

VEHICLE INFRASTRUCTURE INTEGRATION PRIVACY POLICIES FRAMEWORK

VERSION 1.0.2

LESLIE JACOBSON
ON BEHALF OF
THE INSTITUTIONAL ISSUES SUBCOMMITTEE OF THE
NATIONAL VII COALITION

FEBRUARY 16, 2007

REFER TO THIS DOCUMENT AS “**VII PRIVACY POLICIES FRAMEWORK, VERSION 1.0.2**”

PRIVACY POLICIES FRAMEWORK FOR VEHICLE INFRASTRUCTURE INTEGRATION

Executive Summary

This **PRIVACY POLICIES FRAMEWORK** describes high-level policies that address privacy and personal information issues and scope limits in the context of the Vehicle Infrastructure Integration (VII) Initiative. Additional detailed privacy and personal information policies will augment these initial Framework policies, as the design and operation of a National VII Program become more settled. This Privacy Framework document is divided into four parts: (1) an Introduction that explains the basis both for the VII privacy principles and for the VII scope limits, (2) Definitions of terms used in this **PRIVACY POLICIES FRAMEWORK** document, (3) VII PRIVACY PRINCIPLES and (4) PRIVACY LIMITS ON THE USES OF PERSONAL INFORMATION IN VII. Since a National VII Program remains under development, some of the definitions, principles and limits are subject to refinement in light of changes in the Program over time. This **PRIVACY POLICIES FRAMEWORK** recognizes and reflects the complexity of the many VII functions that will be implemented in both similar and quite different ways by the public and the private sectors that will cooperate in a National VII Program.

Nine VII PRIVACY PRINCIPLES are designed to articulate basic privacy protections in a National VII Program. These are the broadest and highest-level privacy policies intended to govern all aspects of VII. The VII PRIVACY PRINCIPLES begin with the Principle of Respect for Privacy and Personal Information, followed by the Information Purposes Principle, Acquisition Principle, Notice Principle, Fair Information Use Principle, Information Protection and Retention Principle, Openness Principle, Participation Principle and Accountability Principle. These principles emphasize the importance of anonymity secured, in part, through technical methods designed and built into the VII System. The VII PRIVACY PRINCIPLES seek to make sure that individuals who will use VII-equipped vehicles will be able to do so anonymously. Personal information that is used within a National VII Program should be limited to information necessary to carry out an articulated and valid VII purpose. To the extent that personal information is used in a National VII Program, the VII PRIVACY PRINCIPLES emphasize the importance of fair information practices, such as notice and consent, as well as careful protection of personal information and limits on how long personal information will be retained by users and administrators in a National VII Program.

The PRIVACY LIMITS ON THE USES OF PERSONAL INFORMATION IN VII set boundaries with regard to uses and users of VII personal information. The PRIVACY LIMITS are organized according to the functional areas in which the National VII Program will operate. These functional areas include public-sector transportation, public-sector commerce and toll collection, public-sector regulation and commercial vehicle permitting, law enforcement/investigation, public security surveillance, private-sector commerce, and private-sector transportation. The PRIVACY LIMITS emphasize the importance of anonymous options provided by and protected through the technical design of the VII System, as well as operational controls over the National VII Program. Voluntary individual consent and choice with regard to personal information used in, or derived from, a National VII Program are additional privacy values articulated in and protected by the PRIVACY LIMITS. Except for specific public sector regulation and commercial vehicle permitting applications in which personal information is required by law, individuals using VII-equipped vehicles should not be required to supply personal information.

Index

Introduction	3
Definitions	6
Anonymous information	6
Impersonal vehicle data	7
Individual	7
National Vehicle Infrastructure Integration Program (National VII Program)	7
Personal information	8
Personal information subject	8
Personal information user	8
Vehicle Infrastructure Integration System (VII System)	9
VII System administrator (information administrator)	9
Vehicle Infrastructure Integration Privacy Principles	10
1. Principle of Respect for Privacy and Personal Information	10
2. Information Purposes Principle,	11
3. Acquisition Principle	12
4. Notice Principle	14
5. Fair Information Use Principle	15
6. Information Protection and Retention Principle	17
7. Openness Principle	19
8. Participation Principle	21
9. Accountability Principle	22
Vehicle Infrastructure Integration Privacy Limits on Uses of Personal Information	23
Limit 1: Regarding Public-Sector Transportation	24
Limit 2: Regarding Public-Sector Commerce and Toll Collection	25
Limit 3: Regarding Public-Sector Regulation and Commercial Vehicle Permitting	26
Limit 4: Regarding Law Enforcement/Investigation	27
Limit 5: Regarding Public Security Surveillance	29
Limit 6: Regarding Private-Sector Commerce	30
Limit 7: Regarding Private-Sector Transportation	31

Introduction

The goal of this **VII PRIVACY POLICIES FRAMEWORK** is to provide guidance regarding how a National Vehicle Infrastructure Integration (VII) Program should respond to privacy concerns. This **FRAMEWORK**, and the **PRIVACY PRINCIPLES** and **PRIVACY LIMITS ON THE USES OF PERSONAL INFORMATION** contained within it, anticipate that there may need to be modifications to this **FRAMEWORK** over time in response to future changes in the National VII Program, including changes in the VII System technical design and National VII Program operational specifications.

The **PRIVACY POLICIES FRAMEWORK** is the product of an intensive iterative process that began in 2004. Now called the **VII PRIVACY POLICIES FRAMEWORK**, the contents of this document began as two related documents (privacy principles and boundaries) and has carried various titles, most recently “The VII Privacy Document.” Nevertheless, the underlying policies and direction of these privacy protections has remained remarkably constant throughout the extensive development process. The Institutional Issues Subcommittee of the National VII Working Group took the lead in drafting these policies, assisted by the National VII Working Group, as well as the National VII Executive Leadership Team. Gradually consensus formed around the privacy policies expressed in this **FRAMEWORK**. In the future, it is anticipated that additional layers of more detailed privacy guidance (for example, privacy policies for National VII Program management and operational levels) will be added to this overarching framework. Suggestions are welcome with regard to further development and application of these basic privacy policies.

Legal and social concepts of privacy in the Western democratic tradition are based on respect for individual self-determination with regard to personal matters, including information about the individual. In the United States, privacy as a personal right is associated with Louis D. Brandeis, who described privacy as “the most comprehensive of rights and the right most valued by civilized men.”¹ The **PRIVACY PRINCIPLES** and **PRIVACY LIMITS** set forth in this **VII PRIVACY POLICIES FRAMEWORK** focus on protections for personal information² and on fair information practices as they pertain to the National VII Program currently being developed by the National VII Coalition.³ Respect for individual choices about, and control over, an individual’s personal information is the foundation of these **PRIVACY PRINCIPLES** and **PRIVACY LIMITS** intended to guide the technical and operational development of the National VII Program.

The **PRIVACY PRINCIPLES** apply at a general level. The **PRIVACY LIMITS** regarding uses of

¹ Justice Brandeis was dissenting in *Olmstead v. United States*, 277 U.S. 438 (1928).

² There are many definitions of personal information, sometimes also referred to as “personally-identifiable” or “sensitive” information. Linkage with an individual to whom the information refers is central to the concept of personal information. For example, The federal Privacy Act of 1974 provides a standard definition: “Any item, collection, or grouping of information about an individual ... that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” 5 U.S.C. § 552(a) (2005). In contrast, anonymous information or information that has been summarized to the extent that it cannot refer to an individual, is not personal information.

³ The “National VII Coalition” refers to an informal collection of primary stakeholders brought together by the U.S. Department of Transportation to evaluate the feasibility of deployment of a National VII Program. The National VII Working Group and the Institutional Issues Subcommittee of that Working Group are participants in the National VII Coalition.

personal information in and from a National VII Program address specific concerns about appropriate uses of personal information in a National VII Program (such as for toll collection), as well as inappropriate uses (such as for public security surveillance or external vehicle control by law enforcement). If a National VII Program is deployed, the VII PRIVACY PRINCIPLES and PRIVACY LIMITS discussed in this **VII PRIVACY POLICIES FRAMEWORK** will need to be reconciled with existing and future laws and regulations pertaining either directly or indirectly to a National VII Program. This document serves as a statement of intent from which specific rules and policies can be derived for the purposes of governing privacy protection, in the context of a National VII Program.

This **FRAMEWORK** focuses on personal information, as defined in the DEFINITIONS section that follows this INTRODUCTION. Personal information will include data stored or transmitted to or by a vehicle when that data can be associated with a human person, such as the owner, driver or occupant of a vehicle. Such “personal information” raises privacy concerns because it can be linked with an individual person. Within this **VII PRIVACY POLICIES FRAMEWORK**, personal information refers to personally identifiable information, i.e., information about a specific individual person. Examples of personal information include a particular individual’s itinerary, birth date or employer information. Such data is personal information when it can be used to identify, contact or locate a particular individual. Personal information includes an individual’s name, location, addresses or telephone numbers, as well as information that an individual uses to identify herself or himself, such as the individual’s username, password or other customer identifier. In contrast, information that is not personal, in the sense of not being linkable to an individual, is described as anonymous information that is not treated as personal information for the purposes of the **VII PRIVACY POLICIES FRAMEWORK**.

The concept of anonymity, in the VII context, as in other contexts, is flexible and sometimes fluid. Whether information is anonymous or not depends on particular circumstances. As a result, there is rarely a solid divide between personal information and anonymous data. For example, information collected as personal information may be sufficiently aggregated and summarized so that it no longer identifies a particular individual. At that point the information is anonymous. Such data remains anonymous unless or until it again becomes linked or linkable to an individual. Techniques such as data mining and relational databases can take aggregated, anonymous information and link it back to one or more particular identifiable individuals. When such linkage to an individual occurs, anonymous information is transformed back into personal information. Such transformations are often accomplished through correlation of otherwise anonymous, aggregated information with information in other databases that identifies a particular individual. Since aggregated personal information is susceptible to being correlated with other information through data mining and relational database techniques, summarizing personal information (such as through averaging the speeds of several individual vehicles or expressing a mean, median or range of speeds of traffic within a roadway segment at a particular time of day) will provide better assurance of continuing anonymity.

Information regarding only vehicles (as opposed to people) is not usually considered personal information in the United States. Examples include the VIN and vehicle license plate number. However, although a VIN or vehicle license plate number, as such, is generally not considered personal information, once a VIN or vehicle license plate number is associated with an individual (for example, in Motor Vehicle Department records), it may become personal information. For example, it would become personal information when a VIN or vehicle license

plate number is linked back to a registered owner of a vehicle identified by the VIN or to an individual person to whom the vehicle license plate was issued. In a National VII Program, there may be instances where impersonal VII data is linked by an identifier to other data that is personal information. In such a situation, what had been anonymous information in the form of impersonal vehicle data could become personal information regarding an identifiable individual. The Drivers Privacy Protection Act, 18 U.S.C. § 2721 *et seq.*, reflects such concerns about linking otherwise anonymous vehicle information with other information that can be used to identify a particular individual. In the VII context, a partial VIN - at present, the initial digits of the VIN without the last six digits that refer to a unique vehicle - would be impersonal vehicle data, rather than personal information. Such a partial VIN would be considered impersonal vehicle data because these partial VINs reference only a category or model of vehicles. Since partial VINs do not refer to any particular identifiable individual who may own or drive a particular vehicle, they are not considered to be personal information.

This **VII PRIVACY POLICIES FRAMEWORK** recognizes that all information generated by people is not necessarily always personal. Nor is such information always anonymous under all circumstances. When information has been collected as anonymous information, but is later correlated with databases that contain personally identifying information, otherwise anonymous information can be transformed into personal information regarding a particular identifiable individual. A National VII Program will deal with a range of more and less personally identifiable information with potential impacts on the privacy of individuals who will participate in such a Program. As a result, the development of a National VII Program will eventually require more specific rules that apply this general **VII PRIVACY POLICIES FRAMEWORK** to such a Program as it actually operates.

The VII PRIVACY PRINCIPLES and PRIVACY LIMITS contained in this **VII PRIVACY POLICIES FRAMEWORK** are designed to express some of the best current thinking about privacy policies that will assist in keeping a National VII Program in sync with reasonable privacy expectations of individuals who will participate in such a Program. After all, VII safety and mobility goals will come to life only if individuals actually use VII-equipped vehicles and networks. As a result, realizing VII safety and mobility goals will depend in part both on technical design and the operation of a National VII Program in ways that respect the reasonable privacy expectations of individual VII users that are articulated and explained in this **VII PRIVACY POLICIES FRAMEWORK**.

*Professor Dorothy J. Glancy
Santa Clara University School of Law
Consultant to the Institutional Issues Subcommittee of the National VII Coalition*

Definitions

Definitions are essential to understanding the **VII PRIVACY POLICIES FRAMEWORK**. The definitions provided here treat privacy and personal information functionally. Information that is likely to expose individuals to personal risks, such as liability, identity theft, stalking, embarrassment and the like, is treated as personal information. For example, credit card information used to pay road tolls and GPS location data for an identified vehicle is considered personal information that can be used in ways that have potential consequences for an individual.

In contrast, anonymous information, unconnected with an individual who could be exposed to such risks, is not considered personal information in the context of a National VII Program. Similarly, information that relates only to vehicles, such as vehicle diagnostic data that does not reflect on any individual, and would be manifest the same way regardless of who owns or drives the vehicle in question, is not considered personal information. Rather it is defined here as impersonal vehicle data.

Some VII information will be neither completely personal nor completely impersonal, but rather in an intermediate category of information that may become personal depending on the context of its collection and use. In some instances, information from a National VII Program may or may not expose an individual to risks, depending upon the uses that are made of the information. For example, a person's origin-destination information is personal information when it identifies a particular individual. On the other hand, when that same origin-destination data is rendered anonymous, such as through aggregation and summarization, it is no longer personal information so long as identifying information cannot be extracted from or connected with it to again refer to a particular individual.

It is important to note that the principles and limitations described in this document apply to the larger complex of the National VII Program, which includes the physical, technical and functional subsystems and components that receive, transmit, store, and disseminate data and information (see definition of "VII System"), as well as institutional structures and measures implemented to govern VII System users and administrators (see definition of "National VII Program").] In many cases the VII System (the physical structures that collect, transport and deliver data and services between the users) will implement specific technical measures to assure compliance with these principles and limitations, while in other cases this assurance will be achieved through National VII Program governance policies to which VII System users and administrators will be expected to conform.

anonymous information

Anonymous information means data collected, disclosed or used by or through the National VII Program that does not identify or relate to an identifiable individual. Some of the types of anonymous information that will be in the National VII Program include information collected without personal identifiers, personal information that has been stripped of personal identifiers, or aggregated and summarized, and impersonal vehicle data as defined below that relates only to vehicles or vehicle parts, and not to any particular owner, occupant or operator of a vehicle. The essence of anonymous information is that it cannot be linked with an identifiable individual.

Explanation: Anonymous information unrelated and untraceable to any individual is not

“personal information” as defined below. This anonymous information includes impersonal vehicle data (defined below) derived from vehicles and vehicle parts that will be vital to a National VII Program’s important safety and mobility functions.

impersonal vehicle data

Impersonal vehicle data means information collected, disclosed or used by or through the a National VII Program that relates only to the vehicle rather than to any particular owner, operator or occupant, and that cannot reasonably be linked with an individual.

Explanation: Impersonal vehicle data is a form of anonymous information regarding a vehicle or a vehicle part that cannot be associated with a specific individual and does not reflect on the owner, operator, or occupants of a vehicle. Impersonal vehicle data includes a vehicle manufacturer’s proprietary information and systems within a vehicle that generate information about the vehicle, rather than the individual who owns or drives the vehicle. A Vehicle Identification Number (VIN) with the final six digits removed is an example of impersonal vehicle data that is not linked to any particular vehicle. Such a partial VIN identifies a category, type or model of vehicle. Although such impersonal vehicle data is not personal information governed by the VII PRIVACY PRINCIPLES and PRIVACY LIMITS, it is usually good practice to provide information to vehicle purchasers and drivers regarding equipment built into vehicles that can collect and transmit even such impersonal vehicle data generated from a vehicle. Information users should protect impersonal vehicle data from being linked to other data or data systems that might correlate, or associate, such impersonal vehicle data with information that identifies an individual.

individual

Individual refers to a particular, unique human person, as distinct from a group or an entity.

Explanation: Each human occupant, operator or owner of a vehicle is a unique individual. An individual who potentially provides personal information in a National VII Program will be respected as a human person and will be considered an appropriate focus for privacy protection.

National Vehicle Infrastructure Integration Program (National VII Program)

National VII Program refers to the broad complex which, if deployed, would include all physical, technical and functional aspects of the subsystems and components used to collect, receive, transmit, store, and/or disseminate data and information, as well as the institutional structures and measures implemented in order to govern VII System users and administrators.

Explanation: A National VII Program is a hypothetical construct that would exist if a VII System (defined below) were to be deployed. It is broader than the technical system architecture definition of the VII System, because the National VII Program comprehends

institutional structures and measures that would be required to govern deployment of a VII System.

personal information

Personal information means information collected, disclosed, used, or enabled by a National VII Program that can be linked to a particular identifiable individual.

Explanation: Personal information includes several types of data: (i) information *about* an individual (e.g., an individual's location or itinerary); (ii) information that can be *used to identify, contact or locate* an individual (e.g., an individual's name, address, social security number, driver license number and other personal identifiers and identifying information); and (iii) information used by an individual to *identify* herself or himself (e.g., an individual's password, username or other customer identifier). Personal information does not include anonymous information, such as impersonal vehicle data defined above. As noted in the previous introductory section, there will be a range of more and less personally sensitive information that may affect the privacy of individuals using a National VII Program.

personal information subject (also, information subject or subject)

A personal information subject (also referred to as an information subject or subject) is an individual from whom personal information may be collected, disclosed or used by an information user, defined below.

Explanation: This definition focuses on the particular individual who is the source of personal information. Information subjects do not include entities, such as corporations, or tangible objects, such as vehicles, as sources of personal information. For example, in the future if a National VII Program enables vehicles to exchange anonymous positional and other vehicle information to help avoid collisions, the vehicles communicating are not personal information subjects, to the extent that the vehicles communicate only anonymous, impersonal vehicle data and do not communicate personal information associated with an identifiable individual.

personal information user (also, information user or user)

A personal information user (also referred to as an information user or user) is a participant in a National VII Program that collects, uses or discloses personal information, as defined above, from or about an individual who is a personal information subject in such a National VII Program.

Explanation: Participants in the National VII Program that collect, use or disclose personal information transmitted through or by a VII System, are personal information users. To the extent that such users only deal with anonymous information, they are not personal information users included in this definition. In the context of anonymous vehicle-to-vehicle communications, the vehicles are not personal information users to the

extent that they do not communicate personal information.

Vehicle Infrastructure Integration System (VII System)

Vehicle Infrastructure Integration System refers to the technical and functional portion of the National VII Program. This “VII System” is defined in the National VII Architecture as follows: “The VII System is projected as a nationally-deployed collection of enabling infrastructure that provides a variety of services to external users. It includes physical subsystems deployed in vehicles, on the roadside, and located within user facilities to provide new functionality at those respective locations.”

Explanation: The VII System is a technical system, including both hardware and software as well as architectural design, subsumed within the larger National VII Program, which includes the physical, technical and functional aspects of the subsystems and components that transmit, receive, store, and/or disseminate data and information that constitute the VII System, as well as the institutional structures and measures imposed to govern VII System users and administrators.

VII System administrator (information administrator)

A VII System administrator is a person who manages VII System physical, technical, and functional properties in compliance with standards, laws, regulations, and/or policies implemented to govern a National VII Program.

Explanation: A VII System administrator may, in the course of carrying out authorized duties, have access to or control over personal information, or technical processes controlling personal information, during network transport and distribution within the VII System. Such system administration activities are not considered “use” of personal information as described above in the definition of a “personal information user.” Although not an information user, a VII system administrator who has access to or control over personal information within the VII System is nonetheless bound by the applicable privacy policies described in this Framework.

VEHICLE INFRASTRUCTURE INTEGRATION PRIVACY PRINCIPLES

The purpose of these Vehicle Infrastructure Integration (VII) Privacy Principles is to provide general guidance regarding privacy and personal information used in a National VII Program. The nine VII Privacy Principles are designed to reflect fair information practices that will help ensure that a National VII Program is implemented in a way that is properly respectful of reasonable privacy expectations on the part of personal information subjects. These principles were adapted from the privacy principles published in guidelines adopted by the Organization for Economic Cooperation and Development, as well as the National Information Infrastructure Privacy Principles (1995), and are ultimately based on Fair Information Practices (FIPs) widely used in both the public and private sectors. A National VII Program is in the process of development, with the precise roles of various public and private entities as yet undetermined. As a result, these privacy principles are stated in general terms. They express a commitment to respect the privacy and personal information of individuals who will participate in a National VII Program, if deployed.

The VII Privacy Principles discussed here are not implementation rules specifying rights, responsibilities, and enforcement measures within a National VII Program. The **VII PRIVACY POLICIES FRAMEWORK** will later include a variety of implementation privacy rules for a National VII Program. These implementation privacy rules will be developed in the future based on these privacy principles and the privacy laws then-applicable to a National VII Program.

1. Principle of Respect for Privacy and Personal Information

Commitment to respect for individual privacy in a National VII Program means that VII-derived personal information should be acquired, retained, disclosed, and used only in ways that protect the privacy of individuals. Personal information users should collect, retain and use only anonymous information whenever possible. Users of VII-derived personal information and VII System administrators are expected to be accountable with regard to the personal information they collect and/or use in a National VII Program.

This first and most general privacy principle recognizes that VII will flourish only if a National VII Program is designed, built and operated so that personal information subjects are respected and privacy is protected. As the fundamental principle regarding privacy and personal information protection in a National VII Program, this principle reflects the realization that privacy and individual control over personal information deserve to be placed first as the most basic of a National VII Program's privacy principles. This principle emphasizes collection and use of anonymous information that is not linkable to any individual whenever possible. VII technology should be designed so that personal information is only collected or used when necessary. In other words, a deployed National VII Program should rely on anonymous information to the greatest degree possible. Accountability for proper treatment of personal information in the operation of a National VII Program will rest with personal information users and VII System administrators. Reflecting commitment to respect for individuals, this basic principle declares that a National VII Program will protect individual privacy and respect an individual's reasonable privacy expectations.

An individual's reasonable privacy expectations are not just an individual's subjective

expectations of privacy. Such privacy expectations must also be recognized as reasonable by society. The concept of reasonable expectation of privacy under these VII Privacy Principles is not limited by what counts as a reasonable expectation of privacy under the Fourth Amendment of the United States Constitution. In many instances, society has deemed it reasonable to protect privacy at a level higher than that required by the Fourth Amendment. See, e.g., Electronic Communications Privacy Act, 18 U.S.C. § 2701 (1988); Right to Financial Privacy Act, 12 U.S.C. § 3401 (1988); Privacy Act, 5 U.S.C. § 552a (1988); Drivers Privacy Protection Act, 18 U.S.C. §§ 2721-2725; and Federal Communications Law and Regulations protecting wireless communications under 47 U.S.C. § 222. This Principle, and the VII Privacy Principles in general, anticipate that personal information users and VII System administrators in a National VII Program will comply with such existing and future laws and regulations, as well as these privacy principles.

This initial privacy principle is also based on the notion that individual privacy will be best protected when information subjects, information collectors, information administrators, and information users have a shared understanding about how personal information will be acquired, disclosed, and used in a National VII Program.

2. Information Purposes Principle

A personal information user should acquire, use, disclose and retain personal information only for valid purposes, consistent with the goals of a National VII Program, as described in the VII Privacy Limits, below. A personal information user should:

- *inform a personal information subject about the purposes for which personal information will be collected, used or disclosed before collecting personal information from that subject so that the personal information subject can decide whether or not to agree to use of their personal information for those purposes;*
- *use and/or disclose personal information to third parties, only for valid purposes about which the information subject has been informed; and*
- *retain personal information for only as long as the information serves a valid purpose;*
- *limit the storage of personal information to a specified duration that should reflect the period of time necessary to fulfill the purpose for which personal information was collected. (See Information Protection and Retention Principle, below.)*

Acquisition, use, disclosure and retention of personal information should be restricted to serving valid goals. The PRIVACY LIMITS ON THE USES OF PERSONAL INFORMATION that follow these PRIVACY PRINCIPLES, discusses some particular types of valid and invalid purposes for which personal information should and should not be collected, used and disclosed within or by the VII System, or by authorized National VII Program users and VII System administrators.

Before personal information is collected, information users should articulate specific, valid purposes for the use of such personal information collection. As reflected in the Notice and Acquisition Principles, below, personal information users should inform personal information subjects about these purposes and describe all intended uses of personal information *before*

collecting personal information from individuals. If personal information will be disclosed to third parties by a personal information user, any such disclosure should be consistent with the purposes about which the information subject has been informed. These personal information purposes will normally be described at the time personal information is collected when the personal information subject is told about the intended uses and disclosures of his or her personal information.

When information about the purpose of a new use or disclosure has not been provided previously, personal information subjects should be informed of the purposes of any further personal information disclosure or use before such a new type of disclosure or use is made. One reason for such additional explanations of new purposes for personal information is to enable the personal information subject, who may have chosen to opt-in to a particular VII application, to reconsider that choice in light of additional disclosures or uses of his or her personal information. Indeed, information subjects should be given the opportunity to make an informed choice about continuing to participate in an application when the application's purposes for collecting personal information have changed. Where only anonymous information, including summarized or aggregated personal information is to be used or disclosed, no further notice should be necessary. Nevertheless, it is good practice to inform personal information subjects about plans for such aggregation or summarization of personal information when the information is collected.

Encouraging clarity and completeness with regard to valid and announced purposes for collecting personal information from personal information subjects, this principle also fosters several kinds of beneficial privacy practices. Having to explain why personal information is being collected, used or disclosed tends to illuminate and often to eliminate, unnecessary personal information collection. In addition, these announced purposes provide the essential basis for informed consent by the information subject with regard to collection or disclosure of personal information. Moreover, articulation of the purposes for personal information collection provides a restraint against misuse of personal information for other purposes.

From the point of view of individuals who will use VII services and applications, articulated purposes for collecting personal information helps also to foster openness. Articulated purposes also provide assurance that a personal information subject will retain basic choices regarding whether or not to provide personal information.

These purpose requirements are intended to encourage elimination of personal information when there is no longer any valid purpose for keeping it. Retention of personal information after it has served articulated valid purposes that have been explained to the information subjects should be discouraged. (See the Information Protection and Retention Principle, below.)

3. Acquisition Principle

In acquiring personal information, a personal information user should:

- *assess the potential impact on the privacy of personal information subjects;*
- *collect only personal information that is reasonably expected to support current or planned activities; and*
- *collect personal information consistently with valid purposes for information collection (See Information Purposes Principle, above) and the notices that the personal information user has provided to personal information subjects. (See Notice Principle below.)*

Before acquiring personal information, personal information users should assess the potential impact of such information collection on privacy. Personal information collection should be limited to that reasonably expected to support currently planned activities that have been explained in advance to the personal information subjects who will provide personal information. Mere possibility of future use for an undefined potential project would not be a sufficient “planned activity” under this principle.

This Acquisition Principle recognizes that a critical characteristic of privacy is that once privacy is lost, it can rarely be restored. As a result, privacy protection needs to be addressed at the outset, and not merely considered as an afterthought subsequent to personal information acquisition. Under this principle, personal information users and information administrators should explicitly consider impacts on privacy as they design and operate VII networks and applications. Most important, personal information users and information administrators need to take seriously privacy impacts on personal information subjects in deciding whether and how to acquire or use personal information in the first place. It may be that anonymous information is sufficient for identified purposes. In such circumstances, only anonymous data should be acquired or used.

In assessing the privacy consequences of acquiring personal information, personal information users should consider the effects their activities may have on the lives of personal information subjects from whom personal information is acquired. The appropriateness of any particular acquisition or use of personal information will also be affected by other factors, such as public opinion and market forces, as well as the availability of technologies for rendering data anonymous.

Once a personal information user decides to acquire personal information in pursuit of a currently-planned activity, the personal information user should disclose the planned activity in advance to affected personal information subjects so that potential personal information subjects can make informed choices regarding whether to provide personal information. In all cases, a personal information user should use both technical and administrative means to ensure that only that information reasonably expected to support those activities that have been disclosed in advance, in accordance with the Notice Principle below, are acquired. The purposes of the personal information acquisition should both be explained to information subjects and also be consistent with the Information Purposes Principle above.

Some VII applications will involve transactions that require disclosure of personal information. For example, if an individual chooses to purchase a VII navigation-assistance application, personal information in the form of transactional data will be generated that requires disclosure to pre-defined third parties in order to complete a financial transaction. Personal information acquired from such transactions should not be used or disclosed for any other purpose that was not defined and disclosed in advance to the personal information subject participating in the application. (See the Information Purposes Principle, above.) Moreover, VII System administrators who have access to or control over transactional processes for transmitting such personal information are also bound by this principle to the extent that such access and control has bearing on privacy protection.

4. Notice Principle

Before a personal information user collects personal information, the information user should provide effective advance notice to each information subject about:

- *what personal information is collected;*
- *why the personal information is collected;*
- *how the personal information will be used;*
- *what steps will be taken to protect the confidentiality, integrity, and quality of the personal information;*
- *any opportunities to remain anonymous;*
- *the consequences of providing or withholding personal information;*
- *how long the personal information will be retained, and;*
- *rights of recourse and redress. (See Accountability Principle, below.)*

The Notice Principle insists that appropriate prior notice be given to personal information subjects so that information subjects know in advance about personal information collection and how that personal information will be used. Such knowledge allows personal information subjects to make informed choices about whether, when and how to use VII applications that involve sharing information about themselves.

In the context of some opt-in services, the responsibility for providing notice may devolve upon several different personal information users in cases where multiple users are involved in providing the same opt-in service, depending upon the nature of the contractual agreement(s) that govern service provision. If the third party information user has a direct contractual relationship with the personal information subject, such as a bank that has issued a personal credit card to an information subject, then the responsibility to provide notice according to this principle rests with the third-party personal information user (i.e., bank that issued the credit card), rather than with the entity that originally acquired the personal information (i.e., a service provider). If, on the other hand, the third party information user is a sub-contractor to an entity that has contracted with a personal information subject to acquire personal information in order to provide a service, such as a concierge service provider sub-contracted to a vehicle manufacturer to provide services to that manufacturer's customers, then responsibility to provide notice rests with the entity that originally acquires the personal information (i.e., the vehicle manufacturer), rather than with the sub-contracted third-party information user.

Under the Notice Principle, notification about any planned uses of personal information by third parties should be disclosed before that personal information is acquired. (See the Acquisition Principle, discussed above.) To the extent that personal information has been rendered anonymous, such as through aggregation and summarization, no additional notice would be necessary. Since the information has ceased to be personal information, such use of anonymous information would not require additional notification under this aspect of the Notice Principle. Nevertheless, it is good practice to provide notice to personal information subjects regarding known or expected uses of anonymous information derived from personal information provided by information subjects.

This Notice Principle seeks to assure that personal information subjects are given sufficient advance information to make informed decisions about how their personal information will be used. The importance of providing adequate notice cannot be overstated because the content of the notice substantially determines a person's understanding of, and agreement to, how that individual's personal information will be used in a National VII Program. This

understanding, choice and agreement should be respected by all subsequent users of that personal information. Non-personal, anonymous information would, of course, not be so restricted.

This principle specifically applies to personal information in the form of transactional data about individuals generated as by-products of financial transactions. All parties to transactions utilizing personal information derived from or through a National VII Program are expected to abide by this Notice Principle. This Notice Principle applies not only to the party principally transacting with the personal information subject (e.g., in providing a product or service), but also to transaction facilitators such as communication providers and electronic payment brokers who help to consummate financial transactions that make use of a National VII Program. As noted above, the responsibility for providing notice to personal information subjects in cases where opting-into a service requires that personal information be shared among multiple parties may vary, depending upon the nature of the contractual agreement(s) implemented for particular opt-in services.

The Notice Principle suggests some basic elements of adequate notice, but does not prescribe any particular form for that notice. Rather, the Notice Principle sets an objective of ensuring that a personal information subject will have sufficient, understandable information to make an informed decision regarding whether or not to choose a particular application. Ultimately, what counts as adequate, relevant information satisfying the Notice Principle will depend on the circumstances in which the personal information is collected. As a general matter, Notice would be adequate when it provides a personal information subject sufficient information to make informed decisions about whether to agree to use various VII services and applications.

5. Fair Information Use Principle

A personal information user should use personal information about an information subject only in ways that are compatible both with the notice provided by the information user (See Notice Principle above) and with the information subject's reasonable expectations regarding how the personal information will be used.

Personal information users should use personal information only in ways that are compatible with the personal information subject's understanding of and agreement to how it will be used. The Fairness Principle recognizes that a personal information subject's reasonable understanding of how personal information will be used, and the scope of the information subject's consent regarding use of personal information, are determined before the personal information is collected. A personal information subject's informed consent is predicated on advance notice of planned uses being provided by a personal information user. Such understanding and consent will depend both on the notice provided by a personal information user (See the Notice Principle, discussed above) and on information available to the individual pursuant to the Openness Principle, below. This Fair Information Use Principle seeks to limit use of personal information in a National VII Program to uses and purposes disclosed to personal information subjects when they consent to collection and use of their personal information.

Some personal information users may seek to use personal information in a manner inconsistent with information about use that was originally provided when the personal information was collected. In such circumstances, before such changes in the use of personal information can legitimately be made, the information user should first notify affected personal information subjects and obtain their consent to any new use(s) of their information. The nature

of the new use(s) will determine whether such consent should be express or implied. In some circumstances, the consequences to an individual may be so significant that the prospective new data use should proceed only if, and after, the personal information subject has expressly agreed to the new use of his or her personal information. In other circumstances where the new use of personal information has minimal consequences for individuals, a notice offering the personal information subject the ability to impliedly consent to a new use of personal information – for example, by continuing to participate in a VII application after the changed use has been described to the information subject – may be appropriate. The opportunity to cease participation in a VII application (i.e., an opt-out choice), may be adequate in some instances of implied consent. Additional uses of anonymous information (in contrast with new uses of personal information) would of course not require such additional notice.

Because all personal information users should abide by the Fair Information Use Principle, both transferors and transferees of personal information derived from or through the VII System are responsible for ensuring that a personal information subject's understanding regarding limits on permitted uses of the personal information is transferred along with the personal information. Since this principle applies not only to primary personal information users, but also to any subsequent users of the personal information, any use of personal information should be compatible with the personal information subject's understanding of the uses to be made of his or her personal information, based in part on the notice provided under the Notice Principle, above. In determining whether a specific new use of personal information is “incompatible” with the information subject's understanding, personal information users should evaluate whether a particular personal information use was expressly disclosed in the original notice about personal information uses and is otherwise consistent with the notice. Uses of personal information beyond these conditions are incompatible with the Fair Information Use Principle.

The Fair Information Use Principle involves balancing. It will not apply uniformly in every setting. An incompatible use is not necessarily an unfair use; in fact, some incompatible uses may be extremely beneficial to the personal information subject and to society. Some incompatible uses may produce great societal benefits and have at most a trivial effect on the personal information subject or on her or his privacy. For example, in conducting a statistical study that examines traffic safety data in order to develop improved countermeasures, in which no individual information subject is identifiable, use of summarized and aggregated information will result in no impact on any personal information subject or his or her privacy. Such anonymous studies can have significant benefits in terms of improved traffic safety systems and policies. Obtaining the consent of each personal information subject to permit further statistical uses of already existing anonymous data would have no impact on any individual's privacy interests. However, personal information users should inform the personal information subject about potential uses even of such personal information that has been rendered anonymous through aggregation and summarization.

6. Information Protection and Retention Principle

Within a National VII Program, the VII System's technical architecture and structure should be designed to implement advanced security and other technologies to protect personal information against improper collection, disclosure or misuse in ways that may affect the privacy interests of personal information subjects..

Personal information users and information administrators should apply administrative, physical and technical controls appropriate to the protection of personal information derived from or obtained through the VII System. Particular attention should be given to:

- *maintaining the security of personal information;*
- *protecting confidentiality of personal information against improper access; and*
- *assuring the quality and integrity of personal information collected or maintained.*

Personal information users and information administrators should only retain personal information that is relevant to a valid purpose and only for as long as, and to the extent that, the information is protected against improper access, disclosure or use. Personal information users and information administrators should have data storage procedures that assure appropriate, secure disposal of personal information:

- *when there is no longer a valid purpose for retaining the personal information, or*
- *when a stated or required time limit on data retention has been reached, or*
- *when data transmission has been completed within the VII System.*

Identifiers, such as data addresses (potentially identifying a data source) captured during transmission or transport of data within the VII System should not be retained longer than is necessary to accomplish the data transport or transmission.

Personal information users and information administrators should use technical, physical and administrative measures to protect the confidentiality and integrity of personal information. The VII System should be designed so as to limit the potential for problems regarding information quality and security. For example, strong encryption of personal information transmitted through the VII System will greatly reduce risk of unauthorized access, as well as disclosure, alteration, or destruction of personal information.

In addition, not retaining personal information any longer than necessary for valid purposes is a particularly important and useful protection for personal information. These retention limitations apply both to administrative controls on personal information users and to VII System administrators in a National VII Program, and include technical VII System controls that automatically delete personal information that may be incidental to accomplishing data transmission with the VII System. For example, MAC addresses should be deleted promptly at the conclusion of a private service transaction requiring communication through more than one consecutive RSU along a particular vehicle's travel route.

Personal information should be retained only to serve explicit purposes that have been disclosed to information subjects. Retention of personal information for extended period or for other potential purposes is inconsistent with this Information Protection and Retention Principle. Personal information users should adopt time-limits on storage of personal information, inform personal information subjects about such time limits, and abide by them in actual operations.

Robust processes must be implemented by National VII Program users and VII System

administrators to maintain the privacy and integrity of personal information derived from the National VII Program. In determining what controls are appropriate, personal information users and information administrators should recognize an important obligation to manage personal information in a manner that protects it from inadvertent disclosure, as well as from intentional misuse and abuse. Preparations to react quickly and effectively in the event of a security breach should be evaluated in advance. It is likely to be difficult to keep out unauthorized users, such as a hacker or cracker. Such intruders may either seek access to personal information stored in a personal information user's database or make hard-to-detect changes in such data that would then be relied upon in making critical decisions. As a result, risks of potential security breaches should be analyzed on an ongoing basis, and measures taken to minimize threats. In addition to information security threats posed by unauthorized users (i.e., hackers and crackers), information security and privacy protection may also be threatened by authorized VII System users and information administrators. In general, this type of threat is both inherently more detrimental and harder to detect than unauthorized breaches. VII System designers and information administrators responsible for technical information security solutions should therefore avoid the temptation to focus on security solutions that aim to "catch" unauthorized users at the necessary expense of increasing exposure to threats from authorized VII System users and administrators.

In protecting personal information, personal information users and information administrators should adopt a multi-faceted approach that includes both technical and administrative controls, as well as physical security. Among important technical controls, personal information users and information administrators should encrypt personal information whenever possible. In addition, administrative controls, such as computerized audit trails, should be implemented to help detect and eliminate any improper access to personal information. Employees with access to personal information should be appropriately trained in proper data handling and management techniques, and be carefully supervised to prevent inadvertent or deliberate lapses. Personal information users should establish policies that clearly forbid the use of personal information acquired for one activity from being used for another, unrelated activity as stated in the Purposes Principle, above. Regular data storage limitations and disposal procedures should similarly restrict how long personal information is retained.

Personal information should be of sufficient quality to be relied upon for purposes that may have consequences for personal information subjects, personal information users or both. This means that personal information should be accurate, timely, relevant and complete for the purposes and uses for which it was collected and about which information subjects have been notified as contemplated in the Notice Principle, above. Maintaining only relevant personal information is particularly important in preventing the pernicious tendency for data acquisition to spawn "mission creep." The fact that personal information collected for one purpose could also be useful in serving other possible purposes does not justify retaining personal information for later uses serving new purposes that have not been explained in advance to personal information subjects. Any such expansion of use would be inconsistent with both the Notice Principle and the Purposes Principle discussed above.

In a National VII Program, both personal information subjects and personal information users, should be able to rely on the integrity of personal information derived from the Program. Thus, personal information users should protect personal information against improper alteration or destruction either by employees of personal information users or by unauthorized intruders into information systems containing personal information derived from the National VII Program. Similarly, VII System administrators should protect personal information against

improper alteration or destruction that may result from inadvertent or malicious intervention into data management processes during data transport within the VII System. Advance planning to prevent, detect and eliminate every intrusion or attempted data alteration will be an important responsibility of personal information users and information administrators. Providing information subjects with access to information that is collected and stored about them (See the Participation Principle below) is one effective means to ensure integrity and quality of personal information used in a National VII Program.

7. Openness Principle

Personal information users and information administrators:

- *should be informed about privacy issues and the best ways to protect personal information derived from the National VII Program;*
- *should inform prospective personal information subjects about personal information the personal information user collects through the National VII Program; and*
- *should explain to personal information subjects protections for personal information derived from National VII Program, and the length of time personal information will be retained by the personal information user.*

Personal information subjects should be able to rely on personal information users for adequate information about:

- *the nature and extent of personal information collected from them;*
- *the purposes for which such personal information is collected;*
- *the uses of personal information made by personal information users;*
- *the opportunity not to provide personal information;*
- *the protections for confidentiality, integrity, and quality of personal information;*
- *the consequences of providing or withholding personal information;*
- *opportunities to remain anonymous; and*
- *rights of recourse and redress for misuse of personal information. (See Accountability Principle, below.)*

The Openness Principle addresses the need for transparency in a National VII Program. Personal information users, information administrators, and personal information subjects need to be able to make informed decisions regarding what personal information is collected and used, and how it will be protected within the National VII Program. Such transparency with regard to personal information practices helps to reassure personal information subjects that their privacy interests are understood and reasonably protected through the National VII Program design, security, access policies, and other measures. Openness is intended to encourage personal information users and information administrators to adopt coherent privacy protection processes and policies that users have articulated both internally and in communications to personal information subjects who participate in a National VII Program. In doing so, personal information users should seek current, reliable information about potential privacy issues and the best ways to maintain the privacy of personal information.

Traditionally, government has educated the public regarding matters of rights and responsibilities. If a National VII, Program is deployed, government agencies will continue to

play a leading educational role. However, as design and implementation participants in a National VII Program, the private sector also has a crucial role in informing information users, information administrators, and personal information subjects about privacy issues. Typical opportunities for education designed to help information subjects understand personal information practices in a National VII Program should involve Internet privacy “help” sites and published privacy compliance guidelines. Comprehensive marketing and publicity campaigns should provide clear explanations by National VII Program information users of how they deal with personal information. The overall goal of the Openness Principle is to assure that personal information users, information administrators, and personal information subjects remain well-informed and up-to-date regarding privacy issues, including effective privacy protection strategies within a National VII Program.

Since all possible privacy consequences of use of personal information in a National VII Program cannot be anticipated, personal information subjects may not initially be aware of how their lives could be affected by personal information collected in such a Program. As a result, it is important that personal information subjects, information administrators, and personal information users continue to engage in a shared understanding of how a National VII Program affects personal information privacy.

A personal information user should inform each personal information subject about all of the ways in which that information subject’s personal information is collected and used by the personal information user. Similarly, each personal information subject also has the responsibility to understand the consequences of providing personal information in the course of using VII applications. For example, a VII toll collection authority may ask for personal information prior to permitting a customer to participate in electronic toll payment systems. In such a situation, one use for the personal information is clear – to process toll payments. To the extent that other uses are intended by the toll authority that are not so obvious, such as to generate traffic management data, those other uses need to be brought to the attention of the information subjects, as well. Similarly, use of information about a toll customer’s itinerary to contribute to an anonymous data base for highway planning purposes should be disclosed before the personal information from the toll authority is used for such a purpose. However, additional uses of already anonymous data, that no longer contain personal information, need not be repeatedly explained.

The Openness Principle is intended to make it possible for a personal information subject to actively shape the terms of his or her participation in a National VII Program. In general, when a personal information subject chooses whether and to what degree to participate in a VII application requiring disclosure of personal information to a personal information user, the information subject should take an active role in learning about the terms of such disclosure. Of course, if personal information subjects are to be responsible for their choices, they must be provided sufficient information to make informed decisions, including the potential decision not to participate in a VII application because it requires disclosure and use of personal information. This Openness Principle works in conjunction with the Notice Principle, above, to enable a personal information subject to take responsibility for whether or how his or her personal information will be disclosed and used in a National VII Program. The overall goal of this principle is to make uses of personal information clear so that each information subject has an opportunity to understand and evaluate the benefits and potential risks of choosing among VII applications and services, or of making the choice not to participate in applications that require personal information from them.

8. Participation Principle

In addition to receiving information regarding how personal information is collected and used in a National VII Program, each personal information subject should be expected to protect his or her own privacy. Personal information users should provide each personal information subject opportunities to:

- *access personal information about himself or herself;*
- *correct any inaccurate personal information about the personal information subject;*
- *object to improper or unfair personal information use; and*
- *choose to remain anonymous, and not provide personal information.*

Personal information subjects should participate in the protection of their own privacy. That means that a personal information subject needs to be given notice of personal information collected from or about him or her (See Notice Principle, above.), as well as access to the information subject's personal information held by a personal information user. A personal information subject should also be able to correct his or her personal information to the extent that it is demonstrated to be inaccurate. A personal information subject should also have the opportunity to object to improper or unfair use of his or her personal information. The nature of the means provided by a personal information user to enable a personal information subject to have access to, and the ability to correct, his or her personal information should depend on various factors, including the seriousness of the consequences to the information subject of continued use of erroneous personal information.

As a general matter, personal information subjects should have the opportunity to avoid personal information collection by remaining anonymous in their uses of a National VII Program. However, as explained in Limit 3, below, in some public-sector regulation and commercial vehicle permitting applications personal information may be required because of legislative or regulatory mandates. As a result, although anonymity is normally appropriate when a vehicle driver or occupant seeks, for example, information about nearby restaurants or parking facilities from a VII service provider, anonymity might not be possible under certain commercial vehicle applications, such as hazardous materials permits, for which personal information is required by law. In other VII services and applications, choice should be the rule with regard to providing personal information.

9. Accountability Principle

A personal information user should respond to inquiries and complaints about interference with privacy interests or misuse of personal information, including use of personal information in ways that are incompatible with notice provided to information subjects (see Notice Principle, above). If an information subject has a complaint that he or she has been harmed by improper collection, retention, disclosure or use of his or her personal information by a personal information user, the information subject should have appropriate means to raise and resolve the complaint.

Personal information users should provide appropriate means for personal information subjects to raise privacy issues and to make complaints regarding interference with privacy interests. This Accountability Principle contemplates an internal process compatible with the operations of the personal information users. The implementation of privacy officers or boards, as well as other strategies, can be useful ways to carry out such privacy recourse functions. However implemented, an information user should provide an identified person or office that can respond formally and try to resolve privacy problems and complaints by personal information subjects.

This Accountability Principle does not determine whether improper action or harm has occurred in any particular instance or whether any specific form of resolution is required. Complaints from personal information subjects should be taken seriously when they involve claims that harm was suffered because personal information was misused, or was not accurate, timely, relevant, or complete, or was retained for longer than necessary. Providing resolution of complaints in the most timely and cost-effective manner should be the goal.

VEHICLE INFRASTRUCTURE INTEGRATION PRIVACY LIMITS ON USES OF PERSONAL INFORMATION

Much of the success of the Vehicle-Infrastructure Integration (VII) initiative will depend on the institutional and policy issues that affect technical approaches and solutions for implementation of a successful National VII Program. The policies discussed here are intended to serve as the basis for operational rules incorporated into a National VII Program and/or for potential enabling legislation or regulation that may precede the deployment of a National VII Program.

Earlier discussion within the National VII Coalition identified the following issues that should be addressed as key areas of focus:

What are the limits on the use of personal information and the functions that will be allowed in a National VII Program?

- Will real-time video/voice recording of occupants be allowed by either the public or private sectors?
- Will the VII System allow the association of precise vehicle identification numbers (VIN) with location to enable:
 - (in the case of public-sector use) *post facto* traffic or criminal law enforcement and surveillance (including anti-terrorism and Homeland Security activities)
 - (in the case of public-sector use) automatic crash or incident notification
 - (in the case of public and private sector use) providing consumer-specific services
 - off-board vehicle control
 - (in the case of public-sector use) preemptive law enforcement
 - (in the case of private sector use) automated crash prevention/mitigation

These privacy limits respond to these questions by setting boundaries on the use of personal information that is collected, or enabled to be collected, by or through a National VII Program. Applied early in the planning process, these limits clarify intentions regarding personal information in broad terms, and help to allay common privacy and civil liberties concerns. As policy provisions that will determine system requirements, these privacy limits also assist in framing the context in which technical, business, and policy solutions to such concerns will be addressed by the National VII Coalition. Eventually, there may be a national policy debate culminating in legal authorizations and possible restrictions with regard to some of these issues.

These privacy limits are designed to help shape policy debates both within the National VII initiative and more broadly in governmental decision making about a National VII Program. From the standpoint of public policy, they set appropriate limits for the use of personal information in a future deployed National VII Program. Respect for these limits would be essential for the successful deployment of a National VII Program that is socially and politically acceptable to the American public. These limits also help to narrow the range of policy issues that remain to be addressed by the National VII Coalition in the course of undertaking a deployment feasibility analysis for a National VII Program. Were a decision made in the future to change these limits, additional analysis would be required to reassess the implications for privacy protection in such a Program.

There are seven areas in which privacy limits on the uses of personal information in a National VII Program will be discussed below:

1. Public-sector transportation
2. Public-sector commerce and toll collection
3. Public-sector regulation and commercial vehicle permitting
4. Law enforcement/investigation
5. Public security surveillance
6. Private-sector commerce
7. Private-sector transportation

It is important to keep in mind the primary goals of the National VII initiative. The driving forces behind this initiative are safety and mobility. The two primary goals of a National VII Program are to enhance crash prevention/mitigation and to collect and disseminate information that will provide mobility benefits. Safety and mobility applications include intersection collision avoidance, real-time warnings and alerts, weather data collection to support travel information and snow-and-ice control decision-making, as well as overall enhanced traveler information services. In addition to safety and mobility, a deployed National VII Program may also support a range of convenience and productivity applications, such as electronic payments for road tolls, fuel and food, as well as other commercial vehicle services. The Federal Communications Commission's authorization for use of the DSRC spectrum notes that these convenience and productivity applications are allowed to share use of the DSRC spectrum on a lower-priority basis in real-time, relative to public safety applications.

1. Public-Sector Transportation

One of the primary uses for VII data will be to enhance transportation functions, such as real-time safety applications, traffic data collection and public-sector information dissemination, and traffic and transportation management functions. Data are envisioned to be used for implementing a range of real-time crash avoidance and mitigation applications, and for deriving travel time, speed, and anonymous point-to-point information. Public-sector agencies will use VII data for a range of public purposes, including to generate and disseminate traveler information through traditional delivery mechanisms, such as websites, 511 systems, highway advisory radio (HAR), and dynamic message signs (DMS). Many agencies are likely to also use the VII System to disseminate information directly to travelers in their vehicles by sending messages to all vehicles in a particular area through specific road-side units. Eventually, direct dissemination to vehicles via a VII System may even replace the need for HAR and DMS.

Travel time, speed and anonymous point-to-point information is critical to transportation system performance measurement and for planning and designing transportation infrastructure. It is also important as a source of real-time information to be used in improving roadway safety, operating transportation facilities and enabling the public to make more informed travel decisions. Such information is generally seen as high value, not only within the transportation

profession, but by the traveling public as well. However, privacy concerns are likely to be raised by the public regarding storage and use of personal information derived from a National VII Program, especially if individual travelers or vehicles can be identified in the data.

The value of the VII data to transportation professionals is in using the data to describe the quality and characteristics of traffic flow and real-time conditions on particular roadways. Such information helps to facilitate improvements in transportation safety and mobility. Data used for these purposes that do not include personal information meet the transportation function needs and ensure that potentially sensitive information about an individual driver, passenger, or vehicle will not be captured or released. The National VII Program limit for public-sector transportation can be stated as:

Limit 1 *For the public-sector transportation functions discussed above, public sector entities that are VII data users may collect and retain only anonymous safety- and traffic-related data derived from the National VII Program, and vehicle operator/owners shall not be required to provide personal information for such functions.*

Rationale: The public-sector transportation functions mentioned above do not require that public-sector agencies collect and retain personal information. Ranges of functional characteristics of transportation routes are important, but can be described using anonymous data aggregated and summarized for statistical purposes. Because there is no need for public-sector agencies to receive or retain personal information for these transportation functions, acquiring such information would not be permissible. This rationale is consistent with the guidance contained in the “Data Acquisition Principle” of the VII Privacy Principles.

Limiting data collection in this category to anonymous data, only, allays the concern that data passed automatically from vehicles to the public sector from all VII-equipped vehicles could otherwise be used to trace or track particular vehicles historically or in real time.

2. Public-Sector Commerce and Toll Collection

The public sector already offers some commercial-like services, such as electronic toll collection and traveler information. Currently,⁴ toll authorities must be able to identify individual vehicles or tags and have the ability to debit personal toll accounts appropriately. By opting to use electronic toll collection, the vehicle owner or driver chooses to allow the toll agency to generate toll tag data. Personal information should be used only for the purposes that are explicitly stated when an individual signs up for electronic toll collection.

Some road-pricing strategies are essentially outgrowths of electronic toll collection. High-occupancy toll (HOT) lanes and congestion-pricing apply the concepts of electronic toll collection to high-occupancy vehicle (HOV) facilities, specific corridors, or regions. Travelers have a choice of whether to use the priced facility or to travel in the more congested “free” lanes. By opting to use the priced facility, the driver chooses to allow the agency to generate toll tag data. As in electronic toll collection, personal information should be used only for the purposes that are explicitly stated when an individual signs up for participation in the toll program.

Electronic toll collection technologies may also allow road use taxes to be collected electronically. There has been much discussion about collecting road use taxes electronically in

⁴ It should be noted that anonymous payment options are expected to be enabled through a National VII Program, which may obviate the need to collect personal information for the purposes of making electronic payments.

lieu of gas taxes, and some pilot studies have gotten underway in the United States to examine the feasibility of such an approach. However, there have been no decisions about implementing these strategies anywhere in the country yet. Some of the proposed approaches include clear ways to protect privacy, while others do not. It is too early in the discussion to know if road use taxes will rely on VII technology and, if so, how privacy concerns would need to be addressed. Although road use tax discussion has evolved from electronic toll collection, these two applications differ significantly in that road use taxes, if implemented, would be required by law. If a National VII Program were used to collect road use taxes, this application would fall under Public-Sector Regulation and Commercial Vehicle Permitting, described in the following section.

Other public-sector commerce applications will undoubtedly arise that will make use of the National VII Program. These applications should not necessarily be excluded, but individuals should be able to choose whether or not they want to participate in these applications. If an individual chooses to participate, the public-sector agency should provide specific information about how personal information collected for this application will be used. Personal information should not be used for any purposes outside those required for the specific application(s) for which the individual applies. The National VII Program limit for public-sector commerce can be stated as:

Limit 2 *For public-sector commerce purposes, public sector entities that are personal information users may collect and use personal information derived from the National VII Program to the extent that personal information subjects have provided consent. Personal information held by public agencies shall be protected by agency privacy policies and present or future privacy protection laws.*

Rationale: Although the public-sector commerce functions mentioned above currently necessitate that the public-sector agencies collect and retain personal information, the information collected and retained should be limited to that which is required by the specific applications in which vehicle owners, operators, and other personal information subjects have chosen to participate. Additional information is simply not needed and should not be collected or retained. In order for people to make an informed choice regarding the applications or programs in which they want to participate, the personal information collected and the uses allowed must be explicitly stated. This rationale is consistent with the emphasis on anonymity and respecting individual choice with regard to providing personal information contained in the VII Privacy Principles.

3. Public-Sector Regulation and Commercial Vehicle Permitting

There are a variety of potential regulatory or commercial vehicle permitting VII applications that have been identified. Commercial vehicle regulation and permitting examples include automated weigh station operations and permits to haul hazardous materials. A National VII Program provides the ability to accommodate existing commercial vehicle tag applications along with all of the other VII applications, such as electronic toll collection and traveler information. These commercial vehicle regulation and permitting applications should be encouraged to use a National VII Program. As mentioned under public-sector commerce above, individual operators or companies should be able to choose to take advantage of these

applications or programs where appropriate. However, the critical nature of some applications, such as hauling hazardous material, are so important that government agencies require collection of personal information and should be allowed to require use of VII technology in order to obtain a permit or pay commercial use taxes. Only when specific laws or regulations require the use of a National VII Program for these applications should the Program collect personal information on a mandatory basis. In the absence of legal or regulatory requirements, some regulatory agencies may potentially offer this type of VII application as opt-in with regard to providing personal information.

Whether the regulatory or permitting process requires the use of VII technology or allows operators to choose to participate, the public-sector agency responsible for the regulation or permitting must provide specific information about how personal information will be used. Personal information should not be used for any purposes other than those required for the specific application(s) for which the individual applies. The National VII Program limit for public-sector regulation and commercial vehicle permitting can be stated as:

Limit 3 *For public-sector regulation and commercial vehicle permitting purposes, public sector entities that are personal information users may collect and use personal information derived from the National VII Program to the extent that a personal information subject has provided consent, unless the nature of the regulation (e.g., legal requirement) or permit requires uniquely-identifiable vehicle information for specific applications. In these exceptions, the personal information shall only be used for explicitly-stated purposes that are necessary for the required application. Personal information held by public agencies shall be protected by agency privacy policies and present or future privacy protection laws.*

Rationale: Public-sector regulation and commercial vehicle permitting programs are designed to enhance safety and improve commerce. A deployed VII System can facilitate the implementation and operations of such regulations and permitting programs, thus easing the administrative burdens imposed on authorities managing, as well as those subject to, these programs. Although public-sector regulation and permitting functions mentioned above may require that public-sector agencies collect and retain personal information, such information should only be collected and retained if it is required by the specific applications in which vehicle owners, operators, and individuals have chosen to participate, or as required by law. Additional information should not be collected or retained and the information collected and the uses allowed must be explicitly stated.

4. Law Enforcement/Investigation

A major concern voiced by privacy and civil liberties advocates (as well as others) is the potential use of VII System to gather information for law enforcement (e.g., to issue citations for traffic violations or to preempt violations through off-board vehicle control) and for investigation purposes (e.g., crash investigation). A VII System could also potentially provide information on criminal wrongdoing unrelated to travel. The potential use of a VII System as a surveillance tool for law enforcement is a highly-controversial issue. Were a National VII Program to be proposed that would use a VII System as a surveillance tool for law enforcement purposes, concerns with regard to privacy and civil liberties would be raised by the public and its

representatives and advocates, which would threaten the implementation of such a Program. The primary purposes of VII are to enhance transportation safety and mobility through improving driver situational awareness, to help avoid and/or mitigate crashes and to use technology to optimize anonymous traffic monitoring and control strategies. The program is being developed, and policy-makers are making decisions, with these purposes in mind. To expand the program beyond these purposes to include punitive uses of the VII System for enforcing traffic or other laws would cast doubt regarding the true intent of the initiative. If a National VII Program were used to facilitate or automate enforcement, many would likely seek ways to disable the VII communications system on their vehicles, or to purchase or retain an older, non-VII-equipped vehicle. This would negatively impact not only their safety, but also the safety of other road users, because a VII-disabled or non-equipped vehicle would no longer be sending or receiving safety data. There are other transportation efforts, outside of the National VII initiative, that are designed specifically to address enforcement, without invoking the risks discussed above. One such non-VII program uses cameras to enforce red-light violations. The issues surrounding gathering electronic information for law enforcement and investigation purposes are better discussed in forums about such targeted programs.

Early in the National VII initiative, participants in the National VII Coalition agreed that law enforcement- and investigation-related functions would not be directly supported by the program. This limit reinforces that agreement. In essence, a similar principle is at work in this area as discussed above under public-sector transportation. Anonymous data is the only data that should be released for law enforcement or investigation purposes, without a warrant (or its equivalent). Such anonymous National VII Program-derived data can be used by law enforcement personnel to identify areas where traditional law enforcement mechanisms can be better targeted. However, such data cannot be used to impose sanctions on individuals for past infractions, nor be used to prevent infractions by implementing off-board vehicle controls.

Two of the questions posed at the beginning of this section are germane to the law enforcement and investigation area:

- Will real-time video/voice recording of occupants be allowed for law enforcement or investigation purposes?
- Will the VII System allow the association of precise vehicle identification numbers (VIN) with location to enable off-board vehicle control for preemptive law enforcement purposes?

Based on the above discussion, the answer to both questions is no. The National VII Program limit for law enforcement and investigation can be stated as:

Limit 4 *No specific information about an individual or vehicle shall be derived from the National VII Program to be used for law enforcement or investigation purposes without a valid warrant (or its equivalent). However, anonymous data may be collected and used by law enforcement to, for example, assist traditional law enforcement efforts or to analyze transportation problem locations. Specifically, the National VII Program shall not be used by law enforcement for:*

- *recording real-time video or voice of vehicle occupants, or*
- *associating precise vehicle identification numbers (VIN) with times or locations, or,*
- *off-board control of vehicle driving or maneuvering functions.*

Rationale: If a National VII Program were designed as a tool of law enforcement and investigation, significant concerns over privacy and civil liberties would be raised. In the case of use of a National VII Program for law enforcement purposes, few would find pervasive automation of enforcement an acceptable approach, especially for traffic laws. In the case of automatic collision investigation, it is worth noting that the federal government estimates that over 40% of all collisions occurring on public roadways currently go unreported to authorities and a recent study of naturalistic driving⁵ found the rate of unreported collisions to be over 80%. Given this, it would be both costly and unpopular to force persons into the legal system who are otherwise willing and able to manage the consequences of such collisions privately. These concerns would likely be significant enough to threaten successful deployment of a National VII Program, thus jeopardizing the safety and mobility benefits for which such a Program was envisioned and is being designed. On the other hand, anonymous transportation data that does not identify individuals should be as available to law enforcement agencies as it is to other types of agencies.

It should be noted that, due to the risks described above regarding a predictable desire on the part of many to avoid enforcement liability if enabled through a National VII Program, the future durability of this law enforcement limit is important to the continued viability of the VII program. Were a National VII Program implemented by the US Congress by a statute that codifies this limit on law enforcement, but later reversed by a new act of Congress, public and stakeholder support for such a Program would be jeopardized.

5. Public Security Surveillance

Security concerns have intensified since the terrorist attacks in 2001. Some have suggested that a National VII Program could be used to gather information on, and track movements of, suspected terrorists or others who may pose a security threat. As with law enforcement and investigation, use of a National VII Program as a tool for homeland security surveillance would likely be very controversial and could threaten successful deployment of a National VII Program, thus jeopardizing the benefits for which such a Program is being designed.. A National VII Program is being developed specifically to support safety and mobility improvements, not to enhance homeland security. A National VII Program will not be designed as a tool of national security, homeland security, or anti-terrorist agencies who might otherwise want to use such a Program to track specific individuals or vehicles. As such, anonymous data are the only data that should be released without a warrant (or its equivalent), even for homeland security purposes. In the future, specific legislation may be necessary to restrict intelligence gathering activities using a National VII Program. The National VII Program limit for security surveillance can be stated as:

Limit 5 *The National VII Program and VII System will not be designed to gather specific information about an individual driver, occupant, or vehicle for national security, homeland security or anti-terrorist surveillance purposes.*

⁵ Neale, V.L., Dingus, T.A., Klauer, S.G., Sudweeks, J., (Virginia Tech Transportation Institute) and Goodman, M, (National Highway Traffic Safety Administration) *An Overview of the 100-Car Naturalistic Study and Findings* (2005). NHTSA Paper No. 05-0400, at 10.

Rationale: If a National VII Program were designed as a tool of national security, homeland security and anti-terrorist agencies, significant concerns over privacy and civil liberties would be raised. Due to the pervasive nature of the National VII Program under contemplation, combined with our highly-mobile society, were VII to be used for homeland security surveillance purposes, it would raise the specter of totalitarian governance. These concerns would likely be significant enough to threaten successful deployment of a National VII Program, thus jeopardizing the safety and mobility benefits for which such a Program is being designed. As noted earlier with regard to access by law enforcement agencies, anonymous data that cannot be used to identify individuals should be available to public security agencies.

6. Private-Sector Commerce

A variety of commercial services are envisioned that will be enabled by VII technology. traveler information, fleet management, enhanced and targeted yellow pages services, reservation services, business services, concierge services, ePay / eBuy, and enhanced trip planning and route guidance are just a few of the possibilities. Most, if not all of these services will be available only through a subscription (i.e., a voluntary contract between service providers and recipients stipulating terms, conditions, and payment), and thus will require participants to “opt in” to the service. Part of this subscription process will inform subscribers about the personal information to be collected and purposes for which their information will be used. Vehicle owners will need to choose to take advantage of those services in order for their personal information to be used. Personal information obtained from vehicles that may be communicating with the infrastructure for the purposes of providing such subscription-based services should be treated essentially the same way as that described above regarding public-sector commerce functions. Just as in public-sector commerce, the collector of personal information, in this case a private company, should provide customers with the choice of whether to participate, and, if so, with specific information about how such information will be used. Personal information should be used only for the purposes that are explicitly stated when an individual subscribes to the selected applications. The National VII Program limit for private-sector commerce can be stated as:

Limit 6 *For private-sector commerce purposes, private sector entities that are personal information users may collect and use personal information derived from the National VII Program to the extent that personal information subjects have provided consent. Personal information held by private entities shall be protected by privacy policies and present or future privacy protection laws.*

Rationale: In order to preserve privacy, personal information subjects must be allowed the opportunity to choose whether to participate in applications that collect personal information. (They must first be informed about how such information will be used and if it will be retained or disclosed.) Personal information subjects must be informed of the intended uses of their personal information in order to be able to make a valid and informed choice. Any use of personal information outside that which was agreed to would be a breach of trust that could threaten the credibility of a National VII Program, and is thus forbidden.

7. Private-Sector Transportation

Private-sector companies are expected to offer a variety of services not covered under the private-sector commerce section above. These services will include real-time safety applications, and may include general vehicle diagnostic notifications and recall management. These services would not include vehicle-specific information, which involves the exchange of personal information; such vehicle-specific services would fall under Limit 6 above. These services will include real-time safety applications, and may include general vehicle diagnostic notifications and recall management (not to include vehicle-specific information, which involves the exchange of personal information). Vehicle manufacturers will be the primary providers of these services. These applications generally need to be implemented on a fleet-wide basis in order to be effective, and would be compromised in their effectiveness if not all vehicles were enabled with these services. For this reason, they are not expected to be offered as “opt-in” services, but could be made available to all users of VII-equipped vehicles, regardless of whether the owner or operator has contracted for specific commercial or regulated services. These private-sector transportation applications will not require or use personal information. (Any private-sector applications that do require personal information will require informed consent by the personal information subjects, as described by the private-sector commerce section above.) The National VII Program limit for private-sector transportation functions can be stated as:

Limit 7 *For the private-sector transportation functions, private sector entities that are VII data users may use only non-personal information derived from the National VII Program (e.g. impersonal vehicle data) and vehicle operator/owners shall not be required to provide personal information for such functions.*

Rationale: The real-time safety applications in this category provide transportation benefits to all road users, which should not be denied by those who choose not to enter into specific, subscription-based agreements for commercial services. Private-sector transportation applications will be categorically defined by a National VII Program operational entity.