

Technical Memorandum No. 3.7

Florida's 2003 Intelligent Transportation System Strategic Plan Update

The Florida Department of Transportation Intelligent Transportation Systems' Information Privacy Policy

February 24, 2005
Version 2



Prepared for:

Florida Department of Transportation
Traffic Engineering and Operations Office
Intelligent Transportation Systems (ITS) Section
605 Suwannee Street, M.S. 90
Tallahassee, Florida 32399-0450
(850) 410-5600

*Technical Memorandum No. 3.7 – Florida’s 2003 ITS Strategic Plan Update
The FDOT ITS’ Information Privacy Policy*

DOCUMENT CONTROL PANEL		
File Name:	<i>Technical Memorandum No. 3.7: Florida’s 2003 ITS Strategic Plan Update – FDOT’s ITS Information Privacy Policy</i>	
File Location:	W:\ITS Program\ITS GC\TWO25-StrategicPlanUpdate\TM3 - Issue Papers\TM3-7 - Information Privacy\050224 TWO25 TM3-7 V2.pdf	
Deliverable Number:	3.7	
Version Number:	2	
	Name	Date
Created By:	Joe Schuerger, PBS&J	May 18, 2004
Reviewed By:	Diane E. Quigley, PBS&J	May 18, 2004
	Diane E. Quigley, PBS&J	July 26, 2004
Modified By:	Dave Hodges, PBS&J	May 25, 2004
	Pamela L. Hoke, PBS&J	July 8, 2004
	Dave Hodges, PBS&J	December 28, 2004
	Pamela L. Hoke, PBS&J	February 16, 2005
Completed By:	Pamela L. Hoke, PBS&J	February 24, 2005

Table of Contents

List of Appendices	iii
List of Tables	iii
List of Acronyms	iv
1. Introduction	1
2. Background	2
3. Information Privacy Issues in Florida	3
3.1 Privacy.....	3
3.2 Data Privacy and Security	4
3.3 Data Ownership	4
3.4 Data Usage.....	5
3.5 Public-Sector Competition with Private-Sector Partners.....	5
3.6 Access and Security	5
3.7 Archived Data	6
3.8 Information Accuracy.....	6
3.9 Liability.....	6
4. Information Privacy in Federal and State Policies.....	7
4.1 Other State Legislation	8
4.2 Initial Actions for the Florida Department of Transportation’s Intelligent Transportation Systems Section.....	9

List of Appendices

Appendix A – The ITS America Fair Information and Privacy Principles

List of Tables

Table 4.1 – Relevant 2003 Intelligent Transportation Systems’ Information
Privacy Legislation.....8

List of Acronyms

§.....	Section
AB.....	Assembly Bill
Assm.	Assemblyman
CCTV.....	Closed-Circuit Television
D.....	Democrat
ETC.....	Electronic Toll Collection
FBI.....	Federal Bureau of Investigation
FDOT.....	Florida Department of Transportation
<i>FOIA</i>	<i>Freedom of Information Act</i>
HB.....	House Bill
ITN.....	Invitation to Negotiate
ITS.....	Intelligent Transportation System
ITSA.....	Intelligent Transportation Society of America
NCSL.....	National Conference of State Legislatures
<i>NITSA</i>	<i>National ITS Architecture</i>
R.....	Republican
Rep.....	Representative
RFP.....	Request for Proposal
SB.....	Senate Bill
Sen.....	Senator
TEOO.....	Traffic Engineering and Operations Office
USC.....	United States Code
USDOT.....	United States Department of Transportation

1. Introduction

The collection, analysis, fusion, and dissemination of information is one of the primary roles of intelligent transportation systems (ITS). The accurate and timely dissemination of this information creates value for individuals, the traveling public, and those agencies that manage transportation using ITS components. The primary focus of this information is to improve travelers’ safety and security; reduce travel times; and enhance individuals’ ability to deal with highway incidents and events. Travel information is collected from many sources, some from the infrastructure and some from vehicles, while other information may come from transactions – such as electronic toll collection (ETC) – that involve interaction between the infrastructure and a vehicle. As with all forms of advanced information technologies, the privacy of individuals must be respected at all times.

The purpose of this *Technical Memorandum* is to identify and address the key privacy policy issues relating to the information collected from ITS components, and to recommend future actions or strategies to ensure individual privacy while collecting and disseminating data vital to the operation of ITS in Florida. These core actions will be incorporated in the update of *Florida’s Intelligent Transportation System Strategic Plan*.¹

¹ PB Farradyne, *Florida’s Intelligent Transportation System Strategic Plan – Final Report* (August 1999). Available online at http://www.dot.state.fl.us/trafficoperations/ITS/ITS_default.htm.

2. Background

There is a direct relationship between privacy laws and privacy policies. Privacy laws govern an activity, while privacy policies dictate a plan of action. Current privacy law is a patchwork of federal and state statutes, as well as federal and state judicial opinions. The “right” to privacy as a matter of law in the context of transportation on public roads and other facilities is limited.

The best examples of a detailed privacy policy can be seen by viewing various Internet sites’ privacy policy statements. The following statement can be found on the MyFlorida.comTM² Web site:

*Thank you for visiting the MyFlorida.comTM Web site. Your privacy is very important to us. Simply stated, our policy is to collect no personal information about you when you visit the MyFlorida.comTM Web site, unless you affirmatively choose to make such information available to us.*³

Typically, each Web site details a privacy policy that includes the following essential elements:

- The purpose for which the information is being collected;
- Any consequences for refusing to provide the personal information;
- The citizen’s right to inspect and correct personal records;
- Whether the information is generally available for public inspection; and
- Whether the information is made available to other entities.

This Web site’s privacy policy is clear and concise, and provides the appropriate level of privacy protection to individuals who utilize the Internet. What are not clear are Florida’s laws and policies that address the appropriate level of privacy protection for individuals whose information is collected from ITS components.

This situation may be remedied by creating a strategic plan to address an ITS right-to-privacy policy, as well as developing appropriate legislation and a structured outreach to improve public awareness about the purpose and function of ITS and the data these systems collect.

² MyFlorida.com is a trademark of the State of Florida.

³ The Internet Privacy Policy is available online at <http://www.myflorida.com/myflorida/privacy.html>.

3. Information Privacy Issues in Florida

3.1 Privacy

Intelligent transportation system technologies utilize numerous field devices for traffic surveillance and vehicle tracking. These terms, their associated technologies, and the information collected by these devices generally raise concerns regarding the motoring public’s privacy. Equally great are the concerns associated with closed-circuit television (CCTV), ETC, and photo enforcement, all of which have the potential for use and misuse by law enforcement and transportation officials. Indeed, the *USA Patriot Act*⁴ allows the Federal Bureau of Investigation (FBI) to order the surrender of business records or any other “tangible things” that are sought for an authorized investigation of international terrorism or clandestine intelligence activities. Because this federal law gives law enforcement officials broader powers to demand items previously deemed “private,” the surveillance information that transportation departments obtain is certain to fall within the purview of investigators, especially if the surveillance involves sensitive sites or critical transportation infrastructure.

If ITS deployments for the collection and dissemination of information are to continue, operating agencies must directly confront the privacy issue, which is likely to become a greater problem as the installation of these systems becomes more widespread. A strong consideration should be given to the development of well-publicized ITS information privacy policies and standards. For example, the privacy standards should require that all probe-based technologies (e.g., cellular geolocation, toll tag tracking, and instrumented vehicles) be designed in a manner that ensures the absolute privacy of the vehicles and passengers being tracked. The standard should also ensure that raw data allowing the “recreation” of an individual vehicle’s route not be archived.

In most cases, the public is unaware that the images obtained from CCTV traffic surveillance are neither recorded nor used for enforcement purposes. There is a rising concern among the traveling public that individual privacy is being violated by the use of these surveillance technologies. To address this issue, the Florida Department of Transportation’s (FDOT) policies and standards should recommend against the archiving of video data.

⁴ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001* (October 26, 2001). Pub.L.No. 107-56, 115 Stat. 272.

3.2 Data Privacy and Security

Many individuals perceive ITS as another form of government intrusion, sometimes call the “big brother” complex. As a result, this perceived privacy intrusion might become unpalatable to many citizens. In many instances, planning agencies have archived ITS data and stored this data for later use in analyzing historical traffic trends and extrapolating them for future estimates. Extreme care (i.e., privacy preservation) must be taken to ensure that individuals are not uniquely identified in the stored data. To this end, technology should be restricted to the compilation and retention of aggregated information rather than individualized information. In addition, privacy preservation must be effectively communicated to the public so that undue political pressure is not brought to bear on the FDOT’s use of ITS.

3.3 Data Ownership

Public agencies have often taken the position that their partnership in the development of ITS data entitles them to ownership of the data, or at least unlimited free access to the data. The State of Florida has a statute that directly relates to “Records made public by public fund use.”⁵ This statute states that “If public funds are expended by an agency . . . then all the . . . records . . . shall be public records . . .” In Florida, ITS data is not owned by the state; therefore, the data is public and cannot be sold to a private-sector partner.

Additionally, on May 13, 2004, Governor Jeb Bush approved Senate Bill (SB) 2008.⁶ This bill brings Florida into compliance with federal law limiting the release of state driver license record information. This new law, which became effective July 1, 2004, may have an obvious flaw that further enables the sale of drivers’ license information. The *Orlando Sentinel* has stated, “But even with this new law, exceptions allow the state to sell personal drivers license information to more than a dozen types of business and government agencies...selling information from driver license records would be expanded to make millions of additional dollars.”⁷ The passage of this new law and its associated vagueness may further complicate the issue regarding the potential sale of travel-related data, which may, in turn, impact the ITS industry.

⁵ FLA. STAT. § 119.012, *Records made public by public fund use* (2001). Available online at <http://www.leg.state.fl.us/stateutes/>.

⁶ Fla. SB 2008, *Motor Vehicle Records/Public Records* (2004) (amends FLA. STAT. § 119.07). Available online at <http://www.flasenate.gov/Session/index.cfm>.

⁷ Mahlburg, Bob, “Selling Drivers’ Data Now Limited,” *Orlando Sentinel*, May 14, 2004, Page B5.

3.4 Data Usage

Intelligent transportation systems may create data on individuals. Individuals should have a means of discovering how the data will be utilized. Data usage (i.e., visibility) in the context of this *Technical Memorandum* means to disclose to the public the type of data collected, how it is collected, what its uses are, and how it will be distributed. The concept of visibility is one of central concern to the public and, consequently, this principle requires assigning responsibility for disclosure.

Generally, data collectors should assure the public that ITS information provided to private organizations for secondary uses is stripped of personal identifiers. Individuals, however, may contract to allow use of personal identifiers for secondary use if the receiving organization makes full disclosure of the intended use and obtains informed consent from the individuals affected.

3.5 Public-Sector Competition with Private-Sector Partners

In Florida, the public sector is legally obligated to disseminate some of the ITS data at no cost to a private-sector partner. This particular policy may be limited to the dissemination of incident information to the media. However, in many cases, the dissemination of ITS data by the public sector becomes extensive, including video images, weather information, traffic flow information, and transit information – all delivered in electronic form to any interested distribution source.

While the motivations for this public-sector dissemination are legislated and certainly worthwhile, an agency must recognize that dissemination at this level virtually eliminates any potential source of income for its private-sector partners, and hence destroys the incentive for outside investment. As part of an overall strategic ITS information privacy policy plan, it would be worthwhile to examine this issue on both a national and statewide basis.

3.6 Access and Security

Who has access to ITS data is as important as how it’s used. Explicit controls on the utilization and export of ITS data may be accomplished using a standardized comprehensive agreement for ITS data users.

The use of data encryption and other security technologies can be used to make data worthless to unauthorized users.

3.7 Archived Data

The *National ITS Architecture (NITSA)*⁸ provides guidelines for the archiving and distribution of ITS data. This functionality integrates the planning, safety, operations, and research communities into ITS, and processes data products for these communities. The archived data site must ensure that sufficient security measures are in place to protect the loss, misuse, and alteration of the information under its control. These guidelines should be strongly considered for inclusion in the FDOT’s information privacy policy.

3.8 Information Accuracy

Another ITS information privacy policy consideration relates to ITS data collected by field surveillance equipment. It is well known that these devices are prone to errors due to equipment malfunctions, calibration “drift,” and communication disruptions. Therefore, it is clear that raw data from the field must be subjected to quality control and editing procedures before they are sampled, summarized, and stored. This is typically done at the application level by the development of standard procedures for flagging and treating both missing and erroneous data. At a minimum, the ITS Section of the FDOT Traffic Engineering and Operations Office (TEOO) should be aware of the Districts’ data quality problems and address them in a systematic way.

3.9 Liability

The liability associated with ITS information is unlikely to be any different from that of existing traffic management and traveler information systems. To date, the FDOT has experienced few problems in either of these areas. However, it is important to anticipate the possibility that with the use of real-time, in-vehicle information systems, errors will have an impact on travelers and could become grounds for liability claims.

It is recommended that an ITS information liability policy be developed. This policy would address – and enable – the FDOT to avoid any potential liability problems by executing agreements with organizations to which ITS information is provided, and by assigning any potential liability to the receiving organization.

⁸ United States Department of Transportation, *National ITS Architecture, Version 5.0*. Available online at <http://itsarch.iteris.com/itsarch/index.htm>.

4. Information Privacy in Federal and State Policies

Federal information privacy legislation is found in *Section 409 of Title 23 of the United States Code (USC)*.⁹ The legislation states:

Notwithstanding any other provision of law, reports, surveys, schedules, lists, or data compiled or collected for the purpose of identifying, evaluating, or planning the safety enhancement of potential accident sites, hazardous roadway conditions, or railway-highway crossings, pursuant to sections 130, 144, and 152 of this title or for the purpose of developing any highway safety construction improvement project which may be implemented utilizing Federal-aid highway funds shall not be subject to discovery or admitted into evidence in a Federal or State court proceeding or considered for other purposes in any action for damages arising from any occurrence at a location mentioned or addressed in such reports, surveys, schedules, lists, or data.

The United States Department of Transportation’s (USDOT) Privacy Policy was updated in December 2003 and details may be found on the agency’s Web site.¹⁰

Because the public is unaware that, in most cases, the data and images derived from ITS field surveillance devices are neither recorded nor used for enforcement purposes, there is a rising concern among the public that individual privacy is being violated. In reaction to these concerns, the Intelligent Transportation Society of America, or ITS America™ (ITSA),¹¹ a nonprofit, national ITS consortium, has developed a set of principles to address public concerns about potential privacy violations.¹² These privacy principles are provided in *Appendix A*. Although ITS America’s guidance is broad and general, it is designed to aid states with no formal policy, legislation, or structured outreach to address the public’s lack of awareness about the purpose and function of ITS.

⁹ 23 U.S.C. § 409, *Discovery and admission as evidence of certain reports and surveys*.

¹⁰ Available online at <http://www.dot.gov/privacy.html>

¹¹ ITS America is a trademark of the Intelligent Transportation Society of America.

¹² Intelligent Transportation Society of America, *ITS America Fair Information and Privacy Principles*. Adopted by the ITS America Board of Directors on January 11, 2001. Available online at <http://www.itsa.org/resources.nsf>.

4.1 Other State Legislation

Table 4.1 is an edited version of recent state-sponsored ITS legislation identified in an appendix included in a National Conference of State Legislatures (NCSL) Transportation Review.¹³ This version identifies ITS information privacy legislation introduced for the 2003 legislative sessions. Please note that only three bills are currently active.

Table 4.1 – Relevant 2003 Intelligent Transportation Systems’ Information Privacy Legislation

State	Bill No.	Sponsor	Description	Status
California	AB 198	Assm. Joe Nation (D)	This bill would prohibit the department or any specified transportation agency from selling or sharing the actual driving patterns of a motorist who uses an electronic toll payment device to drive through a toll bridge, toll lane, or toll highway.	Active
California	SB 602	Sen. Liz Figueroa (D)	This bill prohibits the use of information data encoded on a driver's license for marketing purposes or for use in an electronic device that reads personal information.	Active
Nevada	SB 26	Sen. Joseph M. Neal, Jr. (D)	This bill establishes certain requirements relating to monitoring devices attached to the exterior of vehicles to track movement or location of vehicles.	Inactive
Nevada	SB 220	Judiciary	This bill repeals the prohibition against certain uses by a governmental entity of photographic, video, or digital equipment for gathering evidence for the purpose of issuing traffic citations.	Inactive
Washington	HB 1019	Rep. Toby Nixon (R)	This bill pertains to the personally identifying information of people who acquire and use a transponder or other technology to facilitate the payment of tolls. The department may, at the secretary's discretion, disclose aggregate information on toll collection to governmental agencies or groups concerned with public transportation or public safety, as long as the data does not contain any personally identifying information. Personally identifying information may be released to law enforcement agencies.	Active

¹³ Sundeen, Matt, *Traffic Congestion: State Legislatures Examine Intelligent Transportation Solutions, Appendix – State Intelligent Transportation Legislation, 2003* (November 2003). National Conference of State Legislatures (NCSL) Transportation Review, No. 18. © 2003 by the National Conference of State Legislatures. All rights reserved.

4.2 Initial Actions for the Florida Department of Transportation’s Intelligent Transportation Systems Section

The recognition of privacy as a value seems worthy of concern in designing ITS because, in the long run, public acceptance and use of ITS services will depend on public confidence that the technology is not predatory or harmful. Respecting privacy fosters public confidence in ITS and will add to the consumer appeal of ITS services.

The purpose of this *Technical Memorandum* has been to review existing ITS privacy legislation and to make recommendations for further FDOT actions. This section identifies key actions for the FDOT TEOO’s ITS Section.

The following are recommended “next steps” for the implementation of ITS information privacy policies and standards within Florida. The FDOT should:

- Lead the development of a strategic ITS information privacy plan and standards. This strategic plan should specifically address an ITS information privacy policy, the need for enabling legislation, and development of a structured outreach approach.
- Lead the development of a cradle-to-grave policy for ITS data. This policy should specifically address data collection, analysis, access, security, archiving, and retention duration. It should address the terms and procedures whereby ITS data or surveillance images would be furnished to Florida’s law enforcement agencies that seek that information pursuant to their investigations.
- Ensure that the ITS information privacy policy is legally compliant and consumer friendly. One of the greatest obstacles to understanding legislation and policies is the dry, verbose, and ambiguous way in which the legislation is written. To that end, some agencies are providing “executive summaries” of the legalese that allow consumers to get a sense of what companies do with data. If that raises a red flag, consumers can access the full policy for more details.
- Develop standardized privacy and security-related templates to be inserted in requests for proposals (RFPs), invitations to negotiate (ITNs), etc., to ensure consistency across Florida.
- Develop a structured outreach program to inform the general public about the uses of ITS devices on roadways and what is being done to protect individual privacy. Outreach programs should be designed to explain the safeguards against privacy violations and should include procedures that ensure these safeguards are working.

*Technical Memorandum No. 3.7 – Florida’s 2003 ITS Strategic Plan Update
The FDOT ITS’ Information Privacy Policy*

- Determine performance measures to gauge whether the public outreach implemented is having the desired effect.
- Develop a formal policy on the use of all ITS components that may be viewed as intrusive, including CCTV video and the *iFlorida*¹⁴ variable speed limit signs. The policy should be distributed to, and implemented by, the FDOT Districts.
- Develop a standardized, comprehensive agreement among ITS agencies regarding the use of information obtained through ITS components.
- Consider requiring the development of a privacy impact statement, similar to the environmental impact statements already required under federal law, before an ITS program is implemented.

¹⁴ More information regarding the FDOT’s *iFlorida* Surface Transportation Security and Reliability Information System Model Deployment Project is available online at <http://www.iflorida.net/>.

Appendix A

The ITS America Fair Information and Privacy Principles

ITS America Fair Information and Privacy Principles¹⁴

- 1. INDIVIDUAL CENTERED. Intelligent Transportation Systems must recognize and respect the individual’s interests in privacy and information use.**

ITS Systems create value for both individuals and society as a whole. Central to the ITS vision is the creation of ITS Systems that will fulfill our national goals. The primacy focus of information use is to improve travelers’ safety and security, reduce travel times, enhance individuals’ ability to deal with highway disruptions, and improve air quality. Travel information is collected from many sources, some from the infrastructure and some from vehicles, while other information may come from the transactions – such as electronic toll collection – that involve interaction between the infrastructure and vehicle. That information may have value in both ITS and non-ITS applications. The individual’s interest in privacy must be respected. This requires disclosure and the opportunity for individuals to express choice if personal identification is collected.

- 2. VISIBLE. Intelligent Transportation Information Systems will be built in a manner “visible” to individuals.**

ITS may create data on individuals. Individuals should have a means of discovering how the data flows operate. “Visible” means to disclose to the public the type of data collected, how it is collected, what its uses are, and how it will be distributed. The concept of visibility is one of central concern to the public, and, consequently, this principle requires assigning responsibility for disclosure.

- 3. COMPLY. Intelligent Transportation Systems will comply with applicable state and federal laws governing privacy and information use.**

Privacy law is a patchwork of federal and state statutes, as well as federal and state judicial opinions. The “right” to privacy as a matter of law in the context of transportation on public roads and other facilities is limited. Intelligent Transportation Systems should provide, at a minimum, privacy protections in conformity with the law of respective jurisdictions.

- 4. SECURE. Intelligent Transportation Systems will be secure.**

ITS databases may contain information on where travelers go, the routes they use, and when they travel, and therefore must be secure. All ITS information systems will make use of data security technology and audit procedures appropriate to the sensitivity of the information. ITS systems should use technological and administrative safeguards to assure that access to personally identifiable information is restricted to duly authorized individuals.

¹⁴ © 2003 ITS America. All rights reserved.

5. **LAW ENFORCEMENT. Intelligent Transportation Systems have an appropriate role in enhancing travelers’ safety and security interests, but absent consent, statutory authority, appropriate legal process, or emergency circumstances as defined by law, information identifying individuals will not be disclosed to law enforcement.**

ITS has the potential to make it possible for traffic management agencies to know where individuals travel, what routes they take, and travel duration. Therefore, ITS can increase the efficiency of traffic law enforcement by providing aggregate information necessary to target resources. States may legislate conditions under which ITS information will be made available to law enforcement agencies. Absent government authority, however, ITS systems should not be used as a surveillance means for enforcing traffic laws, nor used as a tool of criminal investigation. Although individuals are concerned about public safety, persons who voluntarily participate in ITS programs or purchase ITS products should be informed of how information they are providing is used.

6. **RELEVANT. Intelligent Transportation Systems will only collect personal information that is relevant for ITS purposes.**

ITS, respectful of the individual’s interest in privacy, will only collect information that contain individual identifiers that are needed for the ITS service functions. Furthermore, ITS information systems will include protocols that call for the purging of individual identifier information that is no longer needed to meet ITS needs.

7. **ANONYMITY. Where practicable, individuals should have the ability to utilize Intelligent Transportation Systems on an anonymous basis.**

Certain ITS applications (commercial vehicle operations or “mayday”) require personally identifiable information to function. Others (such as automated fee payment) may be designed to enable use by individuals without identifying themselves (through anonymous debit accounts) or with identifiers for convenience (credit cards). Unless provision of identifiers is required by the ITS application, users should be provided with the opportunity to choose anonymity.

8. **COMMERCIAL OR OTHER SECONDARY USE. Intelligent Transportation Systems information stripped of personal identifiers may be used for non-ITS applications.**

American consumers want information used to create economic choice and value, but also want their interest in privacy preserved. ITS information is predictive of goods and services that interest consumers – for example, the right location for stores, hospitals, and other facilities. However, personally identifiable information collected by ITS surveillance technologies is extremely sensitive. Therefore, the following practices should be followed:

- ITS information absent personal identifiers may be used for ITS and other purposes.
- Generally, data collectors should assure that ITS information provided to private organizations for secondary uses is stripped of personal identifiers.
- Individuals, however, may contract to allow use of personal identifiers for secondary use if full disclosure in the intended use is made and informed consent obtained.

9. **FOIA. Federal and State Freedom of Information Act (FOIA) obligations require disclosure of information from government-maintained databases. Database arrangements should balance the individual’s interest in privacy and the public’s right to know.**

In determining whether to disclose ITS information, governments should, where possible, balance the individual’s right to privacy against the preservation of the basic purpose of the Freedom of Information laws to open agency action to public scrutiny. ITS travelers should be presumed to have reasonable expectations of privacy for personal identifying information. Pursuant to the individual’s interest in privacy, the public/private framework of organizations collecting data should be structured to resolve problems of access created by FOIA.

10. **OVERSIGHT. Jurisdictions and companies deploying and operating Intelligent Transportation Systems should have an oversight mechanism to ensure that such deployment and operation complies with their Fair Information and Privacy Principles.**

Governments and companies should implement proper procedures to ensure that they protect the individual user’s right to privacy, at a minimum, to the extent outlined in these principles. This mechanism may include internal directives, the appointment of a privacy officer, and/or penalties for violations. Governments and companies should have the flexibility to tailor such a system to their respective needs or circumstances.