Santa Clara High Technology Law Journal

Volume 11 | Issue 1 Article 8

January 1995

Privacy and Intelligent Highways: Finding the Right of Way

Sheri A. Alpert

SYMPOSIUM PAPER

PRIVACY AND INTELLIGENT HIGHWAYS: FINDING THE RIGHT OF WAY

Sheri A. Alpert†

"Technology is driving the future. It's time to find out who's steering."
(1990 poster from Computer Professionals for Social Responsibility)

I. INTRODUCTION

The U.S. Department of Transportation (DOT) is coordinating an endeavor that will change the way people interact with public and private road transportation systems. The overall program is called the Intelligent Vehicle Highway Systems (IVHS). Its aim, according to DOT, is to apply advanced communications, navigation, and information systems technologies to reduce traffic congestion, improve highway safety, and reduce environmental harm from vehicular traffic.

Few would contest the value of the program's intent. There are, however, other attendant outcomes that must be considered as the various IVHS technologies and applications are being contemplated and developed, particularly because public acceptance of these applications will be important to their success. Among these is the impact of IVHS applications on individuals' privacy.

IVHS creates data on individuals' travel patterns. It has the potential to make it possible for traffic management agencies to know where individuals travel, what routes they take, and their travel duration. For instance, after a relatively short period of tracking a vehicle, it may be possible to predict "when someone is or is not at home; where they work, spend leisure time, go to church, and shop; what schools their children attend; where friends and associates live;

† Ms. Alpert has worked for the federal government for the past 10 years, specializing in information privacy policy issues for the last 4 years. She is currently working on her Ph.D. in public policy from George Mason University.

whether they have been to see a doctor; and whether they attend political rallies"[1]

Traveler information is collected from many sources, including the system infrastructure, private vehicles, and transactions (like electronic toll collection) that involve interaction between the infrastructure and the vehicle. All of this transaction and travel pattern information has potential value in both IVHS and non-IVHS applications, both in real time and in retrospective analysis. Both the collection and the use of this information threaten individuals' informational privacy interests.

Additionally, some of the IVHS applications could greatly reduce an individual's choice by: selectively pricing some transportation options in ways that would be prohibitively expensive for some;[2] assessing the driver's fitness to continue operating the vehicle; and/or taking over the actual operation of the vehicle from the driver. These types of applications may impact an individual's autonomy. Finally, IVHS technologies can perform surveillance of travelers on the roadways.

All of these implications are important because the United States has yet to formulate a consistent public policy with equal applicability to all Americans, that protects an individual's and society's interest in privacy or in the confidentiality of an individual's personal information.

This paper explores the potential privacy interests at stake in IVHS — individual autonomy, intrusion (surveillance), and informational privacy — and how the IVHS applications and technologies may encroach on these interests. The paper will also provide an overview of some of the current legal landscape in which IVHS will be deployed, and make recommendations, where relevant, on how to best protect individual privacy interests as IVHS applications evolve.

II. An Overview of IVHS

In 1991, Congress passed Public Law 102-241, *The Intelligent Vehicle Highway Systems Act of 1991.* It directs the Secretary of Transportation to conduct a program to research, develop, and opera-

1. The Privacy Bulletin 1, 2. (1990).

2. One of the applications allowed by these technologies is the real-time pricing of any road, bridge, or on-ramp that has an associated toll. Parking facilities and public transportation can also be priced in real time. In other words, the infrastructure can immediately adapt to road conditions and traffic patterns/volume to encourage or discourage the use of various transportation options, by adjusting the cost of these options. While this may make the entire transportation system more efficient in the aggregate, it may not allow for individual needs. It is conceivable that the mode of transportation a person might find the most desirable or necessary may be priced, at that particular time, out of their financial reach.

tionally test intelligent vehicle highway systems and promote implementation of these systems as a component of the Nation's surface transportation systems. One goal stated within the legislation is to have the first fully automated roadway or an automated test track in operation by 1997. Congress also recognized within the legislation that there were nontechnical constraints that had to be addressed in IVHS applications. As such, the law required the Secretary to report to Congress on the "antitrust, privacy, educational and staffing needs, patent, liability, standards, and other constraints, barriers, or concerns" relating to the IVHS program.[3] This report was completed in June 1994.

DOT's vision for IVHS is "a future of safer and better informed travelers, improved traffic control systems, and systems aimed at increasing the efficiency of commercial vehicle and transit operations. The safety of highway travel will be significantly increased through products which ensure the driver's state of fitness, enhance driver perception, warn of impending danger, and intervene with emergency control to prevent accidents from occurring."[4] This is to be accomplished by applying technologies to vehicles and roadways that will perform surveillance, communications, data processing, traffic control, navigation, sensing, and other functions. The development and deployment of IVHS will be incremental, over the next several years, and may never be universal in its coverage of the highways and roads.

> The IVHS target concept is an interactive link of a vehicle electronic system with roadside sensors, satellites, and a centralized traffic management system to constantly monitor each vehicle's location and the traffic conditions. With more advanced systems, drivers would receive alternate route information in real time via two-way communications, onboard video screens and mapping systems. The data and communications would be immediate enough to be useful.[5]

3. Intellegent Vehicles Highway Systems Act of 1991, Public Law 102 - 241, Title VI, § 6054.

4. DEPARTMENT OF TRANSPORTATION, *IVHS Strategic Plan - Report to Congress*, December 18, 1992.

5. Andrew H. Card, Jr. *When 'Smart Cars' Meet 'Smart Highways'*, Advertising Supplement to the WASH. POST, March 22, 1994 at D8.

A. IVHS User Services

As described in the October 1993 draft National Program Plan for IVHS, technologies are being applied across 27 user services,[6] grouped into several functional areas or "clusters": Travel Planning, Advanced Traveler Information, Advanced Travel Management, Travel Payment, Advanced Vehicle Control Systems, Commercial Vehicle Operations, and Emergency Management.

- Travel Planning includes pre-trip travel information (e.g., optimal means of transportation and route selection), as well as ride matching and reservation user services.
- Advanced Traveler Information Systems (ATIS) lets drivers know their location and assists them with planning, perception, analysis, and decision-making to improve the efficiency of their travel. ATIS allows communication between travelers and ATMS centers for continuous information about traffic conditions.
- Advanced Travel Management Systems (ATMS) provides technologies to monitor, control, and manage traffic in real time, by communicating with drivers, adjusting traffic operations, and responding to incidents.
- Travel Payment Systems (TPS) features electronic payments for all transportation modes and functions, including toll collection, transit fares, and parking.
- Advanced Vehicle Control Systems (AVCS) will enhance the control of vehicles by "facilitating and augmenting driver performance and, ultimately, relieving the driver of most tasks on designated, instrumented roadways."[7] The services included in this cluster provide: 1) adaptive cruise control to slow the vehicle if it gets too close to the vehicle it follows; 2) warnings and/or vehicle control for lane departure and intersection crashes; 3) vision enhancement and monitoring of the driver's condition and performance to detect impairment or drowsiness; 4) precrash restraint deployment, where air bags would deploy prior to the crash, instead of upon impact; and 5) fully automated vehicle operation, the "Automated Highway System," where the infrastructure, and not the driver, operates the vehicle.
- Commercial Vehicle Operations (CVO) applies ATIS features within the commercial vehicle sector. It also applies ATMS services to fleet management functions.

---

6. In the newest draft Program Plan (May 1994), there are 28 user services, grouped into six differently defined clusters. However, because so many of the familiar IVHS clusters and acronyms are contained in the earlier Program Plan, this analysis will continue to use them.

7. Analysis of Federal and State Privacy Laws and Development of Safegaurdes to Protect Privacy, 58 Fed. Reg. Anouncement 29,444, 29,445 (May 20, 1993).

- Emergency Management includes services designed to notify the proper authorities in cases of emergency, provides hazardous materials notification, and notice to authorities in cases of vehicle breakdown or car-jackings. It also provides for emergency vehicle management, as well as security services for public transportation.

Each of these clusters applies largely existing technologies in innovative ways that can have unintended effects on the privacy of individuals operating vehicles or using public transportation. Taken together, these clusters, and the user services comprising them, could offer the public the ability to maximize traveling safety, minimize travel time, and improve air quality.

B. IVHS Technologies

There are several types of technologies and applications contemplated for IVHS. Generally, these technologies fall into seven broad "families". The families and some of the technologies within them are as follows:

- Surveillance: vehicle probes, infrared sensors, microwave and radar sensors, aerial surveillance, machine vision, Automated Vehicle Identification (AVI), closed circuit television, automated vehicle classification, and automated vehicle location.
- Data/voice communications: (vehicle to and from the infrastructure) local-area broadcast, FM subcarrier (one-way), wide-area radio system (two-way), cellular radio, and satellite (two-way), (within the infrastructure) land lines, microwave, wide-area radio system and satellite; (from vehicle to vehicle) microwave and infrared/radar.
- Traveler interface: touch screen, keypad, voice recognition, visual display, smart cards, heads-up display, personal communications device.
- Traffic control strategies: ramp metering, HOV and/or parking restrictions, signal control, ramp/lane closures, road use pricing, and reversible lanes.
- Navigation/guidance: position and guidance displays, map databases, dead reckoning, map matching, and Global Positioning Systems (GPS).
- Data processing: static and dynamic databases, driver/vehicle/cargo schedules, real time traffic predictions, data fusion technology, incident detection algorithm, and coupled route selection and traffic control.
- In-vehicle sensors: equipment status sensors, vehicle headway sensors, lane keeping sensors, proximity sensors, driver fatigue and performance monitoring, and improved vision.

While these technologies are often associated with one or more user services, and because there is interaction between many of the user services, it is impractical to provide a one-to-one correlation between technologies and user services. If a technology is primarily applicable to one service, it will probably be indirectly applicable to others. Table 1[8] provides a summary matrix of the types of technologies within the various user services.

III. Privacy Interests at Stake in IVHS

Although there is no universally accepted definition of the right to privacy,[9] for most of us, privacy is related to notions of solitude, autonomy, anonymity, and individuality. Privacy is, thus, a very personal notion. Within socially or culturally defined limits, privacy allows us the freedom to be who and what we are. The very fact that we are able to interact with others as we might like is because our privacy allows us that choice.[10] By embracing privacy, we exercise discretion in deciding how much of our personhood and personality to share with others. We generally feel less vulnerable when we can decide for ourselves how much of our personal sphere they will be allowed to observe or scrutinize. James Rachels described privacy as being "based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people."[11]

In the United States, the Constitutional basis of privacy has been found in Supreme Court majority opinions to lie in the explicit guarantees of the First, Fourth, Fifth, Ninth, and Fourteenth Amendments,[12]

---

8. United States Department of Transportation, National Program Plan for Intelligent Transportation Systems (Final Draft, Nov. 1994) at IV-10.

9. See for instance, Anita Allen, Uneasy Access (1988); Ruth Gavison, *Privacy and the Limits of the Law, in* Philosophical Dimensions of Privacy: An Anthology, 346, 347 (Ferdinand Schoeman, ed. 1984); Charles Fried, *Privacy (A Moral Analysis)*, 77 Yale L. J. 475, 477 (1968). *See also* James Rachels, *Why Privacy Is Important, in* Philosophical Dimensions of Privacy, 475-93; Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, reprinted in* Philosophical Dimensions of Privacy, 156, 187-88.

10. Sheri Alpert, *Smart Cards, Smarter Policy: Medical Records, Privacy, and Health Care Reform*, 23 Hastings Center Report 13, 18 (1993).

11. Rachels, *supra* note 9, at 292.

12. The First Amendment guarantees freedom of communications and the expression of ideas; the Fourth Amendment guarantees freedom from unreasonable search and seizure, including (in some cases) electronic, aural, visual, and other types of surveillance; the Fifth Amendment guarantees freedom from self-incrimination, and guarantees due process of the law with regard to the Federal government; the Ninth Amendment recognizes that rights not specified in the Constitution are vested with the people; and the Fourteenth Amendment guarantees due process and equal protection of the law with regard to the states.

TABLE 1: MAPPING OF USER SERVICES TO IVHS TECHNOLOGIES (SUMMARY CHART)

IVHS User Services (arranged by clusters)	1	2	3	4	5	6	7
Travel Planning							
Pre-Trip Information	X	X	X		X	X	
Ride Matching & Reservation		X	X			X	
Traveler Information							
En Route Driver Advisory	X	X	X		X	X	
En Route Transit Advisory	X	X	X		X	X	
Traveler Services Information		X	X		X	X	
Route Guidance		X	X		X	X	X
Travel Management							
Incident Management	X	X	X	X	X	X	
Travel Demand Management	X	X	X	X	X	X	
Traffic Control	X	X	X	X		X	
Public Transportation Management	X	X	X	X	X	X	
Personalized Public Transportation	X	X			X	X	
Travel Payment							
Electronic Payment Systems	X	X	X			X	
Advanced Vehicle Control Systems							
Longitudinal Collision Avoidance		X	X				X
Lateral Collision Avoidance	X	X	X				X
Intersection Collision Avoidance	X	X	X		X	X	
Vision Enhancement for Crash Avoidance			X				X
Impairment Alert		X	X				X
Pre-Crash Restraint Deployment			X				X
Fully Automated Vehicle Operation		X		X			X
Commercial Vehicle Operations							
Commercial Vehicle Preclearance	X	X				X	
Automated Roadside Safety Inspections		X				X	X
Commercial Vehicle Admin. Processes	X	X				X	
On-board Safety Monitoring			X				X
Commercial Fleet Management	X	X			X	X	
Emergency Management							
Emergency Notification & Personal Security	X	X	X		X	X	X
Public Travel Security	X	X			X		
Emergency Vehicle Management	X	X	X		X	X	

TECHNOLOGIES LEGEND:

1. Surveillance
2. Data/Voice Communication
3. Traveler Interface
4. Control Strategies
5. Navigation/Guidance
6. Data Processing
7. In-Vehicle Sensors

(Source: October 1993 National Program Plan for IVHS, p. IV-10)

as well as the broader range of implied rights created by them in what is referred to by courts as "zones of privacy." The ideas expressed in the Constitution supported individual supremacy against the government and other organizations.[13]

In general, current Federal and state laws provide sectorally-based protection for individuals in response to specific and recognized

13. KENNETH LAUDON, DOSSIER SOCIETY 367-68 (1986).

problems.[14] This approach derives from the traditional American fear of government intervention in private activities and the reluctance to broadly regulate industry.[15]

The privacy interests that have been contained in U.S. court opinions often encompass three distinct but related interests: autonomy, intrusion, and informational privacy.[16] Additionally, courts generally speak of privacy in terms of a "reasonable expectation" — it is not an absolute expectation, and as sociologist James Rule noted, ". . .the only safe generalization is that the status of privacy in the modern world is changing. The possibilities of enjoying privacy, in virtually every sense of the term, are not what they have been nor, apparently, what they are going to be."[17] This is the context into which IVHS applications will be deployed.

A. Autonomy

> An important justification for privacy resides in the principle of respect for autonomy. To respect the privacy of others is to respect their wishes not to be accessed in some respect — not to be observed or have information about themselves made available to others.[18]

Autonomy, as it has been interpreted by the courts to date, means that one is free to engage in intimate or private activities, free from government intervention and regulation. The courts have generally used an individual's interest in autonomy in deciding cases involving abortion and the use of birth control. This interpretation is inadequate within the context of this analysis, because the case law has not yet addressed the types of issues involving autonomy that are likely to be brought under IVHS applications. (These cases could conceivably involve instances where the infrastructure takes control of a vehicle away from the driver.) The National Research Council recently described individual autonomy more broadly:

---

14. *E.g.:* the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Video Privacy Protection Act, the Cable Communications Policy Act, and the Family Educational Rights and Privacy Act.

15. Joel Reidenberg, *Privacy in the Information Economy; A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L. J. 195, 209 (1992).

16. *See* GEORGE B. TRUBOW. PRIVACY LAW AND PRACTICE (1991).

17. JAMES B. RULE, DOUGLAS MCADAM, LINDA STEARNS, DAVID UGLOW, THE POLITICS OF PRIVACY 1 (1980).

18. Larry Gostin, Joan Turek-Brezina, Madison Powers, Rene Kozloff; Ruth Faden, Dennis Steinauer, *Privacy and Security of Personal Information in a New Health Care System*, 270 J. AM. MED. ASSO. 2487, 2490 (1993).

> [It] refers to the capacity of members of society to function as individuals, uncoerced and with privacy. Protection of individual autonomy is a fundamental attribute of a democracy.[19]

It is the broader set of privacy interests encompassed by the NRC description that forms the basis for the discussion of autonomy within this analysis.

B. Intrusion

The privacy interest against intrusion means being free from surveillance in situations in which an individual has a reasonable expectation of privacy. It encompasses the individual's interest in preserving his/her anonymity.

> 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 [or other organizations are] systematically and continuously recording who was where, and when.[20]

Anonymity and freedom from surveillance are aspects of privacy that have been explored extensively by many scholars. For instance, legal philosopher Anita Allen writes that privacy "denotes a degree of inaccessibility of persons, of their mental states, and of information about them to the senses and surveillance devices of others."[21] Ruth Gavison speaks of limited accessibility to others, and explains that we enjoy our privacy "not because of new opportunities for seclusion or because of greater control over our interactions, but because of our anonymity, because no one is interested in us. The moment someone becomes sufficiently interested, he may find it quite easy to take all that privacy away."[22]

In the context of this analysis, intrusion will connote those IVHS activities that are more surreptitious. It encompasses monitoring activities that are hidden from view of those making use of the various transportation modes (e.g., visual monitoring using cameras and satellite technology). These are intrusions that occur, for the most part, in real time, and often without the consent of those being monitored.

---

19. NATIONAL RESEARCH COUNCIL AND SOCIAL SCIENCE RESEARCH COUNCIL, *Private Lives and Public Policies: Confidentiality and Accessibility of Government Statistics* 3 (1993).

20. ROBERT BELAIR, ALAN WESTIN, JOHN MULLENHOLZ, PRIVACY IMPLICATION ARISING FROM INTELLIGENT VEHICLE HIGHWAY SYSTEMS 9 (1993).

21. ALLEN, *supra* note 9, at 3.

22. Gavison, *supra* note 9, at 379.

This kind of surveillance can have a chilling effect on individuals, as noted by many sociologists and studies of electronic monitoring. Individuals often change their behavior to conform to what they believe those monitoring their movements/actions will find "acceptable" or "normal".[23] "Simply stated, the knowledge or fear that one is under systematic, asymmetrical [one-way] observation in public places destroys the sense of relaxation that individuals seek in open spaces and public arenas."[24]

C. Informational Privacy

If privacy encompasses the right individuals have to exercise their autonomy and to limit the extent of their personal domain to which others have access, in the "Information Age" this concept is largely defined by how much personal information is available from sources other than the individual to whom it pertains. The less opportunity individuals have to limit access to their own personal information, or to limit the amount of personal information they must give up to others (either voluntarily or by coercion), the less privacy they have.[25] This also involves when such information should be communicated or obtained, and what uses of it will be made by others.

As David Flaherty has noted, vital personal interests are at stake in the use of personal data by public and private sector organizations: "Such activities threaten personal integrity and autonomy of individuals, who traditionally have lacked control over how others use information about them in decision making. The storage of personal data can be used to limit opportunity and to encourage conformity."[26]

> The stakes involved go beyond any individual, however. Information is "a source of ability to make decisions for oneself and to limit the decisional opportunities of others. It is something fought for and prized. Every time you find, on the one hand, a debate between strong privacy advocates . . . and a variety of others who oppose them, [you] find a struggle to decide who controls the essential terms of our social relationships."[27]

---

23. *See, e.g.*, Erving Goffman, BEHAVIOR IN PUBLIC PLACES, (1963); Alan Westin, PRIVACY AND FREEDOM, (1967); Vincent Brannigan and Bernard Beier, *Informational Self-Determination: A Choice Based Analysis*, DATENSCHUTZ UND DATENSICHERUNG, 467-472 (1985).

24. *Private Lives*, *supra* note 19, at 11.

25. Alpert, *supra* note 10, at 19.

26. DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETY: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 8 (1989).

27. Madison Powers, *Consequences to the Individual: Data Collection; Information use, and Electronic Health Systems*, *in* HEALTH RECORDS: SOCIAL NEEDS AND PERSONAL PRIVACY 79, 82 (1993).

This notion is further refined in the writings of James Rule. He differentiates between "aesthetic" and "strategic" privacy. Aesthetic privacy means that personal information is restricted as an end in itself, that is, in instances where disclosure is inherently distressing or embarrassing. Strategic privacy is the restriction of personal information as a means to some other end. In other words, "the issue is not the *experience* of disclosing personal information, but the longer-term consequences of doing so."[28] It is mostly strategic privacy interests that are at risk in the collection and use of personal information within IVHS.

These three elements of privacy (autonomy, intrusion, and informational privacy) are by no means mutually exclusive. They overlap, as noted in part of the National Research Council's definition of autonomy: "If excessive surveillance is used to build databases, if data are unwittingly dispersed, or if those who capture data for administrative purposes make that information available in personally identifiable form, individual autonomy is compromised."[29] In many respects, therefore, there is something of a chain of activities that describes some of the elements of privacy invasiveness: surveillance allows for real time visual monitoring; the data gathered through this process can be stored in databases in ways that can identify vehicles and perhaps people, which then may impact and/or compromise individual autonomy.

D. How Technology & Information Processing Have Changed the "Rules"

The activities being contemplated within IVHS do not occur within a vacuum. They are merely a set of activities that mark a progression of American society toward accumulating more data on individuals. The increase in the number and complexity of policies the U.S. government must administer, a process paralleled in the private sector in products and services offered, has had two consequences insofar as the collection of personal information is concerned: quantitatively, there has been an increase in the amount of information collected in order to appropriately provide requisite services; and qualitatively, there has been a change in the nature of the information collected.[30] As public and private sector programs have become increasingly refined, more sensitive and discriminating information on

28. Rule, *supra* note 17, at 22.

29. *Private Lives*, *supra* note 19, at 3.

30. COLIN BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 18 (1992).

the most sensitive aspects of people's lives and backgrounds has been required. "Even the most obscure and least mobile members of modern societies have the details of their lives recorded and stored in distant places by distant agencies. . . .the written records of one's life, in modern America . . ., shape the treatments one receives by organizations."[31] Colin Bennett further develops this phenomenon, stating:

> Moreover, the ability to assemble information selectively, or to correlate existing information, can be functionally equivalent to the ability to create new information. This capacity, obviously facilitated by information technology, enables [government] agencies [and other organizations] to identify, target, and perhaps manipulate a certain segment of the population that has common . . . characteristics.[32]

These new and more complicated relationships between the individual and those with the power to monitor, collect, and manipulate information are at the root of the informational privacy and intrusion issues. IVHS applications offer this possibility since they hold the promise of amassing enormous amounts of personal information on travel and driving habits, much of which will be gathered from surveillance activities.

IV. IVHS Technology Applications Having Implications for Privacy

Not all of the user services and technologies identified above have the same implications for personal privacy. Table 2 delineates the user services that have the potential to implicate personal privacy interests.[33] (It is mostly within the context of the user services that these technologies have implications for personal privacy.)

A. Autonomy

From an autonomy perspective, the technology application having the greatest implication is the in-vehicle sensor technologies. These include the technologies that will take over the actual operation of a vehicle from the driver, if, for instance, these sensors "determine" that the driver is not performing the task adequately. Other technology applications implicating autonomy are those in the traffic control grouping that selectively price transportation options in real time, according to traffic patterns and other factors. These include parking

31. Gostin, *supra* note 18, at 2.

32. Bennett, *supra* note 30, at 18-19.

33. National Program Plan, *supra* note 8. This is a table I have created from the materials cited in note 8.

TABLE 2: PRIVACY INTERESTS IMPLICATED BY IVHS USER SERVICES

IVHS User Services (arranged by clusters)	Autonomy	Informational Privacy	Intrusion
Travel Planning			
Pre-Trip Information	X	X	X
Ride Matching & Reservation		X	
Traveler Information			
En Route Driver Advisory		X	X
En Route Transit Advisory			X
Traveler Services Information		X	
Route Guidance		X	X
Travel Management			
Incident Management			X
Travel Demand Management	X	X	X
Traffic Control			X
Public Transportation Management		X	
Personalized Public Transportation		X	
Travel Payment			
Electronic Payment Systems	X	X	X
Advanced Vehicle Control Systems			
Longitudinal Collision Avoidance	X		X
Lateral Collision Avoidance	X		
Intersection Collision Avoidance	X		X
Vision Enhancement for Crash Avoidance			
Impairment Alert	X		X
Pre-Crash Restraint Deployment			
Fully Automated Vehicle Operation	X		X
Commercial Vehicle Operations			
Commercial Vehicle Preclearance		X	X
Automated Roadside Safety Inspections		X	
Commercial Vehicle Admin. Processes		X	X
On-board Safety Monitoring	X	X	
Commercial Fleet Management		X	X
Emergency Management			
Emergency Notification & Personal Security		X	X
Public Travel Security			X
Emergency Vehicle Management			X

(Based on breakdown of User Services identified in October 1993 National Program Plan for IVHS)

restrictions and road use pricing strategies. These technologies may not be able to account for unique circumstances people face in making transportation choices.

B. Intrusion

The surveillance technologies are those with the greatest impact on the privacy interest against intrusion. These are the technologies that are not necessarily apparent to the casual observer but that, nonetheless, provide constant monitoring of every activity occurring within

their range. It is the use of surveillance technologies within IVHS that could make it possible to find and track particular vehicles with some degree of precision. This is not always a negative prospect, particularly if the surveillance is tracking a stolen vehicle. However, there are also other circumstances in which this type of surveillance would be unwarranted and unwelcomed. The potentially chilling effect of surveillance on behavior has already been discussed.

C. Informational Privacy

From an informational privacy perspective, the technology "family" having the greatest implication is data processing. Additionally, some of the individual technologies within other "families" also have implications for this aspect of privacy. Included in this latter category would be touch screen and key pad technologies, smart cards, in-vehicle navigation computers, and personal communications devices. Many of these technologies could rely on one- and two-way interactions between the vehicle or individual and the infrastructure, which generate transactional data that may be captured in identifiable form in a computerized database. Anytime this occurs, there is the potential for the vehicle operator's driving habits and travel patterns to be known and conceivably analyzed. It also allows for an additional means for real time tracking of vehicles, and perhaps their occupants. Chief among the technologies accounting for this effect is AVI, automated vehicle identification. AVI utilizes electronic tags or transponders affixed to a vehicle that transmit a signal to a receiver, which then automatically identifies the vehicle to the infrastructure computers. Coupled with the mapping and other surveillance capabilities in IVHS, it may be possible to display, in real time, precisely what vehicle is on what road at what time.

The combined effect of surveillance and the capturing of information about the vehicle's location and destination are among the most serious that must be considered in developing and deploying these technologies as noted in the *Privacy Bulletin.*

> When a computer database is used in conjunction with a vehicle tracking device the potential exists for continuous surveillance of an individual, as well as the cross-matching of that information with information about the movements of other individuals. In this way, the marriage of the two technologies greatly increases the threat to individual privacy.[34]

34. THE PRIVACY BULLETIN 2 (1990).

Several of the technologies have little if any impact on privacy. This is because these technologies, in and of themselves, do not generate data on vehicle operators, or take actions directly affecting drivers. These would include some of the traveler interface technologies, such as heads up displays and variable message signs which appear on highway overpasses. Also included are some of the traffic control strategies, like ramp metering, HOV restrictions, signal controls, ramp/lane closures, and reversible lanes.

V. THE PRIVACY PROBLEM

An underlying issue is that all these technologies generate information that is acted upon in some way by infrastructure operators (humans), or the infrastructure itself (computers). In the case of some technologies and user services (e.g., route guidance, pretrip information, ATMS, ATIS, and travel payment), informational privacy interests are implicated. In the case of AVCS (advanced vehicle control systems) and parking and road use pricing strategies, autonomy is threatened. However, in both cases the implication is rooted in the fact that a person's interaction with the infrastructure and his/her vehicle (or public transportation) generates information that is then acted upon. In the case of the former (informational privacy implicators), the effect upon privacy may often not be immediately apparent. For instance, some of these effects could be delayed, as third parties receive data and analyze them. In the case of the latter (AVCS), the effect upon privacy interests of autonomy is more immediately apparent, particularly if the driver is "priced out" of choices, or if the infrastructure takes over the physical operation of his/her vehicle.

Additionally, the longer traveler data remain in a database and in identifiable form, the more potential exists for the intrusion and informational privacy interests to become autonomy interests. This may happen if data are used by a state to determine whether to renew an individual's driver's license. It may also happen if data are used in ways that are unrelated to the transportation system. As Robert Belair notes,

> 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.[35]

35. Belair, *supra* note 20, at 11.

There are many other potential non-IVHS uses of IVHS data that could have implications for privacy as well. IVHS contemplates the use of an "electronic yellow pages" to identify businesses of interest near where they are located at any point in time. Through the touch screen and key pad technologies in the vehicle, a driver could locate the nearest Tex-Mex restaurant, a particularly convenient service if one is in an unfamiliar location (and wants Tex-Mex food). The question that must be addressed, however, is to what extent the driver's identity should be knowable to the owner of the restaurant (and other area restaurants) merely because he/she is hungry? This seems like a fairly benign example, and it might be, if it ended there. However, it probably would not, given the enormous industry of marketing and selling personal information. There is a potentially huge market waiting to be exploited on the sale of transactional information generated by IVHS applications.

> The fact is, the technologies and techniques of mass surveillance allow companies to learn details we never would have told them if asked directly — details, even, that the law in other contexts prohibits companies from collecting, such as information on race, age, religion, and sexual orientation. The technology gives companies unprecedented power to muscle in on the "sacred" corners of our lives, those personal events we treasure as ours alone, and to transform them into commodities for subsequent sale, rent, or barter, a process consumer theorists call "commoditization".[36]

As an example, a company called National Decision Systems is developing a system called Equis. This system "maintains a database of financial information for over 100 million Americans on more than 340 characteristics, including age, marital status, move history, credit card activity, buying activity, credit relationships (by number and type), bankruptcies, and liens. This information is updated continuously at a rate of over 15 million changes per day."[37] Combining this detailed a level of demographic data with the travel patterns of these people (both of which can be arrayed geographically) will yield a previously unprecedented level of detail on nearly everyone in the United States. The extent to which individuals are given the opportunity to prohibit non-IVHS uses of their personal information will play a major role in how well their privacy is protected.

---

36. ERIK LARSON, THE NAKED CONSUMER 208 (1992).

37. DAVID CURRY, THE NEW MARKETING RESEARCH SYSTEMS: HOW TO USE STRATEGIC DATABASE INFORMATION FOR BETTER MARKETING DECISIONS 264 (1992).

A. Legal Issues

IVHS poses several challenging legal issues, partly because the systems rely heavily on partnerships between the Federal government, state and local governments, and the private sector. (Indeed, IVHS America, a nonprofit, public/private scientific and educational corporation that acts as a Federal Advisory Committee to the U.S. Department of Transportation on IVHS issues has over 300 private corporations as members.) This is challenging legally because of the need to determine which laws apply to IVHS. Not only are there Constitutional issues with which to contend, there are also Federal and state laws as well as common law (determined by cases brought before various courts).

From the Constitutional perspective, the Fourth and Fourteenth Amendments may be most directly tested. The Fourth Amendment forms the basis for claims to be free from government surveillance, protecting against unreasonable searches and seizures. The Supreme Court has found that surveillance of a vehicle travelling on public streets is not considered a search within the ambit of the Fourth Amendment. However, if data are collected from vehicles without consent of the vehicle's owner or operator, questions will "be raised inevitably as to whether the capture violates at least the spirit of the Fourth Amendment."[38] Although drivers and users of public transportation may have implicitly consented to data collection by using the infrastructure, the degree to which they understand the implications of that use for data collection and surveillance may be open to question.

The Fourteenth Amendment allows for due process and equal protection of law with respect to the states. Again, the Supreme Court has relied on this Amendment in deciding cases of individual and familial autonomy in cases revolving around birth control and marital relations. As stated earlier, the types of autonomy issues likely to be raised by IVHS applications have yet to reach the courts.

The Privacy Act of 1974 may have some implications for IVHS. The act provides a set of mandates for personally identifiable records in the custody of the Federal government and delineates the rights individuals have with respect to those records. It is unclear at this time how much of the data generated by IVHS applications will be in the custody of the Federal government. However, in all likelihood very little will "belong" to the Federal government.

Another major Federal law that may be applicable to IVHS is the 1988 Electronic Communications Privacy Act (ECPA), which

38. *Private Lives*, *supra* note 19, at 18.

amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The ECPA prohibits the interception of certain electronic communications and regulates the interception and use of such communications for law enforcement purposes. As currently constructed, the ECPA regulates only the interception of the content of a communication and not the fact of the communication. Additionally, it explicitly excludes mobile tracking devices from coverage. In other words, the ECPA allows the use of an electronic or mechanical device which permits the tracking of the movement of a person or object. On the other hand it is likely that any communication between a vehicle and the infrastructure that is "content rich" (e.g., specific route guidiance requests and responses) would be protected under the ECPA.

There are state laws and common law that must be considered. The protection of privacy is a component of roughly 10 states' constitutions. Additionally, about half the states have personal information statutes that are roughly analogous to the Federal Privacy Act for state governmental entities collecting and maintaining personal information. To the extent that IVHS data will be in the custody of state governments (which may be quite limited), these laws will apply. Between five and ten states have laws regarding employee monitoring. These laws could have an impact on the Commercial Vehicle Operations, because drivers and the trucks they are in will be monitored for fleet management purposes. Common law privacy torts are recognized in at least 47 states. The underlying point is that there is a myriad of state and common laws that have to be analyzed to determine their specific applicability to IVHS applications.[39]

Although it appears that, apart from some state and common law, there are few major legal obstacles to IVHS, this may be a misleading conclusion. Because these applications have yet to be deployed on a broad scale, it would probably be more appropriate to conclude that the current case law has not yet encountered many of the situations that are likely to be raised under IVHS.

VI. Policy Implications and Recommendations

To its proponents, the combination of technologies to be deployed under the Intelligent Vehicle Highway Systems have the potential to provide tangible benefits to the American public, helping reduce billions of dollars of productivity lost to traffic jams, making travel on public roads more efficient and potentially safe, and reducing

39. See the various charts on State privacy laws potentially applicable to IVHS, in this volume.

air pollution. Competing with these benefits, however, are social and legal barriers, one of which encompasses the potential loss of personal privacy and autonomy experienced by people taking advantage of these benefits.

One of the intriguing policy aspects of IVHS is the fact that driving in our society is generally considered by the states to be a privilege, and not a right. However, the public has a set of expectations of how they can exercise that privilege based on decades of precedent as to how the road transportation system has always operated. This could, in some courts, form the basis of what a reasonable expectation of privacy is, that:

> Even when engaged in a public act, such as driving, it is reasonable for the average, law-abiding citizen to expect that his/her actions will attract no more than casual observation by others. Anything more than casual observation has the potential to profoundly affect personal freedom, and in the case of driving, this would include the freedom to travel where and when one pleases and to associate with whom one pleases.[40]

The extent to which the public is willing to be subject to potentially extensive monitoring to continue to exercise this otherwise fairly anonymous privilege, is the fundamental question that may ultimately determine the success of IVHS.

What is needed is a mix of technical and legal remedies to minimize the losses of privacy while maintaining the functionality and benefits to be gained through IVHS. This can be accomplished by addressing both the technology and public policy.

VII. Recommendations for a Technology Response

There are many options with respect to the IVHS technologies that can be implemented to minimize the risks to privacy while maintaining the functionality that will meet the objectives of the program. In many of the IVHS user services, the identification of particular vehicles is not crucial to the service. For instance, in the traffic management service, the essential information is not which specific vehicles are on the road, but rather the aggregation of vehicles creating traffic patterns that the infrastructure must accommodate. Therefore, technology allowing for anonymous transactions (e.g., the use of a "smart card" without identifiers to pay for electronic tolls or public transportation, somewhat like fare cards in the Washington, D. C., Metro sys-

40. National Program Plan, *supra* note 8, at 2.

tem) and anonymous movement are important privacy-protecting tools.

Similarly, having more of the technology (or the "intelligence") reside within the vehicle, not the infrastructure, will also enhance individuals' privacy. For instance, in route guidance systems this can be accomplished, as it has been in some prototype systems, by having the onboard system include a database and computer processing technology to allow the vehicle to determine its own route or location with respect to beacons placed along the road. The simplest of these systems use CD-ROM technology to provide static maps to the driver — in other words, the system does not show the driver where he/she is with respect to any particular point, as a more interactive system using beacons or dead reckoning could. Even if positional information is an important feature to the developers of these systems, however, it is still not necessary for the vehicle to be identified to the infrastructure.

The use and placement of surveillance/monitoring technology is more problematic from a privacy protection standpoint. The very nature of these technologies intends that they be hidden. In the case of these technologies, one way to mitigate the negative and chilling effects is to ensure that the surveillance does not capture enough data from any vehicle to make it (or its occupants) singularly identifiable. In other words, the surveillance should be used to evaluate the general pattern of traffic, and not to single out vehicles or produce and store any photographic images of a particular vehicle.

Technical and technological solutions will be, to a large extent, affected by the overall architecture that is currently being designed. (The architecture provides the general system framework within which the user services will be deployed.) Privacy has been specified as one of the factors that those developing the architecture alternatives must consider. The Interim Status Report of the IVHS Architecture Development Program (April 1994) presents the initial concepts for the design of the architecture. Four different consortia have prepared architecture concepts, which show different levels of concern for and understanding of the privacy issues.

VIII. Recommendations for a Public Policy Response

The other way to address privacy issues in IVHS is through public policy. Ideally, this would include a standardized approach across the country that sets at least a minimum threshold of privacy rights, to ensure that as people travel between legal jurisdictions (i.e., across state lines) they have some rights that are constant, at least with respect to IVHS applications. Perhaps one of the most important as-

pects of protecting privacy from a policy standpoint is to make participation in any of the IVHS user services strictly voluntary, wherever practicable. In this way, people can decide for themselves what their priorities are. This presumes that people will be informed of the consequences of their decisions.

The voluntary nature of participation could be illustrated using the AVCS user services as an example. (Again, these services are the ones that could potentially take over vehicle operation if the driver is deemed unfit to drive.) If the intelligent highways are designed and deployed to offer these particular services only on specified lanes (analogous to the set aside "High Occupancy Vehicle" lanes on many urban roadways), entry onto these lanes might constitute driver consent. The main test of the legitimacy of that tacit consent might again lie in how well the driver is informed of the consequences of the decision. In this case, providing drivers with information about the risks and benefits of that choice will be crucial.

Perhaps one of the most troublesome public policy issues to resolve affecting privacy will be whether or not IVHS applications will be used for law enforcement purposes. Public acceptance of IVHS, partly motivated by privacy concerns, may be difficult to achieve if states can use IVHS as a means for law enforcement. A formal assessment of the risks and benefits of this use should be undertaken at the Federal level before any state uses IVHS for law enforcement.

Other protections should be incorporated into Federal law. Some of these encompass "Fair Information Practices", a draft series of which have been devised for IVHS and were promulgated, through IVHS America, for public comment. Among the other protections that should be enacted at a Federal level include:

- collecting the minimal amount of information necessary to perform IVHS-related functions;
- informing infrastructure users about the data collection, use, and dissemination policies that exist with regard to information identifying them or their vehicle;
- disposing of personally identifiable information no longer needed for IVHS-related uses;
- providing individuals with the means to consent to the use of their personally identifiable information, particularly for non-IVHS uses, or alternatively, prohibiting non-IVHS uses of identifiable information altogether;
- not basing any legal action against an individual solely on data generated by an IVHS application; and

- devising strict rules/procedures for dealing with requests for third party access to IVHS data (mostly for statistical and research use, if other non-IVHS uses are prohibited).

Effective public policy would stipulate that adherence to fair information practices that are ultimately adopted be a prerequisite to the receipt of Federal funding for highways or IVHS programs. The major challenge will be "policing" state and local jurisdictions to ensure compliance. This may be especially contentious, given that these jurisdictions, pressed for revenues, may be tempted to sell some or all of the data within their purview, just as many currently sell their public records.

Additionally, policy should specify that operators of the infrastructure post notices on IVHS roadways that inform the driver that they are being monitored; design onboard IVHS units to indicate when the vehicle is being monitored; and devise strict standards and procedures regarding the interconnectivity and integration of IVHS databases.

Public policy will also need to address the issue of real time pricing, a practice that could place a disproportionate financial burden on poorer populations. It is possible that a solution mitigating the infringement on an individual's autonomy interests may instead infringe on the informational privacy interest. This could happen if a public program is established to qualify people below certain income levels for a transportation system subsidy. In this case, extensive information would likely be required to verify eligibility, which would almost certainly involve considerable data matching.

David Flaherty writes that "the protection of privacy requires the balancing of competing values. Techniques available for legitimate purposes have the secondary effect of being invasive of individuals' perceived right to control their own lives."[41] The sorts of technical and legal solutions laid out above should help ensure the public acceptance of IVHS, while protecting the privacy of individuals in using the infrastructure.

41. Flaherty, *supra* note 26, at 8.