# PRIVACY IMPLICATIONS ARISING FROM INTELLIGENT VEHICLE-HIGHWAY SYSTEMS

Robert R. Belair
Alan F. Westin
John J. Mullenholz

December 8, 1993

This paper was prepared under FHWA Contract No. DTFH61-93-C-00087. The views expressed in this paper do not necessarily reflect the views of the U.S. Department of Transportation.

TABLE OF CONTENTS

# PRIVACY IMPLICATIONS ARISING FROM INTELLIGENT VEHICLE-HIGHWAY SYSTEMS

## I. EXECUTIVE SUMMARY

Intelligent Vehicle-Highway Systems, ("IVHS") involve electronic monitoring and sometimes identification of and communication with motor vehicles operating on public highways for the purpose of improving traffic safety, efficiency and convenience. IVHS applications hold enormous promise for the driving public and for society. IVHS applications, however, also raise numerous, significant privacy issues.

The extent to which IVHS applications raise privacy issues turn on *whether* an IVHS application will identify a specific vehicle or occupants in the vehicle; whether information generated by the IVHS applications will be databased -- i.e. will generate a record which is maintained in an information system; and whether IVHS applications and databases will be operated by government agencies (presumably state or local agencies) or by the private sector.

The paper briefly describes many of the potential IVHS applications and notes the important societal and personal benefits that are expected to result from IVHS implementation. The paper identifies the two generic privacy interests that certain IVHS applications may threaten: (1) an interest in avoiding or minimizing surveillance and a loss of anonymity and (2) an interest in controlling or participating in decisions about the *use* an individual's own personal information.

The paper looks at the policy issues potentially raised by certain IVHS applications from a surveillance privacy standpoint and also from an information privacy standpoint. The paper notes that those applications which identify specific vehicles and track the movement of those vehicles could have a chilling effect on individual behavior. Furthermore, IVHS "surveillance" could also have an adverse impact on individuals tangible interests, such as benefit claims, security clearance applications, license applications, etc. IVHS applications which identify and "track" the movement of automobiles can also have an adverse impact on the sense of anonymity that individuals frequently enjoy in motor vehicles.

The informational privacy interests implicated by IVHS applications raise questions about whether IVHS-generated personal information should be databased and, if so, what kinds of data quality, confidentiality and security protections should apply.

The paper also reviews public opinion surveys to look at public concerns about privacy, about computers and about government identification *cards.* The paper concludes that IVHS engendered concerns about anonymity\surveillance and about protecting information privacy will find a ready audience in the American public given the public's high level of privacy awareness. Nevertheless, the public may well accept and indeed even be enthusiastic about IVHS applications depending, in part, upon how the 57 percent of the public that is pragmatic about privacy weigh the social benefits of IVHS against the privacy threat posed by IVHS, taking into account the privacy safeguards incorporated in IVHS.

The paper also examines IVHS applications from a legal standpoint. The paper concludes that while the *Fourth* Amendment e.xtends limited protection to automobiles, IVHS applications, even if operated by a government agency, will not represent a search within the meaning of the Fourth Amendment. In this connection the paper notes that the courts have rejected the Fourth Amendment challenges to the electronic tracking of vehicles. The paper also concludes that the courts are unlikely to find that First Amendment or other constitutional rights are violated by any type of IVHS application.

The paper further concludes that IVHS applications would not violate federal statutes aimed at protecting against surveillance and intrusion. Chief among these statutes is Title III of the Omnibus Crime Control and Safe Streets Act as amended by the Electronics Communications Privacy Act. Title II? regulates the intentional interception of the contents of wire and other communications. The paper also concludes that state statutes aimed at protecting against surveillance and intrusion will not pose a barrier to the implementation of IVHS initiatives.

With respect to informational privacy legal issues, the paper concludes that even a non-voluntary IVHS data collection and information system program is likely to meet constitutional information privacy standards. The paper further concludes that federal and state information privacy statutes are-also not likely to be violated by IVHS applications. Common law claims are also discussed and are found to be largely inapplicable to IVHS applications. .

The paper identifies a number of strategies that could be used to safeguard privacy interests threatened by IVHS applications, assuage privacy advocacy group concerns and thereby facilitate IVHS implementation. These strategies fall into three categories: (1) research strategies, to include a public policy survey and state statutory research; (2) policy strategies, the centerpiece of which would be the adoption by the industry of a national, comprehensive IVHS privacy code; and (3) legal strategies to

include a model state law and, perhaps, complimentary federal statute law.

## II. BACKGROUND

### A. Description of IVHS

Intelligent Vehicle-Highway Systems is a diverse array of electronic, computer and communications technologies that involve the electronic monitoring, and sometimes identification of and communication with, motor vehicles for the purpose of improving traffic safety, efficiency and convenience.

Presently, more than 20 types of "intelligent" highway projects are being sponsored by state and local governments, among which are California, New York, and New Jersey. Even at this early stage of technical development, the possible uses of IVHS are broad. For example, vehicles could "communicate" -with each other to maintain a safe distance and keep traffic flowing. Anti-lock braking systems could be linked for safe stopping in case of danger, and vision-enhancing systems could improve visibility during poor weather conditions.

The expectations for IVHS can be summarized as follows:

- Reduced traffic congestion -- It is expected that an IVHS system will significantly reduce traffic congestion without building more and wider roadways.
- Safety -- The major benefit would be a reduction in vehicle collisions.
- Increased efficiency -- Considering national reliance on road transportation, from daily commuting to freight transport, increased traffic flow would increase productivity and reduce fuel consumption and vehicle emissions..

Among the expected applications of IVHS technology are:

- large-scale traffic management
- congestion warning
- weather information
- incident detection
- traffic speed management
- route guidance
- variable direction signs
- driver and traveller information
- electronic toll collection.

B. IVHS Applications That Raise Privacy Issues

The right of privacy is not expressly set forth in the Constitution. Rather, this right has been read into the Constitution in numerous court opinions. As articulated in these opinions, the right of privacy encompasses three relatively distinct but related interests:

- Autonomy -- An interest in being free to engage in certain intimate or private activities, free from governmental regulation.

- Intrusion -- An interest in being free from surveillance in situations in which an individual has a reasonable expectation of privacy. This interest encompasses the interest in preserving anonymity.

- Informational Privacy -- An interest in controlling, or at least participating in decisions about the collection quality, use and dissemination of personal information.?

A number of IVHS applications impact at least two of these three interests -- the interest in being free from surveillance and the informational privacy interest. IVHS applications that raise privacy issues share a common and central characteristic -- the IVHS operator's ability to identify a specific motor vehicle and/or driver. IVHS applications that cannot or do not specifically identify a vehicle or driver raise few, if any, privacy issues.

Advanced Traveler Information Systems ("ATIS") assist drivers of specific vehicles by providing them with information about optimal road, weather and traffic conditions. These systems

---

1 George B. Trubow. Privacy Law and Practice Ch. 19 "Constitutional Foundations of the Right to Privacy" (1991); and see; Griswold v. Connecticut, 381 U.S..479 (1965); Whalen v. Roe, 429 U.S. 600 (1977); and Katz v. United Sates, 389 U.S. 347 (1967).

2 It is possible to argue that at least one of the more advanced IVHS applications, Advanced Vehicle-Controlled Systems, which customarily includes intelligent cruise control and automatic braking units, strips an individual of autonomy with respect to the operation of a motor vehicle.The operation of a motor vehicle, however, is considered a privilege and in no event is considered analogous to the types of intimate private behaviors, such as those associated with procreation or marriage, that are protected by the autonomy branch of the right of privacy. Thus, a claim that a mandatory Advanced Vehicle Control System would violate the autonomy interest protected by the right of privacy is unlikely to be taken seriously.

require the identification of specific vehicles. Advanced Vehicle Control Systems ("AVCS") automate some or all driver functions and also require the specific identification of a vehicle and/or driver. Automatic Vehicle Identification Systems ("AVIS"), those used for automatic toll collection, also customarily require the identification of a vehicle. Electronic Vehicle Identification Number Systems ("EVIN") are also organized around the capacity to electronically identify vehicles for a variety of purposes including law enforcement purposes.

The capacity to identify a vehicle implicates interests protected by the right to privacy. Numerous other factors, however, are relevant in gauging how a particular IVHS application will impact upon privacy.

- Does the IVHS application generate a record and, if so, what exactly is the content of the IVHS record -- identification of the vehicle? geographic location of the vehicle? time of day? identification of occupants? speed of the vehicle? direction the vehicle is travelling? other information about the vehicle or information about the vehicle from other sources? information about the *driver* or occupants from other sources?

- Is the IVHS surveillance continuous or episodic?

- Does the surveillance involve cameras and a, "visual identification" or an electronic identification, such as in EVIN systems?

- Do the vehicle occupants have notice that the vehicle is or may be under surveillance?

- Can vehicle occupants "control" the surveillance -- by turning on or off an on-board IVHS unit, for example?

- What types of organizations operate the IVHS system?

- Is the information or the video record generated by the IVHS application retained, and, if so, in what type of an automated system; is information in the system accessible by name or other personal identifiers; and for how long is information retained?

- If IVHS-generated personal information is retained, is the information combined with other data -- such as biographic information or perhaps other driver record information?

- Who can see the IVHS record and for what purposes?

- Can the individual who is the subject of the IVHS record see and correct the record?

- Are IVHS records centralized so that individuals have *one* comprehensive IVHS "dossier"?

- What safeguards assure that IVHS records are accurate or complete?

This paper looks at the privacy interests raised by IVHS applications from both a policy and a legal standpoint. The paper assumes an IVHS environment in which vehicles are specifically identified and at least some information identifying specific vehicles is retained in automated databases.

Much of the analysis in the paper focuses on constitutional doctrine and statute law that governs the information practices of federal and state agencies. These bodies of law are most applicable if IVHS applications are operated by or at least under the supervision of government (and presumably state government) agencies. Federal constitutional privacy safeguards, and most state constitutional privacy,safeguards, for instance, are triggered only by state action. Moreover, many privacy statutes, for example the federal Privacy Act, address only, or at least primarily, governmental agency behavior.

This paper recognizes, however, that private organizations may operate various IVHS applications and may even maintain IVHS generated personal information databases. it is increasingly the case that it makes little difference from either a public policy or a legal standpoint, whether a privacy sensitive program is operated by a government agency or a private organization. Privacy expectations (and legal responsibilities) imposed by statute on private sector organizations operating privacy sensitive programs, such as the national credit reporting system, are similar to the privacy expectations and responsibilities placed on public agencies operating the national criminal record systems or holding other types of sensitive personal records. In both cases, the entities operating the information systems are subject to standards for the collection, maintenance and dissemination of personal data and must provide record subjects with rights of access and correction.

---

3 Rendell-Baker v. Kohn, 457 U.S. 830 (1982).

4 See, for example, "Presenting TravTek" , IEEE Journal (May, 1993) at 2.

5 See the Fair Credit Reporting Act, 15 U.S.C., § 1681, et seq.; and see, pending revisions to the FCRA in H.R. 1015 and S. 783.

Furthermore, of course, even assuming that various IVHS applications may be operated by private organizations, they may do so in concert with government agencies or under license or regulatory charter from a government agency and thus, under applicable legal principles, constitutional safeguards may be applicable.6 Moreover, constitutional privacy precepts increasingly are imported into tort and common law standards covering private behavior because the courts see these constitutional precepts as expressing the state's public policy. Thus, constitutional privacy principles are relevant to a private organization's operation of privacy sensitive programs.

## II. POLICY ANALYSIS OF PRIVACY ISSUES RAISED BY IVHS APPLICATIONS

### A. Introduction

Two stories -- one very recent and one over two decades old -- help to frame a policy analysis of privacy issues and IVHS applications.

In June, 1993, USA Today ran a front page story headlined "High Tech Can Cut Delays, But Privacy May Be The Price." The *story* began by describing pilot electronic toll collection systems in New Orleans, Atlanta, New York's Tappanzee bridge, and Chicago's Interstate 355, and reported the enthusiasm these tests had drawn frcm both officials and motorists interviewed. "This hot new technology promises to cut road congestion, ease tension, slash collection costs and even reduce pollution from idling cars."

But, "no breakthrough comes without *new* questions," the article added, and a major potential collision between "convenience and privacy" is surfacing to confront transportation officials and IVHS-industry projects. "Privacy advocates," the article said, look at the "itemized records" that electronic toll systems can generate and "see trouble." A spokesperson for Computer

---

6 The joint action doctrine and the public function doctrine may result in the application of constitutional safeguards to a private organization's operation of IVHS. See, Privacy Law and Practice (1991) Ch. 31.

7 See, Petermann v. International Brotherhood of Teamsters, 344p 2d 25 (Cal. Ct. App. (1959).

8 Lori Sham, Systems Let You Pay From the Fast Lane, USA Today, June 30, 1993, at Al.

Professionals for Social Responsibility was quoted as warning that "creating mountains of personal informaticn about where people drive" is a highly dangerous technology application.

Even though toll agencies pledge to keep records confidential, the article noted, "some fear 'Big Brother' has arrived when cars can be identified, tracked, and possibly ticketed automatically." Just how these privacy concerns would be addressed, and how the public would feel if such electronic toll systems were -widely installed, were presented in the story's windup as key issues for the future.

In the late 1960's, the federal government gave grants to a New York State criminal justice agency to test ALPS -- an Automatic License Plate Scanning project. A camera and electronic hookup installed at selected toll booths in New York would transmit photo-scanned license plate numbers to the computerized wanted person and stolen property file for the New York State Identification and Intelligence System (NYSIS). When a "hit" was made on a stolen vehicle or a wanted person, a message would be flashed electronically to State Police cars parked just ahead of the toll booth,which would then move in to apprehend the "violator." When the ALPS system was ready to go on line, a major demonstration was arranged for the state and national press, with reporters sitting in a large bus watching the toll booths. The system was turned on, and the reporters waited. After many uneventful minutes, a "hit" finally materialized. As the "violator's" sedan moved past the toll booths, two State Police cars converged on the "violator," and the driver was taken from the car, at gunpoint.

Unfortunately, the "violator" turned out to be a housewife, in bathrobe and curlers, driving to buy some breakfast food at a nearby supermarket. She had been listed as "wanted" in the NYSIS database because she had more than five unpaid traffic tickets. The next day, the front pages of New York City newspapers and national. wire service stories featured photos of the startled and dazed woman surrounded by State Police. "Housewife ALP'd," one headline put it. All the stories featured outraged quotes from the woman about high-tech'police projects arresting average citizens while rapists, murderers and car thieves flourished, The ACLU denounced the test as an example of "mindless technology applications." Not only was the publicity devastating for the NYSIS project and its federal sponsors but the woman went on to sue the State for invasion of privacy -- and received an out-of-court settlement. ALPS never got off the ground, in New York or elsewhere.

This cautionary tale from the 1960's, and the June, 1993 USA Today article, warn that how IVHS applications deal with privacy issues will have major implications for societal acceptance -- or non-acceptance -- of IVHS. With that in mind, we turn to an analysis of privacy as a concept; the balance among privacy,

protective surveillance and public disclosure; and a summary and analysis of current patterns of national public and group opinion about the privacy. standards and protections desired in the 90's.

## B. Privacy and Surveillance

Privacy includes the claim to be free from surveillance whether aural, visual or electronic in those circumstances where individuals have a reasonable expectation of privacy. Few hard and fast rules apply to when such a circumstance exists because both subjective and objective expectations are relevant. Customarily, however, individuals have a reasonable expectation of privacy and freedom from surveillance when in their own hones, when on the telephone and when in places where surveillance is both difficult and unusual.

### 1. Balancing Privacy and Surveillance

At the same time, democratic societies recognize the need to balance the privacy interest in freedom from surveillance against the need for limited surveillance, under carefully controlled conditions, to protect society from anti-social activity, crime, or revolutionary acts. This balancing process signifies that privacy claims or rights are not absolute and that a constitutional system supports reasonable rather than unreasonable expectations of privacy. However, in the American system, it is our historical tradition and current social priority that privacy rights must be given special emphasis and protections, because there will be continuing pressures from private organizations and governments for surveillance.

Perhaps foremost among privacy interests is the ability of individuals to move about in public areas (such as streets, parks, and highways) and to attend various types of public events (such as sports, parades, and public rallies) without fear that the government is systematically and continuously recording who was where, and when. These privacy expectations are not absolute, of course. High-crime rates on key dity streets can lead police to conduct {and society to accept) closed circuit TV' monitoring to deter crimes or identify criminals, and law enforcement officials who suspect specific individuals of engaging in crime can conduct surveillance of those suspects as they walk, drive, or engage in other movement through public places. In those circumstances, societal needs for limited and focused surveillance are deemed sufficient to justify law enforcement officials in overriding individual claims to anonymity-privacy. Similar situations can arise apart from the criminal law, as in location investigations by

---

9 Katz v. United States, 389 U.S. 347 (1967).

public health authorities tracing communicable or sexually-transmitted diseases.

2. The Chilling Effect of Surveillance

However, any activity that amounted to a capacity for the monitoring of the locations, movement, and activities of citizens using the public streets or parks --or driving on highways -- would threaten basic privacy interests in anonymity and freedom from surveillance. When George Orwell wrote his famous book, 1984, the two technological applications that defined "Big Brother" surveillance were: (I) the infamous telescreen that watched and heard individuals inside their apartments or homes; and (2) the Thought Police's ability to identify and monitor citizens as they went about in public places.

Orwell described this surveillance in chilling terms -- there was "no way of knowing whether you were being watched at any given moment . . . you had to live -- did live, from habit that became instinct in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

There is little question that electronic surveillance, or even the threat of this kind of surveillance, changes the way people feel and behave.

> Though this general principle of civil liberty is clear, many governmental and private authorities seem puzzled by the protest against current or proposed uses of new surveillance techniques. Why should persons who have not committed criminal acts worry whether their conversations might be accidentally overheard by police officers . . . The answer, of course, lies in the impact of surveillance on human behavior . . . .
>
> When a person knows his conduct is visible, he must either bring his conduct within the accented social norms in the particular situation involved or decide to violate those norms and accept the risk of reprisal.

---

10 George Orwell, 1984, at 6-7 (1949).

11 Erving Goffman, Behavior in Public Places 243 (1963).

12 Alan F. Westin, Privacy and Freedom 57-58 (1967). A study conducted in the early 1960's found, "when a person is being spied upon by direct or indirect means, he may quickly modify his conduct if he suspects he is being observed, even though he does not know the identity of the particular audience that might be observing him." Goffman, sum-a note 4, at 243.

Numerous studies and reports document that electronic monitoring of employees in workplace settings can lead to stress-related emotional disorders, increased absenteeism, decreased performance and even acts of sabotage.

Goffman and other sociologists note that individuals vary their behavior in surveillance settings for very subjective, psychological reasons. Particularly when a person is spied upon without being able. to contemporaneously watch his observer, (so-called asymmetrical observation) a process of serious behavior modification can result.

> In the asymmetrical case where a person is being spied upon by direct or indirect means, he may greatly modify his conduct if he suspects he is being observed even though he does not know the identity of the particular audience that might be observing him.

Simply stated, the knowledge or fear that one is under systematic, asymmetrical observation in public places destroys the sense of relaxation that individuals seek in open spaces and public arenas.

3. Surveillance Can Have Adverse Tangible Effects

Quite apart from the subjective reasons why individuals experience a sense of unease and often modify their behavior when in- surveillance settings, individuals have rational reasons for behaving differently when under surveillance. **A** primary set of concerns can be grouped under the label of governmental or police abuse. Where the government or private organizations collect information about the location or movement of individuals, such as may occur in certain IVHS applications, there is the possibility of governmental access to and abuse of this information for purposes unrelated to the formal or authorized purposes served by the surveillance. The government might use this information to track political dissidents; assist in law enforcement investigations; assist in investigating claims determinations with respect to health benefits or other types of benefit claims; or use the information in connection with applications for security clearances, licenses or other government-sponsored statuses.

---

I3 Electronic Monitoring of Employees: Issues and Guidelines, 44 J. Systems Mgmt. 17 (1993); and see also. The Case of the Omniscient Organization, Harv. Bus. Rev. March-April 1990 at 12.

I4 Goffman, supra note 4, at 16, n.4.

I5 Westin, supra note 5, at 31.

The point of this brief summary of the kinds of problems that can emerge when privacy/surveillanceinterests are infringed is not to suggest that implementation of IVHS applications will necessarily have these results. IVHS applications, even in their most ambitious configuration, would involve surveillance only in limited settings; only in settings that are already subject to regulation and surveillance; and, in most instances, only involve the vehicle and not its driver or occupants. Moreover, IVHS applications are unlikely to prompt the kind of reaction that photographic surveillance of automobiles and individuals has provoked (such as video camera surveillance of streets, subway stations and other public areas, or even photo radar for enforcement of speeding laws) because IVHS tracking is unlikely to be continuous or as threatening as photographic surveillance. This discussion of IVHS and privacy surveillance interests is important, however, because it illuminates the types of concerns *(and* the basis for these concerns) that privacy advocates and others are likely to voice upon introduction of even a limited program of electronic vehicle surveillance.

C. Informational Privacy

The second dimension of privacy that some IVHS applications could threaten involves the individual's interest in control over the collection and uses of transactional information, especially in *an age of* computerized data systems and on-line, electronic communications.
Information privacy is the claim of an individual to determine what information about himself or herself should be known to others. This also involves when such information should be communicated *or* obtained, and what uses of it will be made by others. in democratic societies, with basic commitments to individualism and freedom of association and the belief that the powers of government should be carefully limited, informational privacy increasingly is seen as a fundamental interest.

The essence of information privacy in a democracy requires that the government refrain from collecting and storing information that has a high and predictable potential to take away or limit the individual's control over his or her sensitive transactional information without overriding societal necessity. This is the heart of the "databanks" issue -- when should the government use data storage and communications technologies to accumulate

---

16 See, David S. Glater, "Technology Spots the Speeder" Urban Lawyer, 7:115,117(1976) "Whenever the specter of government photographic surveillance of citizen activities is raised, concern is promptly voiced over the loss of...privacy...." Citing Belair and Bock, "Poke use of Remote Camera Surveillance on Public Streets" Colum. Human Rights L. Rev. 4; 143 (1972).

sensitive information whose very presence in government files can lead to chilling effects on the First Amendment rights that privacy protects -- freedom of speech and press, freedom of assembly and association, and rights of dissent.

Even if not intended for that purpose, any institutional record system, public or private, that produces and stores personally-identifiable transactional information about large segments of the population raises serious privacy issues. Will the system allow managers of the system and others able to obtain access to it to engage in extensive reconstruction of the locations and movements of masses of the general population (and various elites within the population)? If so, information privacy protection requires probing a series of key questions: is there a necessary or highly-valuable social purpose to be served by the creation of a privacy-sensitive transactional-data collection? Are there other ways to accomplishthe purpose that do not collect personally-identifiable data? If the data are needed, can they be used for immediate operations but not put into long-term storage, and become attractive targets for more intrusive uses, or direct misuses? If a stored-data system is necessary, what kinds of safequards can and will be installed to assure protection of fundamental privacy and due process rights?

IVHS applications could well generate sensitive records. It is certainly conceivable that an IVHS database could include biographic information about a vehicle owner; a record of the location of the owner's vehicle at various dates and times; information about how the vehicle was operated; and adverse information about traffic or law enforcement violations. Information from this type of database has the potential to embarrass individuals ( a vehicle may be at the wrong place at the wrong time); or to adversely affect an individual's access to benefits or statuses.

Having noted the two central privacy issues that will be raised by some kinds of IVHS applications, we turn to a review of national opinion surveys over the past two decades, to shed important light on how the public is likely to..react to such applications and what the public will expect to be done to limit potential privacy abuses.

### D. National Opinion Privacy Surveys

Between 1978 and the present, Louis Rarris and Associates and Dr. Alan F. Westin have collaborated on a series of well-regarded national public and leadership surveys that have steadily examined a wide range of privacy issues, and in great depth. (The 1978 survey was sponsored by Sentry Insurance, and the remaining surveys quoted here were sponsored by Equifax Inc.) Several sets of findings from these surveys are relevant to IVHS applications, and can be summarized as follows:

## 1. Overall Privacy Concerns

- 83 percent of Americans say in 1993 that they are concerned "about threats to their personal privacy in America today." This has climbed steadily upward (in answer to an identical question) from 49 percent in 1977 to 64 percent in 1979, 77 percent in 1983, and 79 percent in 1990. And, in 1993, 53 percent of the public says they are very concerned about such privacy threats.

- 80 percent of the public in 1993 agrees that "consumers have lost all control over how personal information about them is circulated and used by companies."

- 58 percent do not agree in 1993 that their privacy rights "are adequately protected today by laws and organizational practices."

- When asked in 1992 how they believe privacy of information about consumers will be protected in the year 2,000 55 percent said they believe it will get worse, 32 percent said it would probably remain the same, and only 12 percent said they thought privacy protection would get better.

## 2. Concerns About Computers

- 50 percent of the public now believe that "technology has almost gotten out of control'* in the U.S. today.

- While 79 percent in 1992 said that "computers have improved the quality of life in our society" and 78 percent say computers are making it possible to provide "more customized services" to people, 66 percent feel that, in general, privacy of personal information in computers is not adequately safeguarded, and 89 percent feel that "computers have made it much easier for someone to improperly obtain confidential personal information about individuals."

- Fully two thirds of the public -- 67 percent -- believe that "if privacy is to be preserved, the use of computers must be sharply restricted in the future."

### 3. Concerns About Government Cards and Numbers

- in 1978, 57 percent of the public opposed the creation of a *government* national identity card, even thought it would *make* it easier to locate suspected criminals and illegal aliens.

- In 1990, 56 percent of the public opposed the issuance of a national work identity card, worrying more about threats to privacy than supporting the detection of illegal workers.

- And, in 1993, 57 percent said they would be concerned if each person was assigned a national health insurance number to help administer the proposed national health care system.

### 4. The Sources of the Public's Privacy Views

Analysis of the Harris privacy surveys from 1978 to the present shows that the underlying causes of these public concerns are two continuing trends of the past two decades -- (1) high distrust of government and other institutions of American society, and our political processes; *and* (2) generalized fears about misuse of computers and other technologies. These orientations are more powerful than any standard demographics, such as income, education, occupation, age, political philosophy, sex, *or* race, in explaining and differentiating attitudes toward privacy as a general value or toward the majority of specific privacy issues.

- In 1993, a remarkable 75 percent of the American public registered high or medium distrust of government and voting, and concern over controlling technology. This has risen steadily from 49 percent registering such levels of distrust in 1979 and 55 percent in 1990.

- With such a rise over the past three years, there is little likelihood that the high concern about privacy threats -- by four out of five Americans -- will recede any time soon. Thus a "normal baseline'* of public distrust and privacy concern must be assumed when any new technology applications by government or business involving the collection and use of personal information are contemplated in the mid to late '90's.

## 5. The Public Remains Pragmatic Rather Than Absolutist on Privacy Issues

Despite the strong concerns just summarized, the answers to literally hundreds of Harris survey questions on specific matters of consumer, employee, and citizen privacy over the past 15 years show that the public weighs the social needs for disclosure or surveillance against the privacy interest on a cost-by-cost basis. Where those needs are considered important -- and when the public sees what it considers to be appropriate safeguards and protections present -- then strong majorities of the public will accept the collection of personal information and the operations of data systems by government or industry. This "privacy dynamic" produces a basic division of the American public into three continuing groupings:

- About 2.5 percent of the public are "Privacy Fundamentalists". They are very worried about losses of their privacy and what they see as improper commercial and governmental demands for their data; they seek strong legal rules to forbid such data collection and use.

- At the opposite pole, at 18 percent, are the "Privacy Unconcerned". These are people who give their personal information gladly to get commercial opportunities and benefits, support broad law enforcement access to personal data, and simply do not see privacy as a real issue.

- Between these two camps are the 57 percent of Americans who consistently score on surveys as "Privacy Pragmatists". They care about privacy, but they also want access to consumer benefits, believe businesses have a right to get information when they are asked to grant credit, insurance, or employment, and see public records . disclosure and reasonable law enforcement surveillance as social interests also to be met. Basically, when the Privacy Pragmatists believe a valuable social purpose is being served and when relevant fair information practices have been applied and are being enforced, the Pragmatists will support such information uses, and provide a solid public majority for such activity. When the Privacy Pragmatists do not believe that information is being sought for a valid social purpose or when fair information practices are not being followed, they will see privacy as threatened and can be mobilized to oppose such actions.

### 6. Implications of the Survey Findings for IVHS

The survey findings strongly suggest that the kinds of warnings about potential violations of anonymity/surveillance privacy interests and informational interests noted earlier in this paper will find a ready audience in the media, among consumer and privacy advocacy groups, and among many stare and federal legislators. There are sure to be alarms of just the kind voiced in the 1960's ALPS pilot project and in the 1993 USA Today article. How public opinion shapes up in response to these alarms will depend on how the 57 percent of the Pragmatic Public views the social justifications for particular IVHS applications, the extent and sincerity of efforts to hold the collection of identified transactional data to the minimum required for those programs, the quality of the safeguards and protections built into IVHS applications, and the credibility of those managing these applications.

## IV. LEGAL ANALYSIS OF PRIVACY ISSUES RAISED BY IVHS APPLICATIONS

This part of the paper analyzes the constitutional, statutory and common law privacy guestions raised by IVHS applications from both a surveillance privacy standpoint and an informational privacy standpoint.

Our legal analysis focuses on constitutional issues and federal statutory issues because, even assuming that private sector and state agency conduct would be the focal point for any IVHS legal challenge (rather than federal agency conduct), constitutional issues remain relevant because, as noted earlier, constitutional protections may regulate or, at a minimum, influence private organizational conduct and, without question, will attach to state conduct. Furthermore, an analysis of federal statutes regulating the handling of personal information is relevant not only in looking at federal conduct, but because federal statutes have provided a model for legislation regulating the information practices of state agencies and private organizations.

### A. Legal Analysis of IVHS and Surveillance/Privacy Issues

#### 1. The Fourth Amendment and Motor Vehicles

The constitutional basis for a claim to be free from government surveillance emanates principally from the Fourth Amendment. The Fourth Amendment, of course, protects individuals

from unreasonable searches and seizures, including, in some cases, electronic, aural, visual and other types of surveillance.

The identification and even the surveillance of a vehicle travelling on public streets is not considered a search within the meaning of the Fourth Amendment. If, however, an IVHS application captures information from a vehicle, without consent, questions will be raised inevitably as to whether the capture violates at least the spirit of the Fourth Amendment. For this reason, and because so much of privacy law emanates from the Fourth Amendment,it is important to review Fourth Amendment law.

Following the American Revolution, and as a reaction to the unfettered searches authorized by the dreaded writs of assistance in the Colonial period, nearly every state enacted a law prohibiting arbitrary search and seizure. In 1791, protection against arbitrary search and seizure was embodied in the Bill of Rights.

Fourth Amendment protections today require governmental authorities to obtain a valid judicial warrant, specifying the persons, places and property to be searched and/or seized, prior to the execution of a search. Supreme Court decisions have added a further protection by prohibiting any evidence obtained by federal *or stats* officials in violation of the Fourth Amendment from being used during criminal trials.

---

17 See, Duncan v. Louisiana, 391 U.S. 145 (1968). Nearly all of the guarantees found within the Bill of Rights have been incorporated into the Fourteenth Amendment making them applicable to the states.

18 United States v. Knotts, 460 U. S. 276, 281 (1983). In Knotts, the Supreme Court held that, "[A] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another". The Court explained that there is a diminished expectation of privacy in an automobile: "One has a Iesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view . Cardwell v. Lewis, 417 U. S. 583 (1974).

19 Theoretically, at least, it is possible that an IVHS application could constitute a search if the application did more than identify the vehicle in that it also identified the occupants or otherwise captured the contents of the vehicle and the occupants of the vehicle had taken extraordinary steps to shield the contents from plain view. See, Pruitt v. State, 389 S.W. 2d 475 (Tex. Crim. App. 1965); and see, Kirby v.Superior Court, 8 Cal. App. 3rd 591 (Ct. App. 170); C.F., Texas v. Brown, 460 U.S. 730 (1982). As a practical matter, however, the chance that an IVHS application could be considered a search is extraordinarily remote.

While not as sacred as the home, the automobile has become very much a part of day-to-day living in the United States. The Supreme Court recognized the importance of the automobile when it stated that automobile travel is a basic and often necessary mode of transportation, and that many people, "find a greater sense of security and privacy in traveling in an automobile than they do in exposing themselves by other modes of travel." Based on this view of automobile travel, the Court has held that, although an automobile is subject to extensive governmental regulation, and although an automobile travels in plain view a person does possess a legitimate albeit modest expectation of privacy in an automobile. The Fourth Amendment is to safeguard individuals from unreasonable governmental invasions of all legitimate privacy interests, and not merely those-interests found inside the four walls of the home.

Although automobiles are protected from . unreasonable governmental intrusion, the Supreme Court has long recognized a distinction between the warrantless search and seizure of automobiles or other movable vehicles, on the one hand, and the search of a home or office, on the other. The Court has held that vehicles may be searched without a warrant in circumstances that would not justify a warrantless search of a house or office, provided that there is probable cause to believe the vehicle contains articles that police officers are entitled to seize. Moreover, although warrantless searches are qenerally presumptively unreasonable, there is no such presumption that attaches to warrancless searches of an automobile.

Several rationales underlie the less stringent warrant requirements that have been applied to searches of vehicles. First, as the Supreme Court repeatedly has recognized, the inherent mobility of vehicles often creates exigent circumstances that make obtaining a warrant impractical. Second, the configuration and use of vehicles diminish the reasonable expectation of privacy that

---

[20] Delaware v. Prouse, 440 U.S. 648, 662 (1979).

[21] Id. at 662 (police stops solely designed to check driver's license and registration held unreasonable and violative of Fourth Amendment).

[22] United States v. Chadwick, 433 U.S. 1, 7 (1977).

[23] Chambers v. Maroney, 399 U.S 42, 48 (1970); and see Arkansas v. Sanders, 442 U.S. 753, 760 (1979).

[24] United States v. Ross, 456 U.S. 798, 808-09 (1982).

[25] Carroll v. United States, 267 U.S. 132, 153-54 (1925); Chambers, 399 U.S. at 50-51.

exists with respect to differently situated proaerty. People have a lesser expectation of privacy in a motor vehicle because its function is transportation and it serves less frequently than a home does **as** the repository of personal effects. A car has little capacity for escaping public scrutiny; it travels public highways where some of its contents and its occupants are in plain view. As a result, the search of an automobile is far iess intrusive on the rights protected by the Fourth Amendment than is the search of one's home or office.

The expectaticn of privacy as to automobiles is further diminished by the fact that automobiles, unlike homes, are subject to pervasive and continuing governmental regulation and controls, including periodic inspection and licensing requirements. As an everyday occurrence, police stop and examine vehicles when license plates or inspection *stickers* have expired, when violations such as exhaust fumes or excessive noise are noticed, when headlights or other safety equipment are not functioning properly or when police observe erratic driving behavior.[29] These normal police activities bring law enforcement officials into frequent contact with automobiles, and as a result, people should not reasonably expect the same degree of privacy in their automobiles as they do in their homes.

Based on the fact that vehicles are subject to extensive regulation, the Supreme Court has held that a warrantiess but limited intrusion into a vehicle is permissible without probable cause under the Fourth Amendment when important: governmental interests are at stake. Police officers, for example, may enter the interior of a vehicle during a traffic stop in order to search for a vehicle identification number (VIN) without articulating any reasonable justification for the intrusion other than the observed traffic violation. The Court reasoned that because of the important role played by the VIN in the pervasive governmental regulation of automobiles and the efforts by the federal government

---

26 Sanders, 442 U.S. at 761.

27 Cardwell v. Lewis, 417 U.S. 583, 590 (1974).

28 South Dakota v. Opperman, 428 U.S. 364, 368 (1976); and see Cadv v. Dombrowski, 413 U.S. 433, 439 (1973).

19 Opperman, 428 U.S. at 368.

3o New York v. Class, 475 U.S. 106, 116-19 (1989.

through regulations to assure "that the VIN is placed in plain view, there is no reasonable expectation of privacy in the VIN.

To summarize, a citizen does not surrender all of the protection of the Fourth Amendment by entering an automobile. Traditionally, however, a distinction has been drawn between automobiles and homes in relation to the Fourth Amendment. Although automobiles are "effects" and are therefore within the *reach* of the Fourth Amendment, warrantless searches of automobiles are upheld in circumstances in which a warrantless search of a home would not be tolerated for two basic reasons: first, the impracticality of obtaining a search warrant; second, a lessened expectation of privacy because automobiles operate on public streets in plain view of passersby, and because automobiles are the subject of pervasive regulation by the government.

Apart from the general attitude of the courts to the search of vehicles, some specific issues dealing with *new* scientific or technological developments affecting autos and highways may provide guidance as to the approach which will be taken toward IVHS.

### a. Electronic Tracking Devices

Although the Supreme Court has determined that automobiles have at least some protection under the Constitution, new technology resulting in advanced surveillance techniques has created problems in the interpretation of the Fourth Amendment's prohibition against unreasonable searches and seizures. Law enforcement officials are now using small transmitting devices *known* as "beepers" as an aid to physical surveillance, particularly of objects or persons in moving vehicles. Electronic tracking through the use of signalling devices, or "beepers," allows police officers to trail vehicles at a sufficiently great distance to avoid detection, and enables police to relocate a lost suspect. At the same time, however, the use of beepers has the potential to intrude upon an individual's privacy expectations since the transmitter is placed on, or in, the individual's property -- the automobile -- by a law enforcement official.

Determining whether electronic tracking complies with the Fourth Amendment depends on whether this surveillance invades a

---

31 *Id.* at 114.

32 *See,* Note, Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights, 71 Va. L. Rev. 297, 297-93 (1985).

person's reasonable expectation of privacy. Most courts applying this standard have used a two-step analysis to distinguish between beeper installation and the subseguent monitoring of the device. First, in order to protect the expectation that one's possessions will be secure, courts will determine whether the attachment of the beeper to a vehicle required a prior warrant. Second, courts will determine whether monitoring the beeper's signals and ascertaining its location without a warrant violates one's expectation that certain information will remain secret.

As to the attachment of a beeper to a vehicle, the Supreme Court has held that installation of an electronic tracking device does not constitute a Fourth Amendment search where police obtained the consent or a vehicle owner, but not the driver, to install the device. In cases where there is no third party consent to the installation of the beeper, the courts focus on the circumstances surrounding the installation to determine if a warrant is required. Most courts hold that attaching a beeper to the exterior of a vehicle does not constitute a search and that therefore no warrant is required, unless private premises must be entered to get to the vehicle, or the police disregard some other reasonable expectation of privacy. Where, however, a beeper is placed inside a vehicle, it is usually held that a search occurs upon entry into the vehicle.

As to the monitoring of beeper signals, the Supreme Court has held that the monitoring of beeper signals in areas open to visual surveillance is not a search or seizure subject to Fourth Amendment proscriptions because it does not infringe on a legitimate

---

33 Katz v. United States, 389 U.S.347,353 (1967);Smith v. Maryland, 442 U.S.735,740 (1979).

34 United States v. Karo, 468 U.S. 705, 713 (1984).

35 See,Note, supra note 23, at 300.

36 Karo, 468 U.S. at 711.

37 United States v. Michael, 645 F.2d 252, 256-57 (5ch Cir. 1981)(en ban@; United States v. Preminger, 542 F.2d 517, 520 (9th Cir. 1977).

38 United States v. Rowland, 448 F.Supp 22, 24 (N-D. Tex. 1977)(defendant had some reasonable expectation of privacy by placing his plane inside a locked hangar).

39 United States v. Gofer, 444 F.&p?. 146, 149 (W.D. Tex. 1978); Johnson v. State, 492 So. 2d 693, 694 (Fia. Dist. Ct. App. 1986).

expectation of privacy. The Court reasoned that persons travelling in automobiles on public highways have no reasonable expectation of privacy in movements from one place to another. The fact that a beeper augments the police ability to monitor movements is irrelevant as long as the same results could have been achieved by unaided visual surveillance. However, at least one state court (Oregon) has disagreed with the Supreme Court and has held that police use of a beeper to locate a suspect's automobile constituted a search under *the* state's constitution.

In cases analogous to the installation of beepers in automobiles, several courts have found a diminished expectation of privacy in the movements of aircraft through public airspace. These courts found that monitoring beepers installed on aircraft did not violate the Fourth Amendment because the beepers did nothing more than enhance the legal right to observe the aircraft's public movement and did not result in the discovery of private information.

To summarize, some forms of electronic surveillance do not implicate the Fourth Amendment. The monitoring of beeper signals in areas open to visual surveillance ("plain view") is not a search or seizure because it does not infringe on a legitimate expectation of privacy. Similarly the initial installation of a beeper onto (but not into) an object does not constitute a search or seizure within the meaning of the Fourth Amendment.

b. Photo-Badar

Another recent innovation which is closely related to IVHS is "photo radar." Photographic radar enforcement-involves the use of a radar detection device combined with photographic equipment in order to detect and immediately document speeding drivers. When a vehicle exceeding the preset speed limit encounters a radar beam, a camera automatically photographs the license plate and driver of the vehicle, and records the speed, time, date, and location on the photograph. Registered owners are identified from their license plates and are mailed summonses. Signs are posted-along the roads to alert drivers that an area is patrolled by photo-radar. Photo-radar is currently being used in cities in Utah, Arizona, and 'California and is being considered in thirty more cities, while

---

40 United States v. Knotts, 460 U.S. 276, 285 (1983).

41 State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988).

42 See, United States v. Butts, 729 F.2d 1514, 1517 (5th Cir. 1984); United States v. Alonso, 790 F.2d 1489, 1494 (10th Cir. 1986); United States v. Cotton, 770 F.2d 940, 947 (11th Cir. 1985).

similar systems have been operating in Europe for the past twenty years.

Proponents of photo-radar claim that its purpose is to promote traffic safety through deterrence. The theory is that drivers will reduce their speed because of the threat posed by photo-radar and therefore the number of accidents will be reduced, saving lives and decreasing property damage. There is already some evidence that the use of photo-radar may, in fact, help to reduce the number of auto accidents. In Paradise Valley, Arizona, for example, the number of auto accidents has declined by more than fifty percent (from 460 to 224) in the six years since the introduction of photo-radar. By reducing the number and severity of auto accidents, photo-radar may also have the indirect effect of reducing the cost of auto insurance.

Photo-radar raises privacy issues similar to those raised by IVHS applications. Photo-radar is also thought to "depersonalize" law enforcement because drivers will no longer be able to present their extenuating circumstances to a ticketing officer.

Public reaction to photo-radar has been mixed. A survey of 5000 Wisconsin motorists, for example, found that 84 percent of the respondents were opposed to the use of photo-radar. In addition, the American Automobile Association has stated that its members are overwhelmingly opposed to photo-radar. The State of New Jersey has recently enacted legislation banning the use of photo-radar. On the other hand, public response to a photo-radar experiment in Spokane, Washington was favorable. In a survey, 71 percent of the respondents thought photo-radar was an effective deterrent'aqainst speeding, and 82 percent stated that they would be more conscious of speed limits in the future.

### c. Fourth Amendment Summary

To summarize this paper's Fourth Amendment analysis, it is difficult to imagine a situation where an IVHS application would violate Fourth Amendment rights. Presumably, individuals would know about and implicitly or explicitly consent to the use of on-board IVHS devices. Even without explicit or implicit consent, IVHS operators positioned in a place where they are entitled to be 'could use available technology (in this case IVHS technology] to identify and track vehicles (or their occupants) operating on the public streets without implicating Fourth Amendment protections.

Of course unless a judicial challenge to IVHS arose in the context of a criminal investigation, the question of whether an electronic or video IVHS identification constituted a search for Fourth Amendment- purposes would not even arise. A more likely circumstance would involve a generalized claim that an IVHS surveillance system, whether operated by a government agency or a

private organization, violated constitutional rights of privacy, citing Fourth Amendment concepts of a reasonable expectation of freedom from surveillance. Depending upon whether the IVHS threat was deemed to implicate a funaamental right or merely a right, a government IVHS operator would have to establish that the IVHS program served either a compelling state interest or merely had a rational relationship to a legitimate governmental purpose. The likelihood is that a court would find either that an IVHS surveillance program did not infringe any right or would find that while a right was implicated, the governmental purposes served by IVHS meet the rational basis test.

A private sector IVHS operator could conceivably by challenged on common law tort theories including intrusion, and the complainant would presumably cite Fourth Amendment doctrine as establishing that the IVHS application implicates legitimate privacy interests and violates the state's public policy. The chance that this type of claim could be successful are remote.

2. Other Constitutional Issues Raised by IVHS Surveillance

While a judicial challenge to the constitutionality of an IVHS surveillance system would be likely to center on the Fourth Amendment, it would also be likely to -include other constitutional arguments. Those arguments are even less likely to be successful than a Fourth Amendment argument and they merit only 'cursory mention.

The First Amendment, among other things, protects the riqhts of the free speech and association. A First Amendment challenge to IVHS surveillance presumably would arque that the specter of systematic surveillance, particularly governmental surveillance, of the roads and the tracking of vehicles would deter individuals from attending socially or politically controversial or unpopular events; associating with unpopular or controversial individuals or groups; and generally chill the ability to enqaqe'in dissident or unpopular speech.

This argument seems certain to be unsuccessful, however, because IVHS surveillance presents only an incremental increase in existing surveillance and probably cannot be shown to have a significant chilling effect. Even if IVHS surveillance could be shown to have an incidental chilling effect (and this is surely the most that could be shown) the Supreme Court has long established that governmental programs or statutes that indirectly and

43 See, United States v. Mara, 410 U.S. 19 (1973)

adversely effect First Amendment rights are tolerable so long as the effect on speech is minor and the underlying governmental purpose is legitimate.

Indeed, the Supreme Court has upheld surveillance, including photographic surveillance by Army investigators, of vehicles and individuals present at lawful but dissident political events. In Tatum v. Laird, the Supreme Court rejected allegations of a subjective "chill" finding that this harm fell short of the objective, actual harm necessary to make out a First Amendment claim.

Both the Fifth Amendment's protections against self incrimination and the Sixth Amendment's protections for counsel and confrontation present no obstacles to deployment or operation of an IVHS surveillance system, but might present problems in certain limited circumstances with respect to the use of IVHS generated data as evidence in criminal prosecutions. Other constitutional privacy theories, such as the Ninth Amendment's reservation of rights to the people, are also not likely to be found applicable to IVHS initiatives.

### 3. Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act ( "ECPA") amended Title III of the Omnibus Crime Control and Safe Streets Act'of 1968 (Title III) for the purpose of accommodating federal wiretap law to new technologies. Title III regulates and greatly restricts the interception of the contents of wire, oral, and electronic communications by requiring that law enforcement officials obtain a warrant and follow certain procedures both before and after initiating electronic surveillance. Although stat2 laws may not allow interceptions under less stringent requirements than those

---

44 Younger v. Harris,'401 U.S. 37, 51 (1971)

45 408 U.S. 1, 13-16 (1972).

46 Belair & Bock, Remote Camera Surveillance of Public Streets, Colum Hum. Rights v. Rev 4; 193-194 (1972).

47 See Griswald v. Connecticut, 381 U.S. 479, 484 (1965).

58 18 U.S.C. §§ 2510-2521(1988).

imposed by Title III, a state may place stricter limitations on electronic surveillance.

Title III, however, did not address the intentional interception of certain openly transmitted radio communications such as cellular mobile telephones paging systams and other over-the-air transmissions. The ECPA extends Title III protections to these kinds of transmissions.

Even as amended by the ECPA, Title III, regulates only the interception of the contents of a communication. Most IVHS applications would not capture the contents of a communication but would, at most, identifv a vehicle. Moreover, Title III, as amendkd by the ECPA, explicitly excludes mobile tracking devices from coverage. The Act defines a mobile tracking device as "an electronic or mechanical device which permits the tracking of the movement'of a person or object. The definition of a mobile tracking device has not been interpreted by the courts. Nevertheless there is nothing in the legislative history to indicate that the Congress intended to limit mobile packing devices to those that track only in a continuous fashion.

Accordingly, an IVHS application which includes some kind of on-board device that permits an IVHS operator to identify a vehicle episodically as it moves on the streets is likely to be viewed for Title III purposes as a mobile tracking device and thus come within the exception for tracking devices. Title III's content requirement, as well as the existence cf this exception, together with the consensual elements of IVHS, make it extremely unlikely that a court Would apply Title III/ECPA protections to IVHS transmissions.

A few courts have considered the question of whether the use of video surveillance cameras is encompassed by Title III. These courts have held that Title III does not cover the use of Video cameras which record only images and not aural communications." Thus, IVHS photo and video applications do not come within the scope of Title III and, to the extent that they present legal issues, do so only in a constitutional context.

---

49 United States v. Mora, 821 F.2d 860, 863 (1st Cir. 1987).

50 18 U.S. C. § 2510 (12) (D).

51 18 U.S.C. § 3117(b) (1993).

52 See 1986 U.S. Code Cong. and Adm. News at 3555.

53 United States v. Taketa, 923 F.2d 665, 675 (9th Cir. 1991); United States v. Biasucci; 786 F.2d 504, 508, (2nd Cir. 1986).

4. State Surveillance/Privacy Statutes

A majority of states have enacted legislation regulating electronic surveillance of voice communications, whether face-to-face or using communication devices (such as telephones, radios, etc.). Most of these statutes are similar to Title III. Some states have also amended their surveillance laws to comport with the ECPA amendments to Title III. The legislative history of Title III clearly indicates that Congress intended to permit state electronic surveillance laws to be more restrictive than the federal provisions, and therefore more protective of individual privacy. As a result, several states have adopted statutory procedures regulating applications and orders for mobile tracking devices, even though such devices are expressly exempted from Title III coverage. In addition, one state, New Jersey, has banned the use of photo-radar Thus, in considering whether statutory law will have an impact on IVHS applications, state laws that may be more protective of surveillance/privacy interests must also be taken into account.

5. Common Law Claims

Most states recognize a common law privacy claim for "intrusion" An IVHS operator, wherher public or private, could have liability if it could be shown that there was damage arising from a prying *or* harassment or other interference with a private area *or* activity. The courts have made clear, however, that it is not an invasion of privacy to watch or even photograph an individual on the public streets. Accordingly, it is extremely unlikely that IVHS applications would prompt intrusion type privacy claims.

---

54 S. Rep. No. 1097 at 2187.

55 See, Fla. Stat. Ann. §934.42 (West Supp. 1993); Haw. Rev. Stat. Ann. § 803-44.7 (Supp. 1992); Minn. Stat. Ann. §§ 6A.35-626A.39 (West Supp. 1993); Tex. Code Crim. Pro. Ann. art. 18.21 (West Supp. 1993).

56 NJ. Stat. Ann. § 39:4-103.1 (West Supp. 1993).

57 See William L. Prosser, Law of Torts, West Publishing (1971) at 808.

58 See,,Pinkerton Nat.Detective Aaency v. Stevens, 132 S.E. Id 119 (Ga. 1963), and cases cited in Prosser at 808-809.

## B. Legal Analysis of IVHS *and* Informational Privacy Issues

### 1. Introduction

IVHS applications, as noted earlier, hold the potential for generating personal information. The configuration of the personal information generated by IVHS may vary substantially, however, depending upon which IVHS applications are implemented and the decisions that are made with respect to whether personal data will be retained, what personal data will be retained and how the data is organized or "databased".

Depending upon the context, IVHS generated personal information may be quite sensitive. Indeed, in the most ambitious and mature configuration, IVHS applications have the potential to generate data that identifies an individual and builds *a* record of that individual's day-to-day and even hour-to-hour vehicular travels. This kind of a tracking capacity and database would be extraordinarily privacy sensitive, given its potential to chill political activity and generate information that bears on a host of decisions that affect an individual's entitlement to rights and benefits.

For purposes of our legal analysis, this paper assumes that at some point in the implementation of IVHS applications information will be generated that specifically identifies an individual (either as an occupant or, far more likely, as an owner of a vehicle) and that this information will be ratained in an automated format that permits the information to be retrieved on the basis of the individual's name or some other type of personal identifier.

### 2. Constitutional Law and Informational Privacy

Although the Supreme Court has indicated that the constitutional right of privacy includes informational privacy, this right, by any measure, is under developed. As a result, constitutionally-based informational privacy rights should pose little, if any, obstacle to the collection, retention, use and/or dissemination of personal information arising from IVHS applications.

The leading constitutional informational privacy decision is Whalen v. Roe. In Whalen, the Court looked at a New York State statute requiring physicians to report to a state agency the names of patients receiving certain types of controlled, prescription drugs. The Court found that individuals do have a constitutionally based interest in how the government handles and particularly disseminates their personal information. The Court also found,

---

[59] 429 U.S. 600 (1977).

however, that the government's mere collection of personal information for an internal and legitimate governmental purpose, when done under privacy and confidentiality protections, does not violate constitutional privacy interests. The Court suggested, but did not find, that if the statute lacked these protections, the statute might have violated constitutional privacy protections.

In United States v. Westinghouse Elec. Corp., the Third Circuit identified specific criteria *to* be used in gauging whether a governmental program for the collection of personal information runs afoul of constitutional, information privacy principles. Specifically, the court identified six factors which should be weighed in determining whether to permit a government agency to collect personal information: (1) the subject matter of the information; (2) the potential for harm in any subsequent non-consensual disclosure; (3) the damage to the relationship in which the record was generated; (4) the adequacy of safeguards to prevent unauthorized disclosure; (5) the degree of the government's need for the information; and (6) whether there is an express statutory mandate, an articulated public policy, or some other kind of recognizable public interest that tilts toward the establishment of the collection program. Depending upon the application of these factors to the program in question, the court would determine whether privacy riahts are implicated. If so, the program could still pass constitutional muster if the government could demonstrate that the program served a counselling state interest (if the program infringed a fundamental right) or met a rational basis test (if the program merely infringed. a right}.

Even under the Whalen and Westinghouse standards,. a non-voluntary/mandatory IVHS- generated data collection program would be likely to meet constitutional standards, given that the government should be able to articulate a legitimate public purpose for the collection of the IVHS information and assuming that the government could establish that it would handle the information in accordance with reasonable privacy safeguards.

---

[60] 638 F.2d 570 (3d Cir. 1980).

[61] One possible exception to this conclusion would arise if it could be shown that IVHS applications were being used in more than an incidental way to keep track of and collect information about political activity and the exercise of First Amendment rights. In this context, it is likely that the court would strike down the IVHS application on grounds that it places in impermissible burden upon First Amendment rights. NAACP v. Alabama, 357 U.S. 449 (1958); and see also, Murdock, The Use and Abuse of computerized Information: Striking a Balance Between Personal

It is important to emphasize, however, that the 'Whalen and Westinghouse standards are unlikely to apply given the consensual aspects of an IVHS program. Courts may find that individuals expressly consent to participating in IVHS programs -- (either by purchasing an on-board IVHS unit or by activating the unit); or courts may find that individuals constructively consent to participating in IVHS programs by choosing to operate vehicles on IVHS capable roadways, *or* indeed choosing to operate vehicles at all, knowing that the vehicle would be travelling over at least some roadways that are IVHS capable. If the courts conclude that there is a consensual aspect to the IVHS program, courts would be likely to find that individuals waive their privacy interest in any data generated by the IVHS application. The Supreme Court has held that once an individual "chooses" to provide information to an organization, including a governmental organization, the individual assumes the risk that the organization will convey the information to others and thereby the individual "waives" most if not all of the individual's privacy interest in the information.

Thus, it is unlikely that constitutional information privacy principles will have a significant impact upon the collection, retention, use or even dissemination of personal data from IVHS applications, provided that those applications and information systems are operated subject to privacy and confidentially protections.

3. Federal Information Statutes

Existing federal information privacy statutes will be relevant to the collection, retention, use or dissemination of IVHS generated personal data, not necessarily because federal agencies will maintain IVHS-generated personal data, but because these *statutes* provide a model for statutes that govern the handling of personal information by state agencies and the private sector.

It has long been established that the federal government has authority to collect and retain personal data that serves legitimate governmental interests. The Privacy Act of 1974 creates a comprehensive statutory scheme for the federal government's collection, retention, use and dissemination of personal data that is maintained by a federal agency in a system of

---

*Pri vacy* Interests and Organizations' Information **Needs**, 44 Alb. L. Rev. 589, 600-01 (1980).

62 United States v. Miller, 425 U.S. 435, 443 (1976).

63 See, Federal Housekeeping Statute of 1797, as amended and the Freedom of Information Act, 5 U.S.C. §§ 301 and 552.

records from which information can be retrieved by name or other personal identifiers. 5 U.S.C. § 552a. The Privacy Act, however, preserves substantial agency discretion and flexibility.

As to the initial collection of personal information, the Privacy Act "urges" federal agencies to collect personal information directly from the individual. The Act, however, leaves agencies *free to* collect personal information from third-party sources if collecting information from the individual is impractical.

As to the retention of personal information, the Privacy Act instructs agencies to retain personal information only if it is relevant and necessary to an agency purpose. The relevant and necessary standard, however, leaves agencies with ample discretion to retain personal information which is related to the agency's discharge of its responsibilities.

The Privacy Act also covers agency *use* of personal information and requires that before using personal information, agencies have in place procedures to assure that the information is accurate, timely, relevant and comnlete. Further, the Privacy Act forbids agencies *from* permitting Its employees to obtain access to personal information except on a need-to-know basis. Disclosures outside the agency are forbidden, except with the consent of the individual unless the disclosure meets one of close to a dozen exceptions. Taken together, those exceptions permit agencies to release personal information on a non-consensual basis for virtually any governmental purpose.

The Privacy Act does give individuals a right of access to information about them held by a federal agency and opportunities to correct or amend their record. The Privacy Act also includes both general and specific exemptions from its requirements with respect to record systems compiled for certain special purposes or *uses,* including law enforcement. Remedies under the Privacy Act are limited and have proven difficult to obtain.

Thus, although federal agencies that "databased" personal information obtained from IVHS applications will have to conform the collection, retention *use* and dissemination of that data to Privacy Act requirements, this responsibility should pose little problem.

The Freedom of Information Act ("FOIA") 5 U.S.C. § 552 is the other federal information statute that could have a significant impact on the federal government's handling of personal data

---

[64] See, e.g., O'Reilly, Federal Information Disclosure, Chapter 21 Shepard's/McGraw-Hill, Inc., (June, 1993).

generated by IVHS applications. The FOIA makes all federally-held information available, upon request to any person, for any purpose, unless one of the FOIA's nine exemptions apply. One of those exemptions covers information, which, if disclosed, would be likely to result in a clearly unwarranted invasion of privacy. 5 U.S.C. § 552(b)(6).

In adjudicating access to privacy-sensitive information, the Supreme Court has said that agencies should weigh the public's interest in disclosure against the potential for an invasion of privacy. Most recently, the Supreme Court has held that the disclosure of any personal information is presumed to violate privacy interests, and the only disclosure interest to be weighed against this privacy violation is whether the disclosure would give the public information on governmental conduct or misconduct."[65] Thus, as far as FOIA, the present Court has tipped the balance mightily in favor of privacy, at least where disclosure of government-collected personal information is concerned. Accordingly, if a federal agency is holding IVHS generated data which identifies a specific individual and indicates the individual's location at a particular time or the individual's vehicle ownership or some characteristic about the individual's operation of a motor vehicle it is likely that disclosure would be considered a "clearly unwarranted invasion of privacy."

4. Stats Information Statutes

State privacy and recordkeeping statutes will be relevant because IVHS generated personal information could well be collected and retained by state agencies.. However , these statutes like their federal counterparts, are not expected to create significant obstacles to the databasing of IVHS generated data.

Approximately a dozen states have enacted their own statutes modeled after the federal Privacy Act. The remainder and majority of the states have not enacted comprehensive privacy statutes to regulate the collection, retention, use and dissemination of personal information held in state files. Rather, most states have a patchwork of privacy statutes governing specific types of personal records such as medical records and educational records. These statutes, impose on the private sector the same kinds of information responsibilities imposed by statute on federal and state governments. These responsibilities customarily include modest limits on the collection of personal information; standards

---

[65] Reporters Committee for Freedom of the Press v. United States Department of Justice, 489 U.S. 749, 773 (1989).

[66] See, Robert Ellis Smith Compilation of State and Federal Privacy Laws, June, 1991.

for the accuracy and completeness of information; confidentiality and data security standards; and data rights standards that provide subjects with access and correction rights.

Most states have also adopted statutes that regulate the handling of motor vehicle registration and operating information and license and driver violation information, In over 30 states this information to varying extents, is available to the public. The public availability at this kind of driver information is under attack, however, and the Senate recently passed legislation to limit the public availability of motor vehicle and driver license information. These developments strongly suggest that if IVHS information is databased, whether in state or private sector databases, there will be a strong push for confidentiality protections.

Thus, it is certainly possible that state statute law, either as presently existing or as enacted in the future, would effect a state agency's or a private organization's practices in databasing personal information generated by IVHS applications.

Every state has also adopted its own open records or Freedom of Information Act. Most of these statutes are modeled after the federal law, and all of these statutes include an exemption that provides protection against the disclosure of personally identifiable information. In light of the Supreme Court's landmark decision in Reporters Committee, however, it is probably safe to conclude that many state FOIA statutes do not provide the same degree of privacy protection provided, at present, under federal law. Therefore, to the extent that IVHS generated personal data is held in state files, there is the possibility that some of this data could be accessible and placed in the public domain as a result of access requests filed under state open record or freedom of information statutes.

5. Common Law Informational Privacy Claims

Common law informational privacy protections, like their constitutional analog, are underdeveloped.

Over forty states have adopted Prosser's four part articulation of common law privacy/tort actions. One of those 'four common law actions is essentially an informational privacy

---

[67] Id.

[68] See Drivers Privacy Protection Bill of '93 at Cong. Rec. S. 15761, Nov. 16, 1993.

[69] Prosser Law of Torts, Chapter 20, "Privacy" ,West Publishing Co., (4th Edition) (1971).

action which creates a duty not to publicly disclose private facts in cases where the disclosure would be highly offensive to a reasonable person-and is not of legitimate concern to the public.

The obstacles to making out a claim for public disclosure of private facts are substantial. A plaintiff would have to establish that the IVHS-generated personal data should be considered a "private fact". Moreover, the plaintiff would have to *show* that the disclosure was unauthorized because made without lawful authority or the benefit of the individual's implicit or explicit consent. Further, the plaintiff would have to show that the disclosure was not a limited, targeted disclosure, but rather a disclosure to the general public. All of these hurdles suggest that it would be difficult for a vehicle owner or occupant whose information is collected and retained as a result of an IVHS application to successfully prosecute an informational privacy tort claim. As a practical matter, common law privacy claims are unlikely to have much impact on the collection and retention of personal information arising from IVHS applications.

Taken together, existing constitutional, statutory and common law informational privacy standards are not expected to pose significant obstacles to the collection, retention, use or dissemination of IVHS generated personal data.

## IV. STRATEGIES TO FACILITATE THE IMPLEMENTATION OF IVHS APPLICATIONS AND TO PROTECT PRIVACY

### A. Introduction

The strategies recommended in this paper are based upon the following assumptions about IVHS architecture.

- At least some IVHS applications will identify specific vehicles and perhaps specific drivers.

---

[70] Although tort privacy claims are customarily referred to as common law claims, in fact, privacy actions did not exist at common law, and their existence today is owed to enactment in over forty states of statutes that expressly create a tort action. Trubow Privacy Law and Practice, Chapter 1, "Tort Law of Privacy" Matthew Bender (1991)

[71] Id. at § 1.05.

- Some IVHS applications will generate personal information which will be "databased" in auromated, name retrievable information systems.

- Both IVHS surveillance programs and any resulting information systems may be operated by government *agencies,* presumably at the state level.

  There may well be exchanges of information between private and public sector organizations, and between local, state and federal agencies.

Our policy analysis strongly *suggests* that privacy and consumer advocacy groups, the media and consumers are likely to raise legitimate privacy concerns about the implementation of at least some IVHS applications. On the other hand, our legal analysis concludes that existing law will offer few obstacles to the implementation of even the most ambitious IVHS applications. The absence of existing legal hurdles puts policy makers in the enviable position of being able to design IVHS privacy strategies that are affirmative and creative rather than negative and defensive, as well as to help guide state and federal legislators in writing new strategies and/or regulations that will be enacted as IVHS applications are seen to call for such new legal definitions.

A strategy for enhancing the public acceptability of IVHS applications while protecting privacy would have three components.

- A research component, the centerpiece of which would be a national public opinion survey. This survey would take a "first reading" of public attitudes in the present early stages of IVHS demonstration and prototype programs, thereby providing a "baseline" that could then be tested across the remainder of this decade as IVHS applications widen and predictable public debates over privacy issues unfold.

- A policy component, the centerpiece of which would be a comprehensive IVHS privacy code.

- A legal component, the centerpiece of which would be model state legislation, or perhaps, a state compact as well as complimentary federal legislation.

## B. Research Recommendations

The literature search undertaken in connection with the preparation of this paper makes clear that relatively little

*serious* attention has been given to the privacy issues raised by IVHS applications, In particular, little is known about the nature and intensity of the public's concerns about IVHS. Accordingly, we recommend the development and administration of a well conceived, national public opinion survey. That survey would have the following components.

- It should present respondents with adequate descriptions of a wide range of IVHS applications; identify the social benefits expected to be realized; and obtain data on how valuable the public sees those applications to be (or not to be).

- It should pose one by one the various issues of privacy raised by each application, and probe the level of concern (or unconcern) respondents feel about each of those.

- It would then present a series of privacy protection standards, procedures, and safeguards for each application, and ask respondents how well those measures would overcome -- or compensate -- adequately for the privacy problems identified earlier. This section would also explore which public or private authorities respondents would trust to administer the safeguards or enforce the rules; what kinds of legislative or regulatory actions respondents wish to see; and what options or choices respondents believe individuals should (and practically could) have to decide when they would or would not participate in various IVHS-based systems or operations.

- It should analyze the sources of the public attitudes the survey would document, and identify those groups within the general public that are especially concerned about IVHS privacy issues. The survey would ask questions developed in Louis Harris privacy surveys over the past 15 years. Those questions -- probing factors such as distrust of institutions, attitudes toward computer *use,* and regulatory philosophy -- have been shown to be powerful explanatory factors in shaping public and group attitudes on privacy issues. Use of these factors would allow comparison of public attitudes on IVHS applications to patterns of public and group attitudes on consumer privacy, employee privacy, health privacy, law enforcement activities, *government* social services, and other major areas.

- This survey project cannot be simply "handed over" to a survey firm, but should combine a *strong* policy and legal expertise <u>with</u> top quality survey specialists. Such a

collaboration is needed in the design, interpretation, writing and public release of the survey findings.

Ideally, sponsorship and funding for such a baseline survey should come from a combination of private, government, and public-interest organizations. The primary players could be IVHS-America, the U.S. Department **of** Transportation; perhaps a state transportation agency or association; and a recognized consumer group, such as the Consumer Federation of America, or perhaps the American Automobile Association, representing the "driving public."

It would be desirable to commission and conduct this study by the end of 1994. Normally, a major national survey of this kind can be designed and conducted, and a refined report produced, in 6 months from the authorization (and availability *of* funds). Obtaining an early and clear picture of the public's IVHS privacy concerns would put the industry, government agencies, and legislatures in the best position to avoid privacy problems, and to design privacy protections while IVHS architecture is still at **a** formative stage. This should permit IVHS development to go forward cost-effectively and expeditiously and avoid or minimize retrofit issues.

In addition, we recommend that state by state legal and, in particular, statutory research be undertaken to establish a leqal/privacy baseline *for* each state. In some states wiretap laws may have been adopted that do not provide an exception for tracking devices or that otherwise might have adverse implications for IVHS. In a few states video surveillance may violate statute law, as may photo-radar. In many states, existing law may permit law enforcement agencies to obtain access to IVHS data, whereas in other states existing statutes would work in a way to preclude law enforcement access without specific subpoena to IVHS generated personal record information.

### c. Policy Recommendations

IVHS America and other IVHS proponents should encouraqe the development and adoption of a national, comprehensive IVHS privacy code. Increasingly, industries and organizations that are involved in privacy sensitive activities see benefit, indeed necessity, in

---

[72] IVHS America, located in Washinqton, D.C. is a broad-based, non-profit research and educational organization of IVHS contractors, academic institutions, government agencies, and others dedicated to the promotion of the development and use of intelligent vehicle-highway systems applications. IVHS America also functions as the federal advisory committee to the United States Department of Transportation.

nd adopting a privacy code. In light of the privacy
i by at least some IVHS applications the development,
nd public promotion of an IVHS privacy code is
hile it is premature to lay out the specifics of such
such code should address that following types of

sider whether IVHS applications can be designed, to
fullest extent possible, so as not to identify
cific *vehicles or* at least so as not to identify
vers and occupants.

sider whether IVHS surveillance programs should be
hibited from including video or photo capabilities.

ider whether IVHS roadways should bear IVHS posted
ices.

ider whether IVHS applications can be designed to
w drivers to initiate IVHS programs by activating an
oard IVHS unit.

ider whether on-board IVHS units can be designed so
they provide drivers with an indication that the
cle is being monitored by an IVHS program.

ider whether IVHS standards can be adopted to
ibit IVHS use except for traffic management and motor
cle operational purposes.

.der whether IVHS generated personal data will be
ased, and *if* databased, whether the information must
me accessible.

der whether IVHS generated personal information can
rged on a regular and frequent basis.

der whether IVHS standards can be adopted to provide
iduals with maximum rights of consent or, at a
im, maximum notice rights.

der whether IVHS data subjects can be given the
t possible panoply of participation rights,
Iing access and correction rights.

ier whether standards can be adopted to maximize the
.cy of IVHS- generated personal data and further
ed to avoid the mismatching of data.

er whether internal need-to-know standards and
entiality standards can be adopted with respect to
to IVHS-generated personal data and, in

andards can limit
he IVHS data was
or expressly and

with third party
[This is a
en that an IVHS
rich and unique
gatory purposes;
as civil justice
e purposes; and a
es.

*IVHS* database
adopted. [This
en that civil
an important
0 separate IVHS
s opposed to a
rconnected IVHS

privacy audits
for management

:y standards can

comprehensive
cations and the
uld be given to
accomplish the ,

*in* whole or in

code,

ypes of state
mplementation.

IVHS personal
party access
opriate third

- Insulate IVHS from law enforcement uses and other types of uses that are inconsistent with IVHS purposes, and setting safeguards for appropriate third party access.

- Institutionalize a partnership role in IVHS for the private sector.

IVHS America and other proponents of IVHS applications could work with the National Conference of State Legislators, the National Conference of Commissioners on Uniform State Law and other organizations to develop and implement a model state law. In conjunction with the state statutory initiative, consideration should be given to developing and moving a "State Compact" which would have the effect of binding every state that adopts the compact, as well as the federal government if it adopts the compact.

The model law or compact could be a vehicle for institutionalizing a public\private IVHS partnership. The model law or compact, for example, could establish or denominate a private organization, such as IVHS America, as the "Advisory Committee" to the model law or the compact. Indeed, state compacts customarily establish a permanent multi-jurisdictional body which sometimes has private sector participation to consider implementation issues as well as amendments to the compact.

Efforts to institutionalize a public\private partnership could also direct state and local agencies which are operating or sponsoring IVHS applications to consult and work with responsible private organizations *in* implementing and operating IVHS. Model legislation could also establish in each state an IVHS task force to include industry and consumer and privacy advocacy members in order to provide input for IVHS applications.

Finally, IVHS proponents should consider whether adoption of a federal statute would contribute to the implementation of IVHS applications and the protection of privacy. A federal law could serve as a follow-on to the Inter-modal Surface "Transportation Efficiency Act of 1991 and could institutionalize federal and Department **of** Transportation leadership, research and financial assistance. Federal law could also provide an alternative method for institutionalizing privacy standards by making federal funding to. the states contingent upon state compliance with federally imposed privacy standards. A federal statute could also institutionalize rules for federal access to IVHS databases, including access by federal law enforcement; federal courts; Secret Service for Presidential protection; the intelligence community for security clearance determinations; and other predictable federal access attempts.

## CONCLUSION

IVHS applications have enormous potential to improve traffic safety; enhance convenience; save fuel; and reduce pollution. Some IVHS applications, *however,* also threaten legitimate privacy interests. It is likely that the public will weigh the potential IVHS benefits against the IVHS privacy threat. It is also likely that the public will embrace or accept privacy- sensitive IVHS applications only if convinced that the benefits are real and that the privacy threats can be minimized through a comprehensive and effective privacy protection program.