Privacilla.org

http://www.privacilla.org

Prepared Statement of Jim Harper, Editor of Privacilla.org
at the Hearing on Red-Light Cameras
U.S. House of Representatives
Committee on Transportation and Infrastructure
Subcommittee on Highways and Transit

July 31, 2001

Chairman Petri, Ranking Member Borski, and Members of the Subcommittee:

It is a great pleasure to appear before you to discuss red-light cameras and their implications for privacy. I am Jim Harper, the Editor of Privacilla.org, a Web-based think-tank devoted exclusively to privacy. I started the Privacilla project a little less than a year ago to help improve the quality of the privacy debate in Washington and in capitols around the country. Privacy is one of the most complex and difficult public policy issues around today. I am pleased to lend what knowledge I have to your consideration of red-light cameras.

Privacilla is a Web site that attempts to capture "privacy" as a public policy issue from top to bottom. Anyone may submit ideas, information, and links for inclusion on

the site. The site represents the thinking of many people and I would refer you to the Privacilla "Support" page to get an idea of the groups we work with. Please visit the site and use it as a resource whenever your work brings you to a privacy policy question.

Privacilla takes a free-market, pro-technology approach to privacy policy. There certainly are other views, and you should consider them all. Please also be aware that Privacilla is currently a project of my lobbying and consulting firm, PolicyCounsel.Com. My firm does not represent anyone on privacy specifically, but nearly all issues touch on privacy in some way, so you should consider my potential for bias, as you would with any privacy advocate.

Chairman Petri, I salute you for holding these hearings. Increasingly, as Americans travel the streets and highways of the nation, they see cameras bristling from stoplights and streetlights — and many people are bristling back. They find these cameras offensive, insulting, and an invasion of their privacy.

It is incumbent on Congress and policy-makers at the state and local levels to examine whether red-light cameras are being used fairly and appropriately, or whether they are better regarded as an intrusion into our lives and routines. You are brave to take on this challenge because it is not a small one. The issues are difficult and the balances to be struck are delicate.

Red-light cameras are only one, highly visible example of the rapid advance of technology in law enforcement and government. There is no question that technology in the hands of both government and the private sector has provided us enormous benefits and will continue to do so. We must be vigilant, however, to make sure that we enjoy as many of the benefits as we can while minimizing the costs and drawbacks.

A significant cost posed by many information technologies is the threat they pose for privacy. The challenge is particularly difficult while we as a society learn how these technologies work. At this early point in the Information Age, we are particularly prone to overreacting either against or in favor of information technology.

I am happy that you recognize the importance of privacy as a significant consideration regarding red-light cameras. This technology represents only the tip of an iceberg. Beneath the water lie many questions about Americans' privacy interests and expectations as all elements of society incorporate digital technology into their basic functions.

Red-Light Cameras Raise a Host of Issues

Red-Light cameras raise a whole host of issues in addition to privacy. They may be cash cows for governments and the technology companies that design, build, and install them. Their use may be unfair if they are not reliable, or reliably checked. There are important due process questions, too, such as whether a person is denied the right to

confront his or her accuser when an automated system purports to discover and record the only evidence of crime.

And there are problems of proof. As you know, criminal responsibility attaches only to people. Evidence of a car passing through an intersection does not prove who drove it unless the driver is photographed too.

There is a lot to be said for law enforcement by men and women in uniform. More often than not, they are members of the community. Through in-person contacts, they help make clear that the traffic laws reflect society's collective judgment about the safety of people. Traffic laws are not just technical rules that take a bite out of us when we are tripped up by an indifferent machine.

One can only imagine what investigative tangles could arise from red-light cameras. It is a fair guess that some portion of the population will deny that they were driving the cars photographed by red-light cameras, because they actually were not driving or because they think the authorities will not press these cases. From time to time, jurisdictions may seek to prosecute "false deniers" and mete out large punishments to "teach them a lesson." This could create an atmosphere of widespread disrespect for law combined with sporadic and draconian enforcement.

Importantly, *post hoc* investigations into red-light running may mean that citizens have to submit alibis in response to automatically issued summonses for traffic violations. These alibis may be investigated and turn a traffic violation into a privacy-invading inquest. We clearly start down a path where what should be ordinary traffic enforcement can become a legal and investigative mess.

"Big Brother" Technologies Are Upon Us

Red-light cameras are only the first installation of the Big Brother infrastructure. There is much more to come.

Little technical difference separates a digital camera that takes occasional snapshots from one that records continuous footage. With optical character recognition, there will soon be the technical capability for nominal red-light cameras to scan for the license plates of specific cars. Networked cameras will soon be able to track cars throughout a city and on the highways. And database technology will make it possible to create permanent records of the movements of all cars captured on camera.

It should not go without saying that these technologies can be used for good. And there is a lot of good to be gotten from them. Known or visible red-light cameras will tend to deter red-light violations among the small number of people who consciously run red lights or push the limits. Red-light cameras can improve safety — as long as they are not used in conjunction with shortened yellow-light times. When traffic cameras can be

used to find stolen vehicles, the effect on car-jacking, for example, may be dramatic. Criminals will know that they have only minutes from when they steal a car to when that car effectively turns them in. These technologies may allow the last movements of missing persons to be more easily learned thanks to records of where their cars were.

When it was revealed that face-scanning technologies were used at the Super Bowl earlier this year, the crime-suppression benefits were obvious. This type of surveillance may make air travel and any large public event eminently safer because terrorists or rioters — even pickpockets and purse-snatchers — will be aware that they could be identified and apprehended even before they act.

For these reasons, these technologies are quickly being incorporated into our country's public safety and law enforcement arsenals. These benefits do not dispose of the issues, though. We have important crime-control and public safety benefits arrayed against important values like the legitimacy of law enforcement, fairness, and, of course, privacy.

Technology will soon give governments many capabilities of Orwell's "Big Brother." But, as lawmakers, you have the capability to make sure that governments throughout America use technology only for good and not for invading privacy.

"Big Brother" Government is What to be Concerned About

As Members of Congress, your proper focus, the area where you can do the most productive work, and the area where you are most responsible is privacy from government.

Everyone owes their respect and gratitude to our nation's elected officials and public servants. They work hard, make enormous sacrifices, and devote themselves to the betterment of society — often for little reward and even smaller thanks. Government officials have the best of intentions and they do the best they can to cope with enormous problems and strongly competing demands. There is no question that the *people* in our nation's government sector are honorable, thoughtful, and well-intended.

At the same time, it is my strong conclusion that the government *sector* presents more significant threats to privacy than individuals and businesses in the private sector. More so than the private sector, governments have the capability and the incentive to take, use, and abuse the personal information of citizens. George Orwell wrote *1984*, bringing us the infamous concept of "Big Brother," as a warning against the power of governments — not the private sector.

Many privacy advocates overlook the differences between government and the private sector, and their advocacy suffers because of it. They use wordplay like "Big Browser" and invite Congress to replace consumer choice and the power to contract —

backed up by state privacy tort law — with top-down, one-size-fits-all federal regulation of the private sector. And they do this while government itself is not subject to sufficient privacy-protecting limits.

Government and the private sector have radically different incentives relating to personal information about consumers and citizens, and they operate in entirely different legal regimes. The government sector does not lose customers if it collects too much information or if it uses it in offensive or harmful ways. Businesses do. The fact that governments collect information using the force of law cannot be emphasized strongly enough. When a government agency or program needs personal information to carry out its mission, that information will be collected. Individuals have no choice in the matter. This is not the case with businesses, who must bargain in one way or another for the information they want.

An important upshot of this is that consumers are more often allowed to remain anonymous or use fake names when dealing with businesses. As long as one is not committing fraud, the penalty for lying about one's identity to a business may be, at worst, that a transaction is not completed. When dealing with government, however, anonymity or pseudonymity is often impossible, illegal, or, at the very least, suspicious.

The accountability we require of government also gives rise to privacy problems that are not found in the business world. The public can and should have access to public

records in order to hold officials accountable and because the information was collected using public funds. Open records, a hallmark of open government, can often mean that information citizens were compelled to disclose becomes public.

In lieu of a healthy system of incentives, governments respond to a patchwork of privacy laws imposed on themselves. Most importantly, at the federal level we have the Fourth Amendment, which limits the power of governments to collect information in some respects. It only applies, however, in the criminal context. It does not prevent government from taking information for "administrative" purposes.

The Privacy Act and the Freedom of Information Act strike some balance between privacy and open government. But these laws are a confusing welter of definitions, exceptions, and exceptions to exceptions. As Privacilla revealed in a March, 2001 report, federal agencies constantly share personal information about American citizens; new information sharing programs are introduced more than once every other week.[1] The Privacy Act does not reassure Americans that their information is confidential, safe, or private in the hands of the government.

The laws controlling government do not evolve and respond to change as the law governing the private sector can — such as contract rights and the privacy torts in

common law courts. Government information practices move in fits and starts as new uses of information expose loopholes in government privacy protections. Hopefully, red-light cameras will prompt such a change in our laws as Congress considers reducing the demands programs across the board make for citizens' personal information.

Also, because governments are only subject to the laws they make for themselves, information held by governments — even if confidential "by law" — is not as well protected as information held under similar restrictions by businesses. Governments are sovereigns that can change the laws that apply to the information they hold, and they often do.

Government and the private sector are made up of vastly different entities with dramatically different incentives, and who operate under different laws. Protecting privacy in the commercial world is often difficult, but protecting privacy from government is usually impossible.

Again, there is no question that public servants in all branches and at all levels are dedicated to the best interests of citizens. In their focus on efficiency, law enforcement, or other good-government values, however, officials far too often ignore privacy. The

---

[1] *Privacy and Federal Agencies: Government Exchange and Merger of Personal Information is Systematic and Routine*, Privacilla.org (March, 2001); available at <http://www.privacilla.org/Government_Data_Merger.pdf>.

founders of our nation recognized this, which is why they included the protections of the Fourth Amendment in the Bill of Rights.

The Fourth Amendment Allows People to Protect Privacy — Even in Public

To get at the privacy implications of red-light cameras, we have to dig deeply. The Fourth Amendment says: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[2] This is the primary, essential limit on the power of American governments to inquire into people's lives, arrest them, and seize their property for criminal investigations.

It is important to note that the Fourth Amendment does not protect privacy *per se*. By providing Americans with a protected zone, though, it allows them to maintain privacy as they see fit. Affirmatively creating privacy — the subjective condition of having control over information about one's self — is the responsibility of individuals acting in the shelter of their legal rights. Every day, Americans make highly individual privacy judgments based on culture, experience, and the perceived costs and benefits of interacting and sharing information. This is why broad private-sector legislation aimed clumsily at "protecting privacy" for consumers is doomed to fail.

[2] U.S. CONST. amend. XIV.

The Fourth Amendment requires a search to be based on probable cause. That is, government investigators must have a reasonable belief that a crime has been committed and that evidence or fruits of the crime can be found. The first question a court will ask when a citizen claims to have been unconstitutionally searched is whether that person had a reasonable expectation of privacy in the place, papers, or information that government agents have examined or taken. This is one of the primary questions raised by red-light cameras.

Until 1967, the Fourth Amendment was largely regarded as protecting places — namely the home and the areas closely surrounding the home. When the Bill of Rights was drafted, ours was a low-tech, mostly agrarian, and relatively immobile society. The home really was a person's castle. As America has become more mobile and technological, this early interpretation has had to change. *Katz v. United States*[3] is the landmark Supreme Court decision that updated Fourth Amendment law in light of our advancement.

In *Katz*, FBI agents placed electronic eavesdropping equipment on the outside of a telephone booth where the defendant, a bookmaker, conducted his business. The Court held that eavesdropping on Katz in this way without a warrant violated his Fourth

[3] 389 U.S. 347 (1967).

Amendment rights because he justifiably relied on the privacy of the telephone booth.[4] The Court stated, in a famous passage, "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[5]

Justice Harlan's influential concurrence described a two-pronged test to determine when a person is entitled to assert Fourth Amendment protection. Harlan suggested, first, that a person should have exhibited an actual, subjective expectation of privacy. Second, the expectation must be one that society is prepared to recognize as reasonable.[6]

Under cases like *Katz*, the first reaction of constitutional scholars to red-light cameras may be that people do not have a subjective expectation of privacy when they drive their cars on public streets. Therefore, people can not object based on the Fourth Amendment if government-operated cameras routinely capture the images of their cars or license plates on public streets.

Yet the instinct of many Americans is that this offends privacy. I think that instinct is correct. To understand why, we have to parse out the red-light camera interaction a little more carefully.

---

[4] *Id*. at 353.
[5] *Id*. at 351.

"Anti-Privacy" Law Should Not Prevent Expectations of Privacy in Travel on Public Streets

For good reasons, people often refuse to disclose information about themselves and their identities, or they give others fake information. This maintains privacy at the levels people want. It is a common and appropriate social behavior.

But anonymity and pseudonymity are rarely an option for people when they deal with government, which regularly makes these things illegal in the name of crime control or for other important programs and policies. Governments particularly threaten privacy through law and regulation that prevent people from remaining anonymous or pseudonymous.

The Social Security Number, for example, was devised because anonymity, pseudonymity, and financial privacy from government were inconsistent with the demands of the Social Security system. A similar byproduct of the income tax is that citizens have to reveal a great deal more about themselves to employers and the government than they otherwise might. The federal Bank Secrecy Act authorizes the Treasury Department to require financial institutions to maintain records of personal financial transactions and report them to the government. The Federal Communications

[6] *Id*. at 361.

Commission's E911 program requires mobile phone services to be able to track and communicate the locations of users. The list goes on and on.

A large swath of law and regulation is fairly regarded as "anti-privacy" because it prevents people from protecting privacy as they see fit. Such laws are not automatically "bad" because of it, but we should recognize that they subsume individual privacy to collective social goals.

In this sense, the requirement in all fifty states that cars must exhibit license plates linked to their owners is "anti-privacy" law, as would be a law requiring people to wear name tags in order to walk on public sidewalks. Mandatory license plates prevent citizens from exhibiting the expectation of privacy that Justice Harlan wrote about in *Katz*. Roughly speaking, they require people to expose their identities to police as a condition of driving on our roadways.

Because the law has deprived people of the ability to protect privacy, the better view is that there is a Fourth Amendment search when law enforcement notes the license plates on cars. This search is inherently unreasonable if they do so when they do not suspect crime. As soon as red-light cameras are used for anything other than snapping suspected speeders — and they soon will be — these cameras should be shown a red light themselves.

Though some of the people who object to red-light cameras do so because they do not want to get caught, the rest deplore the idea that their movements are potentially subject to monitoring thanks to new technology. We are a free country and a free people who reject the idea of being monitored by government when we are going through our daily lives peacefully and lawfully.

Eliminating the automobile license plate is obviously not the appropriate response. The slight threat to privacy embodied in the license plate pales in comparison to the benefits we enjoy in terms of safety and crime control. License plates make drivers appropriately accountable to each other and to law enforcement.

Kyllo v. United States Prevents Government From Using Advanced Technology to Invade Privacy

Getting rid of the license plate would be the equivalent of lining the walls of our homes with asbestos if the U.S. Supreme Court's *Kyllo* decision had gone the other way.

In *Kyllo v. United States*,[7] decided in June, the Supreme Court issued an important opinion in the development of Fourth Amendment law. Agents of the U.S. Department of the Interior, suspicious that Danny Lee Kyllo was growing marijuana in his home using high-intensity lamps, had aimed an Agema Thermovision 210 thermal imager at his

[7] No. 99-8508 (U.S. Sup. Ct. June 11, 2001)

triplex on Rhododendron Drive in Florence, Oregon. The imager detected significantly more heat over the roof of the garage and on a side wall of Kyllo's home than elsewhere on the premises. Using this information, the agents got a warrant, searched the home, and found the drugs they suspected.[8]

The war on drugs has pushed law enforcement to test the limits of its search and surveillance powers in many respects, and the Supreme Court has not always defended Americans' privacy rights as it should. In this case, however, the Supreme Court reversed Kyllo's conviction, finding that when a novel device like the thermal imager is used "to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[9]

There are many ways to distinguish the facts in *Kyllo*, and future cases will decide its meaning better than I know how, but the case does have substance for red-light cameras and other surveillance technologies. The case required the Court to confront "what limits there are on [the] power of technology to shrink the realm of guaranteed privacy."[10]

[8] *Id.* at 1-2 (Slip Op.).
[9] *Id.* at 12.
[10] *Id.* at 6.

In remanding Kyllo's conviction, the Court essentially found that the reasonableness of a search is to be judged in light of common privacy-protecting practices, not in light of privacy protection from the best technologies available. Thermal imagers are not in general public use so people desiring to keep the hours of their sauna private from neighbors do not line their walls with asbestos. Likewise, digital video of streets is not in general public use, so a person desiring to keep private his or her trip to the psychiatrist's office does not have to remove or cover the license plates on his or her car (and, legally, one can not).

Soon, Big Brother cameras will enable law enforcement to record or track the movements of cars driven by people not suspected of crime. Used without a warrant or in the absence of exigent circumstances, these would be a grave threat to privacy interests that are protected by the Fourth Amendment.

Congress Should Protect Privacy *and* the Benefits of Red-Light Cameras

Because of their benefits, red-light cameras and other surveillance technologies can not be dismissed out of hand. At the same time, their privacy-invading potential demands a firm response. The correct response strikes a balance between the privacy costs and law-enforcement benefits of surveillance technology.

People have a reasonable expectation, as innocents, that governments will not compile investigative information about them. No surveillance technology should be used to monitor anyone other than people reasonably suspected of crime. Law enforcement should be required to dispose of surveillance data about innocents that is not relevant to a pending investigation of crime.

Congress should protect privacy and reassure the public with a law articulating appropriate and inappropriate government uses of red-light camera data — and all forms of surveillance data — along these lines. This is a clear prerogative of the federal government, which has authority to enact law such as this under section five of the Fourteenth Amendment.

Congress should avoid dictating to states on local law enforcement issues or coaxing them with conditional spending. As long as they do not cross clear Fourth Amendment lines drawn by Congress, states should be free to incorporate technology into law enforcement and use it however their citizens desire. They should be able to experiment and learn from each other how best to respond to the varied, competing, and quintessentially local demands of their citizens.

Conclusion

Chairman Petri, again thank you for conducting this hearing. Red-light cameras are one of the first in what will be a long succession of technologies that raise issues like

this. Through your leadership, privacy from government surveillance will increasingly be recognized as an issue that deserves the full attention of Congress and the country.

Technologies like the Internet have started a useful civic discussion of privacy. Much of what has consumed Congress of late is a reexamination of private-sector information practices that have been evolving for decades. Too often, these discussions tend toward sloganeering by advocates and hysteria in the press. Pro-regulation privacy advocates have yet to articulate any harm to consumers that would justify additional regulation of the private sector.

Red-light cameras are the beginning of the Big Brother infrastructure — and the term "Big Brother" has always referred to intrusive government. Despite the pure intentions of the people in them, governments at all levels pose the greater threat to privacy than the private sector. On privacy from government is where the focus of our public policy should be.

The rapid growth of digital technology is testing Fourth Amendment privacy protections because sensory enhancing, optical character recognition, networking, and database technologies can be so powerful. As the powerful forces of government and technology combine, the results may be very bad for Americans' privacy and freedom. Governments are the only entities in society with legal power to enter our homes without permission, take our possessions, and imprison us.

Our public policy relating to privacy has not been explored well enough. All facets of this issue need to be considered seriously, and I know your committee will do so. Happily, thanks to your work, Congress can ensure that we enjoy the many benefits of technology in the hands of government without suffering the sinister possibilities.