorities and various "approved" institutions. See 15 U.S.C. §§ 6802(e)(5)&(8); various subsections of 45 C.F.R. 164.512.

[10] Privacilla.org, "The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection," (July 2002) http://www.privacilla.org/releases/Torts_Report.html.

Law is essential for protecting privacy, but much legislation plays a significant role in undermining privacy. Dozens of regulatory, tax, and entitlement programs deprive citizens of the ability to shield information from others. Mandated EDRs undermine privacy, despite the protections outlined in the Motor Vehicle Safety Act, as I will discuss below.

Consumer Knowledge and Choice

Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power over information about themselves consistent with their interests and values. This requires consumers and citizens to be aware of the effects their behavior will have on exposure of information about them.

Technology and the world of commerce are rapidly changing, and personal information is both ubiquitous and mercurial. Unfortunately, there is no horn that sounds when consumers are sufficiently aware, or when their preferences are being honored. But study of other, more familiar, circumstances reveals how individuals have traditionally protected privacy.

Consider privacy protection in the physical world. For millennia, humans have accommodated themselves to the fact that personal information travels through space and air. Without understanding how photons work, people know that hiding the appearance of their bodies requires them to put on clothes. Without understanding sound waves, people know that keeping what they say from others requires them to lower their voices.

From birth, humans train to protect privacy. Over millions of years, humans, animals, and even plants have developed elaborate rules and rituals of information sharing and information hiding based on the media of light and sound.

Tinkering with these rules and rituals today would be absurd. Imagine, for instance, a privacy law that made it illegal to observe and talk about a person who appeared naked in public without giving the nudist a privacy notice to that effect and the opportunity to object. People who lacked the responsibility to put on clothes might be able to sue people careless enough to look at them and to recount what they saw. A rule like that would be ridiculous, but legislation of precisely this character has been a staple of privacy proposals in Congress for at least a decade.

The correct approach is for consumers to be educated about what they reveal when they interact online and in business so that they know to wear the electronic and commercial equivalents of clothing.

No, Really: EDRs and Privacy

If you needed any proof that privacy is complex, witness the fact that my introduction of the concept has consumed three written pages. I now turn to how EDR policy currently threatens privacy by depriving consumers of control over personal information.

There are at least three ways that EDRs undermine privacy: In the current market environment, consumers generally cannot control whether or not their vehicles have EDRs; they do not control what their EDRs do; and they have limited ability to control what happens with the data. The Motor Vehicle Safety Act makes the problem worse with regard to the first two, while providing some protection with regard to the third.

Control of Whether or Not Vehicles Have EDRs

As I noted earlier, giving consumers choice with regard to EDRs could improve auto safety by allowing price-sensitive consumers—the poor—to decline having them. The margin of cost savings could move these consumers into safer vehicles, saving their lives and the lives of others.

This would also protect privacy. If EDRs were a choice, auto manufacturers, marketers, dealers, and resellers would give consumers at least some information about EDRs and what they do. There would be greater public discussion of their safety merits, privacy consequences, and value per dollar because car buyers could do something with that information.[11]

Consumers motivated by privacy could opt out of having EDRs entirely. Consumers motivated by personal and public safety could opt to have EDRs in their vehicles. Giving consumers control over the choice whether to have EDRs in their cars would improve their privacy by improving their control over their personal information infrastructure.

Control of What EDRs Do

I note that some states have proposed to give consumers control of whether their EDRs are activated.[12] This would shore up consumers' control of personal information and thus

[11] It is important not to be fooled by today's public ignorance of EDRs. Consumers are able to make choices about EDRs. In the present market environment, with EDRs standard on most vehicles, consumers exercise rational ignorance: There is no plausible benefit from learning about EDRs, so they invest no time or energy in learning about them or their consequences. They are disempowered objects of government and industry policy.

[12] I have not investigated the status of state laws, but a 2006 article cites proposed legislation in Montana, New Hampshire, and New Jersey. Aleecia M. McDonald and Lorrie Faith Cranor, How Technology Drives Vehicular Privacy," I/S: A Journal of Law and Policy for the Information Society, Volume 2, Issue 3 (2006) http://lorrie.cranor.org/pubs/vehicular-privacy-authorsVersion.pdf.

their privacy. Consumers could decide based on their particular circumstances whether they want their vehicle collecting data about their use of it.

Given all the technology built into it, it is not a stretch to say the car is a computer. But consumers do not get to control this computer. Consumers should have more choice and control. At a minimum, government policy should not deprive them of it or channel the market away from consumer control.

Of course, EDRs today are closely integrated with basic vehicle operations and safety features like air bags. This is a historical accident, not something inherent to EDRs. The data recording function could be logically separated from vehicle maneuvering and operated by drivers from the console.

An extension of this thinking would be to give consumers the ability to access and control much of the software that runs inside their vehicles. Red Hat CEO Jim Whitehurst recently made a pitch for automakers to adopt open source principles in a recent, very interesting *Business Week* commentary.[13]

Open source has its place, and I would not recommend open source for the functions integral to stopping, starting, and turning, but the many other computing and communications features in automobiles would benefit from open source software development. A feature of this approach would be that consumers could gain control over the functioning of much of the computing their automobiles do.

This control would improve their privacy by allowing them to select what data is recorded, how long it is kept, where and how it is stored, and so on. Given the opportunity, some drivers might create extensive personal records of their driving, perhaps offering researchers greater insight into driver behavior than the mandatory, one-size-fits-all EDRs envisioned by the Motor Vehicle Safety Act.[14]

One can only guess at why government and corporate policy is converging on requiring EDRs in cars and denying consumers control of the EDRs' functioning. My best guess is that their use in litigation is regarded by industry as an important protection and by litigators as important evidence.

EDR data is being used in litigation today, and its use will increase. Giving consumers control of the data would protect privacy, but it would frustrate the interests of

---

[13] Jim Whitehurst, "Why Toyota Should Go Open Source," Bloomberg Businessweek (Apr. 1, 2010) http://www.businessweek.com/innovate/content/mar2010/id20100329_064567.htm.

[14] Researchers might pay for it, opening up a new market in which some drivers cleverly capitalize on personal information about themselves to subsidize their mobility.

government, industry, and the trial bar. When all these interests unite in Washington, D.C., it is no surprise that consumer privacy loses.

Control of EDR Data

With consumers substantially deprived of control over EDRs' existence and functioning, protections going to the use of EDR-produced data cannot be entirely satisfying. The rules about data proposed in the Motor Vehicle Safety Act provide some privacy protection, but far less than the full array of controls consumer should have.

Section 107(d)(1) would make any data in an EDR the property of the owner or lessee of the vehicle in which it is installed. This restates the appropriate and probable legal status of such data. It is some benefit to privacy to have a restatement because the law in this "new" area is unclear.

The privacy subsection (107(d)(2)) bars collection of the data by anyone other than the owner or lessee except in certain circumstances: when there's a court order, with the data owner's permission, and when a government agency has certain beneficent purposes.

The first two are appropriate restatements of the appropriate legal rules around data, and I take it that the court order provision is not meant either to expand or to contract the circumstances in which courts can authorize or require the acquisition of EDR data.

The third is interesting, though, because it illustrates how the bill giveth with one hand and taketh away with the other. It creates (or affirms) an intellectual property right in EDR data, but prescribes an unrestricted, royalty-free license to that data benefiting government researchers. The license is limited to data that will not reveal the identity of the driver, owner, or lessee—a privacy protection—but on balance this provision reduces the consumer's control by carving another exception from consumer control of data produced by the EDR.

There is little question that the data in someone's computer is their property. So it is with the data in people's cars. But the Motor Vehicle Safety Act would reduce people's property rights in EDR data by a small margin.

Overall the disability on consumers to control the existence of EDRs in their cars and to control the functioning of EDRs in their cars threatens privacy. And it threatens privacy more than the modest protections of EDR data in the bill, which restate, then slightly derogate from, the better view of existing law about who "owns" data.

There is no privacy apocalypse that occurs should EDRs be mandatory nationwide in all new cars. This is but a small step in the continuing erosion of privacy that has been going on for years—and that will continue.

The future trajectory of EDR policy is deeply concerning. As they have in the past, EDRs will probably continue to add new functions and capabilities.

I note with dismay that the bill would allow NHTSA to require EDRs to capture "certain events such as rapid deceleration, full-throttle acceleration lasting more than 15 seconds, and full braking lasting more than 10 seconds, even if there is not a crash or airbag deployment." This is an open-ended grant of authority that could allow recording of travel at 90+ miles per hour or 85 miles per hour, or maybe 70.

Future changes to policy may further erode the weak privacy protections in the bill. Perhaps reasonable suspicion will allow law enforcement officers to access EDR data and issue speeding tickets based on it. The existing ban on location data may fall, or EDR data might be correlated with location data collected by other functions in the car.

The mandatory EDR is surveillance infrastructure. There are no two ways about it. At some point in the future, a day will come when it is "switched on," and drivers across the country may be subject to government monitoring of their comings and goings.

Government and industry appear largely to agree on having EDRs in all our automobiles, with consumers prevented from controlling those EDRs. Because the data collected by EDRs will be available to government and litigators, the Motor Vehicle Safety Act puts a sort of ankle bracelet on every American driver when he or she gets behind the wheel.

These things are not happening because of an evil plot hatched at NHTSA or because of a cabal between NHTSA and the auto manufacturers. They are happening because so few people are looking down the road. You should be aware that the good intentions behind this bill help build "Big Brother infrastructure."

To avoid this, to protect privacy, and to limit the injury and loss of life that I think comes from an overbroad mandate for EDR use, federal policy should prefer EDRs to be optional, or at least not make them mandatory. Consumers should have control over the functioning of EDRs in their cars. And if they choose them, consumers should have full ownership of the data their EDRs produce, being free to barter or trade that data to anyone who wants to access it.