Privacy Issues with the Use of Smart Cards

DETAILS

25 pages | | PAPERBACK
ISBN 978-0-309-43608-3 | DOI 10.17226/23104

AUTHORS

April 2008

TRANSIT COOPERATIVE RESEARCH PROGRAM
Sponsored by the Federal Transit Administration

Subject Areas: IA Planning and Administration;
IC Transportation Law; VI Public Transit

Responsible Senior Program Officer: Gwen Chisholm Smith

Legal Research Digest 25

PRIVACY ISSUES WITH THE USE OF SMART CARDS

This report was prepared under TCRP Project J-5, "Legal Aspects of Transit and Intermodal Transportation Programs," for which the Transportation Research Board is the agency coordinating the research. The report was prepared by Paul Stephen Dempsey, Tomlinson Professor of Law, McGill University, Montreal, Quebec, Canada. James B. McDaniel, TRB Counsel for Legal Research Projects, was the principal investigator and content editor.

CONTENTS

The Problem and Its Solution

The nation's transit agencies need to have access to a program that can provide authoritatively researched, specific, limited-scope studies of legal issues and problems having national significance and application to their businesses. The TCRP Project J-5 is designed to provide this insight.

The intermodal approach to surface transportation requires a partnership between transit and other transportation modes.

Transit attorneys have noted that they particularly need information in several areas of transportation law, including environmental requirements; construction and procurement contract procedures and administration; civil rights and labor standards; and tort liability, risk management, and system safety.

In other areas of the law, transit programs may involve legal problems and issues that are not shared with other modes; as, for example, compliance with transit equipment and operations guidelines, Federal Transit Administration (FTA) financing initiatives, and labor or environmental standards.

Applications

Smart Cards are credit card-sized plastic cards that contain embedded technology enabling an electronic link between the card and the transit provider's reader equipment. The cards allow for a very fast transfer of information that transit providers need to collect their fees. Using Smart Cards to replace traditional transit tickets or tokens reduces cash handling, equipment maintenance, and security costs. Smart Cards hold the promise of increasing convenience for riders, improving collection of ridership data, lending a more modern image to transit, and providing new opportunities for innovative fare structures and marketing.

In March 2000, TCRP published *Legal Research Digest 14: Treatment of Privacy Issues in the Public Transportation Industry*. *TCRP LRD 14* contains a historic and general overview of privacy in the field of public transportation—examining privacy issues associated with employment, as well as those associated with customers of public transportation. It also noted the beneficial use of a Smart Card data collection system to transportation planners. Subsequent to this publication, particularly after the terrorist events of September 11, 2001, public consciousness regarding privacy as it relates to the use of Smart Cards changed. The plea for a higher level of security has supported the rapid growth in technological enhancements and uses of the Smart Card.

This digest examines basic privacy issues associated with the acquisition and storage of financial and trip data, including, but not limited to, who can access the data, what data may be accessed and under what conditions, and how the information can be used. As such, it should be useful to attorneys, administrators, human relations officers, security personnel, financial officers, and others.

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

PRIVACY ISSUES WITH THE USE OF SMART CARDS

By Paul Stephen Dempsey
Tomlinson Professor of Law, McGill University

I. INTRODUCTION

A. The Potential Uses and Abuses of Smart Cards

Transit providers can use Smart Cards for different purposes. They can be used to process transit *passengers* through the transit system, and to bill them for their travel. Thus, the financial and accounting issues surrounding travel can be accommodated efficiently both from the travel customer and provider perspective. Smart Cards can allow prepurchase of travel, from which each trip results in a deduction, or a subsequent billing of the traveler.

Smart Cards can also be used by transit *employees,* principally for security reasons. Employees need Smart Cards for ingress and egress, and many may have safety- or security-sensitive functions posing sharply different government interest concerns as compared to passengers. The transit employee can be prescreened for security purposes and denied access to certain secured areas. The goings and comings of the transit employee also can be monitored should there be a need to locate where an employee is, or has been.

Smart Cards can also serve as a means of collecting data useful for marketing and planning purposes. Thus, if the Smart Card includes passenger demographic or locational data, then the transit provider can determine traffic flows and plan and build infrastructure to accommodate demand, or tailor advertising to induce increased ridership. The data may be stored on the computer chip embedded in the card, or stored in a remote computer database accessed electronically.

Finally, by adding personal information and perhaps biometric data, Smart Cards can be used to enhance security in the transit system. Passengers who pose a security threat can be prohibited entry. Passengers who have been involved in a security incident can be more easily identified and arrested.

Biometric identification has been used for years in Orlando theme parks to ensure that the person presenting the Annual Pass is actually the person who purchased it, so that it is not handed off from one user to another, thereby harming overall sales. A photograph on a driver's license is a rudimentary form of biometric identification to ensure that the person holding the license is actually the person to whom it was issued.

Biometrics technology offers opportunities for personal identification and correlation of identification with historical conduct. Biometrics is the use of the unique physical or behavioral characteristics of an individual to establish his or her identity. Such physical characteristics as fingerprints, hand scans, facial scans, and iris and retina scans can be used as biometric identifiers.[1] Thus, the image of a thumb or palm print, or an iris, can be stored and used to positively identify an individual. Cameras can scan the facial characteristics of passengers, identifying suspects with facial recognition software, and follow them as they walk through passenger terminals.

The algorithm used to identify high-risk airline passengers is a closely guarded secret, but may include the travel history of the passenger—where and when the ticket was purchased, whether the ticket was for one-way or round-trip travel, whether payment was by cash or credit card, where and with whom the passenger flew, and whether baggage was checked. In addition, readily available information exists about the individual:

- Credit card purchases,
- Telephone calls placed,
- Internet sites visited,
- Property title transfers,
- Credit history,
- Employment history,
- Criminal arrests and convictions, and
- Tax returns.

To what extent is, or should, this data be correlated with travel data to identify terrorist or other criminal suspects? Some data may be irrelevant for law or security enforcement purposes, and therefore of little practical concern. For example, visits to Internet porn sites may reveal little about terrorist activity, yet visits to bomb assembly instruction sites may be of legitimate concern to law enforcement and security officials. And is it legitimate to correlate information concerning a passenger's nationality, ethnicity, race, religion, or political affiliation?

The more data that is correlated, the more likely it is that law enforcement agencies will be able to deter terrorist activities. The passenger who is identified as posing a potential security threat can be banned from the public transit system.[2] Such information also can be

[1] Greg Star, *Comment: Airport Security Technology: Is the Use of Biometric Identification Technology Valid Under the Fourth Amendment?*, 20 TEMP. ENVTL. L. & TECH. J. 251, 253 (2002).

[2] "Characteristics such as fingerprints, hand geometry, facial appearance, and retina and iris scans are all considered biometric measures. Because each of these characteristics are, at

used to identify and arrest criminals at large, reduce drug trafficking, and even collar "dead beat dads." Yet, again, the more effective the security screening mechanisms, the higher the price paid in terms of civil liberty. Discrimination against people of Arabic descent, of the Muslim faithful, or of people with darker skin is a real risk for a nation that aspires to ethnic neutrality on such issues.

Improved technology allows enhanced data opportunities. Yet, the more useful the data collected may be—whether financial, demographic, or personal—the more intrusive is the impact on personal liberty and individual privacy. Thus, there is a trade-off in terms of the costs and benefits of the Smart Card. The smarter the card, the more useful it is, yet the more intrusive it becomes.

B. Examples of Smart Card Utilization

1. What Is a "Smart Card"?

A Smart Card is one of several automatic identification (Auto-ID) systems, which include bar codes, optical character recognition systems, and radio frequency identification (RFID) systems. For example, a can of soup may have a Universal Product Code (UPC) bar code on its label that can be scanned with a laser beam at the grocery store checkout counter. The box in which the cans were packed may also have a UPC bar code on it, enabling efficient inventory management at the manufacturing, transportation, wholesale, and retail levels of the supply chain.

A Smart Card may enable a person to enter a building and monitor the door through which he or she enters, perhaps blocking access to some. The system can monitor when and where he or she passes through. While a bar code requires line-of-sight scanning by a laser and a basic magnetic strip requires physical contact with a reader, a Smart Card embedded with an RFID system can be identified at a distance. An RFID system is more convenient and expeditious, and because there is no physical contact, results in less wear and tear on the card and scanning hardware.[3]

Smart Cards are credit-card-sized, wallet-insertable pieces of plastic that contain embedded electronics (such as an integrated circuit chip (ICC) or microchip) and a transponder. The basic magnetic-strip cards (sometimes called a "key card") only operate when placed in physical contact with a reader, which communicates the information embedded thereon to a computer. Newer models, sometimes called "contactless" Smart Cards, have built-in radio frequency antennae embedded in them. In order to send and receive data, the card must be near a radio transmitter (also known as a remote contactless radio frequency interface). Without a separate battery, they usually have to be between 1 and 3 in. from a reader in order to be read, though technology may enhance the size of the radius within which a Smart Card can be read. "Hybrid" or "dual-function" Smart Cards have both a contact interface and a wireless antenna embedded in the same microchip or storage device.[4]

RFID systems have two components—a transponder (the data-carrying device) and a reader (a radio transceiver that communicates with the transponder through radio waves). An RFID tag is a tiny silicon chip comprised of an electronic circuit attached to an antenna. It is about the size of a grain of sand and capable of performing storage and computational functions.[5] An RFID tag has memory where information can be stored. With an embedded microcontroller, Smart Cards can store large amounts of data, carry out on-card functions (such as encryption and mutual authentication), and interact intelligently with a reader.[6] The RFID tag listens for radio signals sent by RFID readers, and when it receives a particular radio query, it transmits its unique ID code stored in its memory to the reader.[7]

In order to work, standard magnetic strip cards must have physical contact with a reader and access to a database at the time of the transaction. In contrast, a Smart Card can either have information embedded in a memory chip with nonprogrammable logic, or in a memory chip and a microprocessor. A Smart Card with a nonprogrammable logic, such as a prepaid phone card, can only perform predefined operations. A Smart Card with a microprocessor can delete and manipulate information. The latter two types of Smart Cards differ from the basic magnetic strip cards in that they carry all necessary functions and information on the card.[8]

A federal district court defined a Smart Card as "a credit-card size device that contains a programmable computer chip that can be encoded with information. A 'key card' such as those often used to permit individuals to open locked doors in a secure environment is a type of smart card."[9] Because smart cards embedded with RFID technology can procure more information about the user than simple key cards, they may raise more significant privacy concerns about what information is collected, how it is stored, who has access, and how the information may be used.

---

least in theory, unique to the individual, biometrics makes it possible to accurately identify a person." Star, *supra* note 1.

[3] Jerry Brito, *Relax Don't Do It : Why Rfid Privacy Concerns are Exaggerated and Legislation is Premature*, U.C.L.A. J. L. TECH. 5 (2004).

[4] Leighton Techs., LLC v. Oberthur Card Sys., S.A., 423 F. Supp. 2d 425–427 (S.D.N.Y. 2006).

[5] Rina Chung, *Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PACIFIC L. & POL'Y J. 442, 444 (2003).

[6] http://www.smartcardalliance.org/pages/smart-cards-intro-primer (Last visited Nov. 8, 2007).

[7] Brito, *supra* note 3.

[8] Margaret Betzel, *Biometrics: Privacy Year in Review: Recent Changes in the Law of Biometrics*, 1 ISJLP 517, 533 (2005).

[9] DirecTV, Inc. v. Deskin, 363 F. Supp. 2d 254 (D. Conn. 2005).

In the transportation context, Smart Cards are one of several emerging technologies collectively known as Intelligent Transportation Systems (ITS). ITS technologies provide an unprecedented means of real-time monitoring of individual and vehicular movements. Moreover, the technologies are capable of recording and maintaining historical travel pattern data—where a person travels, when they travel, and how often—and aggregating and correlating this data with other personal information (including such items as gender, race, religion, political affiliation, place of birth and residence and employment, law enforcement history, credit history, income, and so forth) about the individual throughout his or her lifetime.[10]

Aggregating and correlating such data can allow the viewer to learn quite a lot about the behavioral patterns of the individual. The greater the database, and the more extensively it is correlated with other databases, the less privacy the individual enjoys. Moreover, the technology will evolve over time, allowing enhanced real-time monitoring of individual whereabouts, greater accumulations and correlations of more precise information, and more complete databases. Individuals may be unaware of the extensive information available about their conduct. They may be unaware that their movements are tracked. One source observes, "The relationship between privacy and ITS is reciprocal. Privacy will, no doubt, be affected by ITS. But ITS will also be affected by concerns about privacy. This circular relationship between privacy issues and ITS is complicated by the fact that neither privacy nor ITS is simple or static."[11]

We must be mindful of the fact that Smart Card technology and its applications will not remain static, for technology rarely stands still. Moreover, processing speed, database size, and international networks constitute "an ocean of information waiting to be harvested."[12] For example, the microprocessor could be used to store biometric identification information about the individual, assuring that the holder of the card is its rightful owner and that the information is correctly correlated with that individual. The Smart Card and the computer with which it communicates can contain precise information identifying the owner's unique thumb print, iris, or retina.[13] Moreover, though current technology does enable a Smart Card to be read by Global Posititioning Systems (GPS), because the batteries in the card only enable a broadcast for a few inches, the day may come when GPS can be linked to Smart Cards, enabling real-time monitoring of individuals' whereabouts beyond the areas where the cards are scanned on the ground. Even before then, the day may soon come when the reading radius grows to allow Smart Cards to be read in transit stations and vehicles. In such circumstances, the transit provider could have real-time data about the whereabouts of individual passengers. Thus, if it wanted to track down a graffiti artist, a criminal, or a terrorist, the Smart Card coupled with video monitoring could enhance law enforcement.

2. Origins of Smart Cards

RFID technology was invented in 1969, but has only relatively recently become technologically and economically viable.[14] The banking industry introduced Smart Cards to curtail losses from card fraud and to improve card security. The telephone industry subsequently adopted them as pay phone cards. In Europe, governments use Smart Cards as portable personal files (e.g., for health records, or to store and update data regarding eligibility for benefits).[15] Other uses include, for example, ingress and egress of employees to secured facilities**,** airline trusted travelers, travel visa, and immigration services. The U.S. Department of Transportation (DOT) also has established an Intelligent Vehicle Highway System, which, like Smart Cards, can monitor individual travel patterns.[16]

One source summarizes the uses for Smart Cards:

- Secure identity applications—employee ID badges, citizen ID documents, electronic passports, driver's licenses, online authentication devices.
- Healthcare applications—citizen health ID cards, physician ID cards, portable medical records cards.
- Payment applications—contact and contactless credit/debit cards, transit payment cards.
- Telecommunications applications—Global System for Mobile Communication (GSM) Subscriber Identity Modules, pay telephone payment cards.[17]

C. Advantages of Smart Cards

1. General Advantages

Smart Cards offer the advantages of cost, efficiency, time, and convenience. They can combat identity theft and abuse of welfare and other governmental privileges, and allow for faster access to secure areas and across borders.[18] In general, they may allow more efficient ac-

[10] Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 151–54, 166 (1995).

[11] *Id.* at 152 (1995) [citations omitted].

[12] Dorothy J. Glancy, *Symposium on Internet Privacy: At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 360 (2000). *See also* R. Brian Black, *Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models from South Africa and the United Kingdom*, 34 CORNELL INT'L L.J. 397, 404 (2001).

[13] Chung, *supra* note 5, at 442, 464 (2003).

[14] Brito, *supra* note 3.

[15] http://www.totse.com/en/privacy/privacy/idsmrtpb.html (Last visited Nov. 8, 2007).

[16] See Sheri A. Alpert, *Privacy and Intelligent Highways: Finding the Right of Way*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 97 (1995).

[17] http://www.smartcardalliance.org/pages/smart-cards-intro-primer (Last visited Feb. 10, 2007).

[18] Chung, *supra* note 5.

cess to government services. Smart cards carry computer chips that can:

- Act as keys to buildings;
- Store money electronically and eliminate the need for cash transactions;
- Store personal identification or biometric data, such as photographs, eye patterns, or fingerprints;
- Enable collection of time, location, and frequency data of card use; and
- Store personal information, such as medical records, DNA, religion, age, and address, or personal identification numbers.[19]

2. Individual Identification

Drivers' licenses, credit cards, insurance and health cards, and birth certificates serve as alternative forms of identification. Identification of the individual is important so that the government can provide services, such as medical care and social assistance, to eligible recipients.[20] Individual identification can be enhanced through biometric identification measures, such as a thumb, hand, or retinal scan. Biometric identification requires a three-step process: (1) enrollment, (2) templates, and (3) matching. Enrollment is the process by which the individual provides biometric data. The enrollment template stores the individual's biometric information. Matching is the process whereby the individual's template is correlated with the individual's biometric measure taken "on the spot."[21] The result is a high level of confidence that the individual present is the individual identified on the template. The template, in turn, can be correlated with other information about the individual to determine whether he or she poses a security concern.

3. Enhanced Security

A Smart Card can authenticate the individual holder and the card and authorize transactions offline. It is far more secure than a magnetic stripe card, for it has the processing capabilities of a small microcomputer and can store generous amounts of data. [22] The United States adopted a comprehensive approach of layering one type of security mechanism upon another. The Transportation Research Board addressed the issue of facing the challenges posed by terrorist acts:

> Prospects for defending against…vulnerabilities through traditional means, such as "guards, guns, and gates," are dim. The transportation sector is simply too large and the threats faced too diverse and ever-changing for such blanket approaches to work….
>
> Transportation security can best be achieved through coherent security systems that are well integrated with transportation operations and are deliberately designed to deter terrorists even as they selectively guard against and prepare for terrorist attacks. In particular, layered security systems, characterized by an interleaved and concentric set of security features, have the greatest potential to deter and protect. Layered systems cannot be breached by the defeat of a single security feature—such as a gate or guard—as each layer provides backup for the others, so that the impermeability of individual layers is not required. Moreover, the interleaved layers can confound the would-be terrorist. Calculating the odds of breaching a multi-tiered system of defense is far more difficult than calculating the odds of defeating a single, perimeter protection.[23]

Enhanced data collection and correlation may help identify those individuals who pose a potential security threat, whether as passengers or employees, and prohibit their entry into transit facilities or otherwise deter terrorist acts.

D. Disadvantages of Smart Cards

One fundamental question is whether, in the use of Smart Cards, individual civil liberties/human rights can be adequately protected. Are privacy, free speech or association, due process, equal protection, or protection against unlawful searches and seizures infringed upon by bodily and baggage searches, passenger profiling, biometric identification, and computerized gathering and correlation of personal information (e.g., financial, employment, education, consumer purchases, travel behavior, or political or religious affiliation)?

Protecting the public against terrorist acts is a tremendously important task. However, governmental institutions that provide security must not be blind to the impact that their processes, procedures, and costs have on passenger convenience, personal privacy, and individual liberty. It is the careful balancing of these conflicting objectives that is the formidable task of government.

The fundamental challenge is to create a security regime that is highly effective in preventing acts of terrorism, but does not unduly interfere with the efficiency and productivity of transportation, impose excessive costs, create unwarranted passenger inconvenience, or intrude unnecessarily into individual privacy and civil liberty.

So long as mass transportation systems are open to the public, they will never be totally secure. To the extent security becomes more effective, modern technology enables it to become significantly more intrusive on personal liberty and privacy. Some have suggested that the burden of proving privacy intrusions are necessary should be placed upon those who insist upon them, and that proposed intrusions should be scrutinized care-

[19] http://www.acjnet.org/youthfaq/pricards.html (Last visited Nov. 8, 2007).

[20] *Id.*

[21] Star, *supra* note 1, at 251, 256.

[22] http://www.totse.com/en/privacy/privacy/idsmrtpb.html (Last visited Nov. 8, 2007).

[23] TRANSPORTATION RESEARCH BOARD, DETERRENCE, PROTECTION AND PREPARATION: THE NEW TRANSPORTATION SECURITY IMPERATIVE 1 (TRB Special Report 270, 2002).

fully.[24] The most effective means of screening passengers pose the most significant threats to individual privacy and civil liberties.[25] Biometric technology holds promise, as does passenger profiling, though civil liberties may be compromised. Advanced technology offers promise both in reducing the size of the haystack through which security personnel must sift to find the needles and in creating a "trusted traveler" method to expedite travel for those who do not impose a security risk.[26] Vast amounts of computer information exist with which to monitor an individual's travel, Internet, and purchasing behavior. Nonetheless, correlating personal information on such things as travel, political and religious affiliation, and nationality raises serious questions in terms of intrusion into personal privacy.[27] Certain scanning technologies can produce anatomically correct body scans, devoid of clothing.[28] Others can identify suspects in crowds at airports, with cameras and computers monitoring their movement.[29] All of this raises serious concerns about human rights and the Constitutional rights of free speech, religion, association, due process, and equal protection, and the prohibition against unwarranted searches and seizures.[30]

---

[24] In 2002, the Privacy Commissioner of Canada, George Radwanski, observed:

> I do not suggest that privacy is an absolute right. I recognize that there may sometimes be a need for some new privacy-invasive measures to enhance security and allow law enforcement agencies to investigate crimes and threats to public safety. But proposals for any such measures must be evaluated calmly, carefully and on a case by case basis.
>
> The burden of proof must always be on those who claim that some new intrusion or limitation on privacy is necessary.
>
> I have suggested that any such proposed measure must meet a four-part test:
>
> • it must be demonstrably necessary in order to meet some specific need;
>
> • it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
>
> • the intrusion on privacy must be proportional to the security benefit to be derived; and
>
> • it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.

http://www.privcom.gc.ca/media/le_021125_e.asp (Last visited Nov. 14, 2007).

[25] *See, e.g.*, Jonathan L. Miller, *Search and Seizure of Air Passengers and Pilots: The Fourth Amendment Takes Flight*, 22 TRANSP. L.J. 199 (1994).

[26] Barbara De Lollis, *'Trusted-Traveler' Card Could Speed Security Check*, USA TODAY, July 1, 2002. Trusted traveler (or "registered traveler") cards were first tested at airports near Los Angeles and Philadelphia.

[27] Dr. Bloom notes the significant problems associated with passenger profiling:

> Besides commonly cited problems of profiling including low terrorism-base rates, high false positive rates through low specificity, high false negative rates through low sensitivity, and civil rights violations through racial, ethnic, sex and age discrimination, there are yet additional concerns.
>
> First, even if one could develop reliable and valid profiles, the social transformation of knowledge suggests that their reliability and validity may change through time….
>
> Second, in the continuation of the ancient game of spy-counterspy, profile data inevitably leaks so that terrorists can use the profiles as part of their own deceptive strategies….
>
> Third, in a variant of another ancient game—looking for one's key where the light is better, not where one dropped it—most profilers analyze external factors, such as physical characteristics, behavior or demographics. However, intrapsychic processes may be more robust correlates of terrorist behavior, but are more difficult to identify.

Richard W. Bloom, *Commentary on the Motivational Psychology of Terrorism Against Transportation Systems: Implications for Airline Safety and Transportation Law*, 25 TRANSP. L.J. 175, 179 (1998).

[28] Kevin Maney, *The Naked Truth About a Possible Airport Screening Device*, USA TODAY, Aug. 7, 2002, at 3B, *available at* http://www.usatoday.com/tech/columnist/kevinmaney/2002-08-06-maney_x.htm (Last visited Nov. 8, 2007).

[29] Ann Davis, Joseph Pereira & William Bulkeley, *Security Concerns Bring Focus on Body Language*, WALL ST. J., Aug. 15, 2002, at 1, *available at* http://cryptome.org/naked-face.htm#wsj (Last visited Nov. 8, 2007). Computer programs can assess facial language. An "El Al Protocol" also analyzes how large numbers of passengers behave when walking through an airport, identifying suspicious behavior. *Id*.

[30] The visible signs of security are evident at every commercial airport. Passengers walk through magnetometers, and are sometimes wanded, frisked, asked to surrender their wallets to the x-ray machine, surrender their Swiss army knives for confiscation, turn on their computers and cell phones, and surrender those whose batteries are dead. Occasionally, a passenger is asked to remove articles of clothing, or submit to a more intrusive bodily search. Some are interrogated. Their carry-on luggage is x-rayed, and sometimes opened and inspected. Their checked baggage is also examined with explosive detection technology (EDT), and is sometimes opened and inspected. Their personal contents are revealed. How far can security personnel go before they have engaged in an unlawful search and seizure of persons and their baggage?

Can, or should, a nation require that passengers carry a national identity card? In truth, such a card already exists for the international traveler in the form of a passport, and the identity of its holder is correlated with domestic and international law enforcement databases at all borders. Should a discretionary "trusted traveler" card be available to expedite the movement of low-risk passengers through the security funnels, so as to free resources to sift more carefully through passengers of higher risk? If so, what personal information should an individual be asked to reveal as the quid-pro-quo for the card?

See Samuel R. Gross and Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413 (2002);
Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOYOLA U. CHI. L.J. 933 (2002); Jack Daniel, *Reform in Airport Security: Panic or Precaution?*, 53 MERCER L. REV. 1623 (2002); Suzanne Graves, *Checkpoints and the Fourth Amendment: Saving Grace or Constitutional Martyr*, 32 CONN. L. REV. 1487 (2000); Jamie Rhee, *Rational and Constitutional Approaches to Airline Safety in the Face of Terrorist Threats,* 49 DEPAUL L. REV. 847 (2000). See PAUL DEMPSEY, WILLIAM THOMS & ROBERT HARDAWAY, AVIATION LAW & REGULATION § 9.41 (1993).

Specifically, the principal concerns with Smart Cards include:

1. What Type of Information Is Gathered?

A Smart Card could have minimum prepayment functionality, like a debit card, and readers could merely subtract the cost of individual trips. Financial and trip data might be all that Smart Cards provide. Alternatively, marketing data could be obtained if other information is obtained, such as the name, home and work address, age, and gender of the passenger. The RFID features of a Smart Card may enable centralized monitoring of the venue of individual passengers carrying these cards. Further, Smart Cards could collect information that could be correlated with criminal information to enhance transit security. Biometric identification could be used to ensure that the card belongs to the person using it. The information gathered may be individually personal and private.[31] One source notes:

> As it stands, the government already has all of the resources that are necessary to monitor individual citizens in all aspects of their daily lives: omnipresent video cameras, extensive databases replete with medical, financial, and criminal information; and facial matching technology. Combined, this technology provides unprecedented power to identify, record and monitor the most intimate details of human life: the places we go, the activities in which we engage, and the people with whom we associate.[32]

2. What Are the Potential Uses of Gathered Information?

Information may be used merely for fare payment or for planning and advertising purposes, or to monitor the personal (or political and religious) or criminal behavior of individuals, potentially intruding upon one's civil rights and civil liberties. Transit providers have an increasing interest in protecting public safety and security and may want to share data with law enforcement officials.

3. Who Has Access to the Information?

The transit provider has an obvious interest in payment for trips taken and may have an interest in monitoring trip behavior. Once the information is included in a database, then any transit employee having access to the database may access the personal information contained therein. The data may be shared with law enforcement or other governmental institutions. History is replete with examples of abusive and oppressive governments. Moreover, commercial or criminal interests may have access to data for purposes of personal gain, such as identity theft or raiding one's bank accounts. Further, under state public records laws, the general public potentially may have access to information collected by governmental institutions, some of which may be of a private or embarrassing nature.

4. What Are the Implications for Personal Privacy?

The level of privacy protection depends on what data is acquired and recorded; when and how that data is accessed, distributed and destroyed; and who has access thereto.[33] Personal anonymity is sacrificed when governmental institutions can monitor individual behavior.[34] Advances in technology have outpaced the laws governing privacy of information gathered.[35]

Concerns have been expressed about creation of a "surveillance society," one in which the government monitors every aspect of one's life and correlates it with governmentally-based and private sets of personal information.[36] One source notes, "Those most fearful of biometric technologies warn they are accelerating the trend toward a surveillance society that gained momentum after the 9/11 terrorist attacks."[37] Contemporary computer biotechnology allows more intensive screening of all who enter a bottleneck, such as a transit entry point, though there is a privacy price to be paid. The U.S. Government Accountability Office has observed,

> Once in place, smart card-based systems designed simply to control access to facilities and systems could also be used to track the day-to-day activities of individuals, thus potentially compromising the individual's privacy. Further, smart card-based systems could be used to aggregate sensitive information about individuals for purposes other than those prompting the initial collection of the information, which could compromise privacy.[38]

Greater concerns arise if a consolidated Smart Card is issued for multiple uses and purposes. A State might decide, for example, to issue an omnibus Smart Card for all State governmental transactions such as driver's,

---

[31] "[I]nformation privacy should be viewed as a societal value justifying a resolution in the public interest, much like environmental policy and other societal concerns, with less emphasis on individual self-policing and market-based mechanisms." James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1 (2003).

[32] John Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 67 (2002).

[33] http://www.gcn.com/online/vol1_no1/21158-1.html (Last visited Nov. 8, 2007).

[34] A. Michael Froomkin, *Regulation and Computing and Information Technology: Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996).

[35] Stan Karas, *Privacy, Identity, Databases*, 52 AM. U.L. REV. 393 (2002).

[36] http://www.efc.ca/pages/media/2001/2001-01-15-a-torontostar.html (Last visited Nov. 8, 2007).

[37] Don Butler, *Big Bio Is Watching You: The Biometric State May be Closer Than We Thought*, MONTREAL GAZETTE, June 17, 2007, *available at* http://www.canada.com/montrealgazette/news/insight/story.html?id=444ed893-4237-45b6-96a6-d80a4b90d807 (Last visited Nov. 8, 2007).

[38] GAO-05-82, Smart Card Usage Is Advancing Among Federal Agencies (Oct. 6, 2004), http://www.gao.gov/htext/d0584t.html (Last visited Nov. 8, 2007).

boating, and hunting licenses; Medicare; and transit. Moreover, omnibus public/private cards might be issued that also allow banking and credit transactions or even frequent flyer mileage awards. One source identifies several potential problems with such omnibus cards:

• *Centralization of personal information collection*—A single card used for different purposes runs the risk of creating a centralized warehouse of data about an individual's activities. Today, various recordkeepers have information that reflects different aspects of an individual's life. The bank has banking records, doctors have medical records, and credit card companies have records of credit transactions. The walls between these records protect individual privacy in two ways. First, they limit, to some extent, the damage to individual privacy that occurs through either misuse by an authorized user or unauthorized access by an intruder. Second, they place checks on the surveillance and monitoring capacity of each system. If all of an individual's transactions occurred through, or were recorded at, the same source, we would create a powerful center of data on all citizens that would be ripe for misuse and abuse.
• *Means for new social controls*—The issuance, revocation, or withholding of such a card could be used to control social behavior, limit an individual's activities, or punish unrelated activities. Today, specific tokens enable specific activities. While losing a driver's license may limit a person's ability to drive, it does not impact on his or her ability to purchase goods in the market, seek health care, or engage in other transactions. A single card does not provide the same flexibility.
• *Greater collection and use of personal information*—When a single card is used across all transactions, it could become a default personal identification card or a national ID card. As mentioned above, many of our daily activities require far less personal means of certification. A single certifier will result in more data being collected than is needed for many interactions. In the most extreme case, it could lead to every online interaction being fully identifiable and traceable to an individual. Utilizing a single card for all purposes could create an electronic trail of all personal interactions.[39]

II. THE EVOLUTION OF CONCERNS OVER PRIVACY AND SECURITY SINCE SEPTEMBER 11, 2001 (9/11)

To date, more attention has been focused on airline passengers than surface transportation passengers, probably because commercial aviation has been targeted most prominently by terrorists.[40] Yet as the bombings of Madrid commuter trains and London Underground trains reveal, surface passengers are as vulnerable, if not more vulnerable. The bombings of commuter trains in Madrid in 2004 killed 191 people and wounded 2,000. The bombings of London's Underground subway in 2005 killed 56. In Mumbai in 2006, explosions in commuter trains and stations during rush hours killed 174. In response, in the United States, state patrolmen, national guardsmen, additional police, and sniffer dogs have been placed at various transit stations and parking facilities and on transit vehicles.[41] Though the United States has not yet experienced such an attack on its urban transit system, its vulnerability to attack is much higher than that of the air transportation system post-9/11.

The British were able to bring suspected terrorists to justice through their widespread use of surveillance cameras in public areas throughout the United Kingdom, including Underground transit facilities. Smart Cards offer yet another means of both preventing terrorist access to the system and monitoring passenger whereabouts following a terrorist attack so as to facilitate law enforcement. Thus, Smart Cards offer a means both to serve as an additional layer of prevention and to facilitate conviction of those guilty of terrorist acts.

Though the national interest in individual privacy was a dominant public policy prior to the terrorist events of September 11, 2001, security became a dominant concern after 9/11. There is a natural tension between these values because enhanced security measures are often more intrusive into individual rights, including personal privacy.

Created shortly after 9/11, the Transportation Security Administration (TSA) has jurisdiction over all modes of transportation. TSA has begun a biometrically-coded Trusted Traveler Program to allow the collection of personal information and a biometric identifier in a card permitting more expeditious access through airport security bottlenecks. Over time, one may anticipate that the programs designed for the airline industry likely will be transferred to other passenger modes.

To expedite passenger flows, the Department of Homeland Security (DHS) announced a voluntary program whereby travelers could secure a Trusted Traveler card by consenting to a background check and biometric identification that would give them more expeditious travel through security bottlenecks at airports.[42] The United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) was implemented by the DHS on January 12, 2004.[43] It was de-

[39] Ari Schwartz, Smart Cards at the Crossroads, http://www.cdt.org/digsig/idandsmartcards.shtml (Last visited Nov. 8, 2007).

[40] *See, e.g.*, Star, *supra* note 1, at 251; Paul Stephen Dempsey, *Aviation Security: The Role of Law in the War Against Terrorism*, 41 COLUM. J. OF TRANSNAT'L L. 649 (2003).

[41] *Gov. Rell Says Heightened Transit Security Measures to End as Threat Level Drops*, U.S. States News, Aug. 12, 2005, *available at* http://www.ct.gov/governorrell/cwp/view.asp?A=1761&Q=300118 (Last visited Nov. 8, 2007).

[42] Betzel, *supra* note 8, at 517, 534.

[43] See 69 Fed. Reg. 53318 (Aug. 31, 2004). See Eric P. Haas, *Back to the Future? The Use of Biometrics, Its Impact on Air-*

signed to create an integrated, automated entry and exit system at the U.S. border points that records the arrival and departure of aliens, verifies their identities, and authenticates their travel documents through the comparison of biometric identifiers.[44] The US-VISIT program employs digital finger scans and photos to screen foreign nationals entering the United States against watch lists.[45] After 9/11, the federal government mandated that airline and airport employees have identity cards to access secured portions of the airports.

The TSA and its predecessor on security, the Federal Aviation Administration, have had a computer-based airline passenger screening program since the late 1990s. The newer Computer Assisted Passenger Pre-Screening (CAPPS II) program collects and correlates passenger information such as passenger name, address, birth date, and credit card number against various governmental and commercial databases, such as criminal records, to produce a security code of green, yellow, or red.[46] It also requires airlines to turn over all passenger records and other personal information to the TSA.[47] Those passengers coded red are denied boarding.[48] In Canada, passenger screening involves denied boarding of:

- An individual who has been involved in a terrorist group and who, it can reasonably be suspected, will endanger the security of any aircraft or aerodrome, or the safety of the public, passengers, or crew members.
- An individual who has been convicted of one or more serious and life-threatening crimes against aviation security.
- An individual who has been convicted of one or more serious and life-threatening offences and who may attack or harm an air carrier, passengers, or crew members.[49]

These types of restrictions could be incorporated into Smart Card utilization at transit entry points, to deny entry to persons posing a safety or security threat.

The International Civil Aviation Organization (ICAO) recommends the use of facial features as the primary means of biometric identification in RFID-embedded passports.[50] In 2005, ICAO adopted a new Standard and Recommended Practice requiring that all member states (including the United States) issue biometrically enhanced machine readable passports (MRPs) and travel documents (MRTDs) not later than April 1, 2010.[51] In August 2006, the United States began issuing passports containing RFID chips encoded with biometric and biographical information. One can envision that MRTDs eventually may be required domestically as well.

The impact of the Patriot Act on individual privacy has been much debated. One view, expressed by Professor Orin Kerr of George Washington University, is:

> The Patriot Act did not tilt the balance between internet privacy and security strongly in favor of security. Most of the Patriot Act's key changes reflected reasonable compromises that updated antiquated laws. Some of these changes advance law enforcement interests, but others advance privacy interests, and several do both at the same time. None challenged the basic legal framework that Congress created in 1986 to protect Internet privacy. Studying the Internet surveillance provisions of the Act suggests that the media portrayal of the Patriot Act as "extraordinary" and "panicky legislation" has little in common with the law Congress actually enacted.[52]

To address national security concerns, there has been some discussion of creating a National Identity Card, though there are Orwellian concerns about Big Brother's administration of such a system.[53]

III. FEDERAL PRIVACY LAW

A. Constitutional Law

1. Searches and Seizures

The Fourth Amendment of the U.S. Constitution protects "the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[54] Thus, a threshold question is whether information procured through a Smart Card, such as biometric and other personal data, constitutes a search or seizure, and secondly, if so, whether the search or seizure is "reasonable." The question also arises whether the intrusion constitutes a violation of the individual's right of privacy.[55]

The U.S. Supreme Court has refused to find that a seizure has occurred where a governmental official questions and makes identification requests of people in

---

port Security, and How This Technology Should be Governed, 69 J. AIR L. & COM. 459, 482–83 (2004).

[44] Margaret Betzel, *supra* note 8.

[45] Butler, *supra* note 37.

[46] See Haas, *supra* note 43.

[47] See Pablo Mendes de Leon, *The Fight Against Terrorism Through Aviation: Data Protection Versus Data Production*, AIR & SPACE L. 31, at 320–330 (2006).

[48] Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 709–10 (2004).

[49] http://www.skyserviceairlines.com/eng/airline/arrivalsdepartures/SpecialBulletins.asp (Last visited Nov. 14, 2007).

[50] Butler, *supra* note 37.

[51] ICAO, 1 MRTD Report 5 (2006).

[52] Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 N.W. U.L. REV. 607, 625 (2003).

[53] *See, e.g.*, Steinbock, *supra* note 48, at 697.

[54] U.S. CONST. amend. IV.

[55] Much of the law review literature focuses on privacy in terms of abortion rights, Internet use, and health care. There is some literature on the subject of Smart Cards, mostly on the issue of the airline Trusted Traveler program. *See, e.g.*, Dempsey, supra note 40, at 649, 724; Haas, *supra* note 43, at 459, 480 (2004).

confined circumstances. Thus, in *United States v. Drayton*, plainclothes police requests for permissions to search the baggage or persons of interstate bus travelers during a routine drug and weapons search was upheld as not constituting a Fourth Amendment search or seizure.[56] Similarly, in *Florida v. Bostick,* the U.S. Supreme Court reversed a Florida Supreme Court holding that due to the cramped confines of a bus, the questioning of a person by police officers would so deprive a person of his freedom of movement as to constitute a per se Fourth Amendment seizure. [57]

More recently, the Court has held that an encounter with a police officer only becomes coercive, and therefore a seizure, if a reasonable person would not feel free to decline the request or terminate the encounter.[58] According to Professor Steinbock, "This reasoning easily applies to identification requests that are ancillary to other required official interactions…."[59] Thus, demanding that a transit passenger produce a Smart Card likely would not constitute an unconstitutional search or seizure, even if the person demanding the card were a transit policeman, so long as the other circumstances did not reveal an aura of coercion in the passenger's freedom of movement. Moreover, in a long line of cases, the courts have steadfastly upheld security screening checks and personal identification requirements at airports. Airport terminals are not meaningfully different as venues for Constitutional analysis than transit terminals.

2. A Reasonable Expectation of Privacy

Though the right to privacy is nowhere explicitly mentioned in the U.S. Constitution, in *Griswold v. Connecticut*[60] the U.S. Supreme Court found such a right contained in the "penumbras" of the Constitution. In this case, a married couple's use of contraceptives in their bedroom was protected by a zone of privacy free from governmental intrusion.[61] *Griswold* was the first U.S. Supreme Court decision to recognize a Constitutional right of privacy.

Justice Harlan's Concurring Opinion in *Katz v. United States*[62] identified a two-part test for determining those occasions in which a right to privacy should be recognized: (1) there must be a subjective expectation of privacy, and (2) the individual's expectation must be reasonable. If there is no reasonable expectation of privacy, then there has not been an occasion to violate the individual's Fourth Amendment right.[63] Thus a Fourth Amendment search occurs where "an expectation of privacy that society is prepared to consider reasonable is infringed."[64] Stated differently, obtaining and examining evidence may constitute a Fourth Amendment search, "if doing so infringes an expectation of privacy that society is prepared to recognize as reasonable."[65]

The flip side of this analysis is that a legitimate expectation of privacy is not to be expected when the action in question is openly displayed to the public, such as in a transit station or vehicle. Hence, that which can be seen or overheard by others is not off limits to law enforcement officers or other governmental officials or employees.[66] A passenger passing through a turnstile at a transit station, or standing in a transit vehicle, is exhibiting publicly observable conduct. Should the transit provider monitor his or her movements either through video cameras in the station or vehicle or through a centralized electronic assessment of the individual's whereabouts by reading his or her Smart Card, no reasonable expectation of privacy would have been violated, until perhaps he or she stepped into the stall of a rest room.

In *Smith v. Maryland,*[67] the Supreme Court held that an individual did not have a reasonable expectation even in the telephone numbers that he or she dialed. The Court observed that as an individual understands that the telephone company keeps a record of the phone numbers one dials for billing purposes, no additional incremental invasion of privacy occurs when police place a pen register on the user's line. Because the phone number does not disclose the content of the conversation, it does not constitute a Fourth Amendment search. Recording the information obtained from swiping a Smart Card across a reader would seem to pose no more Constitutional concerns than dialing a telephone number, and would therefore also likely withstand a Fourth Amendment challenge.

In *Paul v. Davis*,[68] the Supreme Court addressed the disclosure of personal information by a public official. In *Paul,* a police chief circulated a photograph of Davis (who had been arrested but whose charges had been dismissed) on a list of "active shoplifters." The Court found that the right of privacy extended only to "fundamental" activities and that arrest information did not constitute such a fundamental activity.[69]

The Supreme Court developed the framework for a Constitutional right to information privacy in *Whalen v.*

[56] United States v. Drayton, 536 U.S. 194, 201-02, 122 S. Ct. 2105, 2111, 153 L. Ed. 2d 242, 252 (2002).

[57] Florida v. Bostick, 501 U.S. 429, 436, 111 S. Ct. 2382, 2387, 115 L. Ed. 2d 389, 399 (1991).

[58] Brendlin v. California, 127 S. Ct. 2400, 168 L. Ed. 2d 132 (2007).

[59] Steinbock, *supra* note 48, at 697, 712.

[60] 381 U.S. 479, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965).

[61] The Court subsequently extended privacy to abortion during the first trimester in Roe v. Wade. 410 U.S. 113, 93 S. Ct. 705, 35 L. Ed. 2d 147 (1973).

[62] 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

[63] Haas, *supra* note 43, at 459.

[64] Maryland v. Macon, 472 U.S. 463, 469, 105 S. Ct. 2778, 2782, 86 L. Ed. 2d 370, 376 (1985) (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

[65] Skinner v. Ry. Labor Executives' Assoc., 489 U.S. 602, 615, 109 S. Ct. 1402, 1412, 103 L. Ed. 2d. 639, 658 (1989).

[66] See Brogan, *supra* note 32, at 65, 73–74 (2002).

[67] 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979).

[68] 424 U.S. 693, 99 S. Ct. 1155, 47 L. Ed. 2d 405 (1976).

[69] *Id*. at 713.

Roe,[70] a case involving a state statute that established a centralized computer file containing names and addresses of all persons who obtained certain prescription drugs. In upholding the state statute, the Court identified two interests affected by this governmental gathering of information: (1) "the individual interest in avoiding disclosure of personal matters," and (2) "the interest in independence in making certain kinds of important decisions."[71] The Court observed that *Paul* was controlling for the second of these two categories. It avoided fundamental activity analysis, instead concluding that the statute posed no significant threat to privacy.

Though *Griswold* seemed to protect the sanctity of one's bedroom against governmental intrusion, the public highways appear to stand on a different footing. In *United States v. Knotts*,[72] the U.S. Supreme Court upheld the use of a radio frequency tracking device (a "beeper") to track a suspected criminal from his purchase of chemicals back to his drug lab. Though the Eighth Circuit had found the use of the beeper to constitute an unreasonable search, the Supreme Court reversed, relying on *Katz* and holding that one does not enjoy a reasonable expectation of privacy when traveling on public roads.[73]

Absent individualized suspicion (reasonable cause), the U.S. Supreme Court explicitly has upheld the constitutionality of highway search and seizures in three areas: (1) border patrol checkpoints, (2) sobriety checkpoints, and (3) information-seeking checkpoints. In dictum, the Court also has indicated that other situations would warrant a reasonable search and seizure, including: (4) a roadblock designed to thwart an imminent terrorist attack, (5) a roadblock designed to catch a dangerous criminal likely to flee via a particular route,[74] (6) a roadblock for the purpose of verifying drivers' licenses and registrations,[75] and (7) searches at airports or government buildings.[76] Searches at transit stations would appear to stand on the same footing as searches on highways or at airports, which have received widespread judicial support.

In the context of Smart Cards, the threshold question is what information about individual passengers is being gathered, and whether individuals have a reasonable expectation of privacy in such information. This might include an wide array of information, such as:

- How much money has been deposited to pay for transit services.
- Where the Smart Card is passing, or being swiped.
- Demographic information about the passenger.
- Biometric information about the passenger.

The transit provider might also correlate the information obtained with information available from other sources, such as information obtained from credit institutions or police or security agencies.

The cases seem to suggest that where the individual is located is important in the determination as to whether a privacy interest exists. Thus, an individual in his home enjoys greater protection against privacy intrusions than an individual on the public highway. Readily observable information obtained while the passenger is in a public transit station or on a transit vehicle likely would not be protected. Where the Smart Card is swiped or passes likely would not be deemed protected privacy.

Certain demographic information, such as the name, address, and telephone number of the person to whom a Smart Card is issued, also likely would not be deemed private information. Yet, one's political or religious affiliation might be considered highly private. One's gender or race ordinarily would be publicly observable, yet one can imagine that a court would be troubled by the collection of such data unless it understood the purpose for which it was to be used. Thus, the reasonableness of the government's action also is of importance in the Constitutional assessment.

Biometric information may intrude on reasonable expectations of personal privacy. One source argues that although biometric hand scanning or facial scanning does not intrude upon the Fourth Amendment, retinal or iris scans constitute Fourth Amendment searches:

> Like fingerprints, retina and iris scans will…constitute Fourth Amendment searches because of the ability of these biometric measures to reveal personal medical information. Furthermore, although none of these biometrics involves physically entering a person's body in a conventional sense, such as using a needle to obtain a blood sample, the means employed to collect the biometric measurements may, nonetheless, constitute a physical intrusion and, thus, be deemed a search. In *Kyllo v. United States*, the Supreme Court recently held that the use of thermal imaging technology to detect the amount of heat radiating from a house was a search even though the device could not penetrate the walls of the house. Although *Kyllo* dealt with searching a person's house and not the person's body, the house in *Kyllo* is analogous to a person's body. For example, retina measurements are obtained by an electronic scan of the retina using a beam of incandescent light to map the pattern of blood vessels in the retina. Scanning of the retina, like the scanning of the house at issue in *Kyllo*, does not involve physical penetration. However, because the use of a beam of light to map a person's retina reveals information that could otherwise not be obtained without physical intrusion, such action may also be viewed as a search even though the method of obtaining the information does not physically invade the body in a conventional sense.[77]

[70] 429 U.S. 589, 97 S. Ct. 869, 51 L. Ed. 2d 64 (1977).

[71] Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U.L. REV. 803, 810 (2003).

[72] 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983).

[73] Knotts, 460 U.S. at 279.

[74] City of Indianapolis v. James Edmond, 531 U.S. 32, 44, 121 S. Ct. 447, 148 L. Ed. 2d 333 (2000).

[75] Delaware v. Prouse, 440 U.S. 648, 99 S. Ct. 1391, 59 L. Ed. 2d 660 (1979).

[76] Edmond, 531 U.S. at 48-49.

[77] Star, *supra* note 1, at 251, 261.

It is, as yet, unclear whether the courts will adopt such a view. It would seem that one's facial features or retina are publicly observable physical features, though not at the detail permitted with modern computer technology. It would also seem that a person has the option of not purchasing a Smart Card if he or she is fearful of a privacy intrusion, in the same way one has the option not to acquire a passport. Individual citizens have a Constitutional right to travel. Though there is a Constitutionally-recognized right to travel,[78] and infringements upon that right must satisfy a compelling governmental interest,[79] no court has yet circumscribed the federal government's right to obtain personal information for use in passport control.

3. Reasonableness of the Government's Intrusion Upon Privacy

In *Kyllo v. United States,*[80] the U.S. Supreme Court held that the warrantless use of a thermal imaging device to scan heat emanating from a home constituted an unreasonable search under the Fourth Amendment. The use of sense-enhancing technology to obtain information that "could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" ran afoul of the Fourth Amendment, at least when the technology "is not in general public use."[81] In dissent, Justice Stevens pointed out that the limitation on technology "not in general public use" was "somewhat perverse," because the evolution of technology and its wider availability over time will increase the threat to privacy.[82]

Once it is determined that the individual has a legitimate expectation of privacy in the information being sought, the analysis turns to an assessment of the purposes of government in seeking such information. In the absence of individualized suspicion, the reasonableness of such a search depends on balancing the interests of the government vis-à-vis the extent of the intrusiveness of the search.[83] Reasonableness is judged by balancing the search's intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests. The factors to be considered include the nature of the privacy interest upon which the search intrudes, the character of the intrusion, the immediacy of the governmental concern, and the efficacy of the search for meeting it.[84] This requires an evaluation of: (1) the reasonableness and legitimacy of the government's interest, (2) the extent to which the action taken can be said to advance that interest, and (3) the degree of intrusion of the search or seizure.[85] Professor Daniel Steinbock concludes: "On the information-gathering side of the process, there are substantial Fourth Amendment questions raised by mandated reporting of personal information produced in the course of everyday life. Though this practice should be regarded as a search, it may not be an unreasonable one, up to a point."[86]

In *Skinner v. Railway Labor Executives' Ass'n*,[87] the U.S. Supreme Court upheld the Constitutionality of U.S. DOT regulations requiring blood and urine testing for the presence of drugs of certain "safety sensitive" employees involved in certain accidents or those who violated certain safety rules. The railroad employees' expectations of privacy were diminished by their employment in an industry extensively regulated for safety, and the persons tested "discharge duties fraught with such risks of injury to others that even a momentary lapse of attention can have disastrous consequences."[88] Weighing the government-as-employer interest in stopping the misuse of drugs by employees in safety-sensitive positions against the individual interest in privacy, the Court found the requirement of a urinalysis test reasonable.[89]

Fourth and Fifth Amendment cases addressing the reasonableness of the government's interest have arisen in the transit context. For example, in *Beharry v. New York City Transit Authority,*[90] a Federal District Court held, "the Authority's request that Beharry provide a small urine sample within a two-hour period caused a minimal interference with Beharry's privacy rights, which must be outweighed by the Authority's concerns with protecting the safety of its employees and customers."[91] In *Holloman v. Greater Cleveland Regional Transit Authority*,[92] the Sixth Circuit held that the transit authority had a compelling governmental interest in "protecting the safety of its passengers and the general public by ensuring that its drivers do not operate buses while under the influence of alcohol or drugs," and that this interest outweighed the employee's expectations of privacy.[93] In *Amalgamated Transit Union v. Suscy,*[94] the

[78] *See, e.g.*, United States v. Guest, 383 U.S. 745, 86 S. Ct. 1170, 16 L. Ed. 2d 239 (1966).

[79] Shapiro v. Thompson, 394 U.S. 618, 634, 89 S. Ct. 1322, 1331, 22 L. Ed. 2d 600, 615 (1969).

[80] 533 U.S. 27, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001).

[81] *Id*. at 34.

[82] *Id*. at 47 (Stevens, J., dissenting).

[83] Chandler v. Miller, 520 U.S. 305, 318, 117 S. Ct. 1295, 1303, 137 L. Ed. 2d 513, 525 (1997). See Jill Dorancy-Williams, *The Difference Between Mine and Thine*: *The Constitutionality of Public Employee Drug Testing*, 28 N.M. L. REV. 451 (1998).

[84] Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 653, 115 S. Ct. 2386, 2391, 132 L. Ed. 2d 564, 574 (1995).

[85] Steinbock, *supra* note 48, at 697, 728–29 (2004).

[86] *Id*. at 701.

[87] Skinner v. Rwy. Labor Executives' Ass'n, 489 U.S. 602, 617, 109 S. Ct. 1402, 1413, 103 L. Ed. 2d 639, 660 (1989). See Dorancy-Williams, *supra* note 83.

[88] Skinner, 489 U.S. 602, at 628.

[89] Skinner, 489 U.S. at 614. See also Drake v. Delta Airlines, Inc., 923 F. Supp. 387, 396-97 (E.D.N.Y. 1996), *aff'd in relevant part*, Drake v. Delta Airlines, Inc., 147 F.3d 169, 170-71 (2d Cir. 1998). Beharry v. MTA, 1999 U.S. Dist. Lexis 3157 (E.D.N.Y. 1999).

[90] 1999 U.S. Dist. Lexis 3157 (E.D.N.Y. 1999).

[91] *Id*. at 30.

[92] 1991 U.S. App. Lexis 6904 (6th Cir. 1991).

[93] *Id*. at 2.

Seventh Circuit held, "the public interest in the safety of mass transit riders outweighs any individual interest in refusing to disclose physical evidence of intoxicating or drug abuse."[95]

Further, a long line of checkpoint cases have upheld police demands for drivers' licenses and automobile registrations as reasonable. Though the Supreme Court has not yet had occasion to rule on checkpoint inspections on pedestrians, the Court has held that forcing people to stop at a checkpoint constitutes a Fourth Amendment seizure; the issue is whether a suspicionless seizure is reasonable.[96] The Court has distinguished between checkpoints whose principal purpose is to "detect evidence of ordinary criminal wrongdoing," and those whose focus is instead on serving some "special needs" other than crime control, the former being per se unreasonable absent some individualized indication of criminality and the latter permissible. In dicta, the Court has indicated that certain stops are not unreasonable under Fourth Amendment analysis, including roadblock-type stops for highway license and registration checks, and "to thwart an imminent terrorist attack."[97] Professor Steinbock notes that,

> Anti-terrorism identification checkpoints would stretch the rationale of "special needs" or "non-criminal purpose" searches to its current limit, but it is not likely that courts would find their use to be distinguishable from general crime fighting, particularly in the face of the enormous public pressures that would probably lie behind their creation.[98]

Hence, an ordinary stop of the passenger for purposes of swiping the card to deduct fares might not be a search or seizure at all, and if it was, likely would be deemed reasonable in any event. Were the government, however, to monitor the location of individual transit passengers as they passed through the network, a more serious issue would be raised, though no more than that posed by surveillance cameras in transit stations and vehicles. A stop predicated on security concerns, or a denial of entry into the transit system, if reasonably conducted and predicated on reasonable grounds, might well satisfy the government's compelling interest in protecting public safety.

Thus, the government's strong interest in protecting public safety can make even an intrusive search reasonable, and therefore consonant with the Fourth Amendment's protection against unreasonable searches and seizures. In the post-9/11 environment, the government's bona fide interest in protecting the public against threats to security likely would support governmental intrusion into personal privacy, so long as the intrusion was reasonably related to security.

But a search in a public transportation venue does not guarantee judicial support. As the Ninth Circuit observed in *United States v. $ 124,570 U.S. Currency*,[99] an administrative airport search would only be upheld if the search is "no more intrusive than is necessary to achieve air safety."[100] In so holding, the court "recognized the danger that the screening of passengers and their carry-on luggage for weapons and explosives will be subverted into a general search for evidence of crime."[101] Thus, the court held that an administrative airport search cannot also serve an unrelated law enforcement purpose, but must be limited to the goal of achieving travel safety.

So too, the requirement of a transit provider that passengers provide personal information for the issuance of a Smart Card must satisfy a legitimate governmental purpose. Requiring the card to be swiped would satisfy the legitimate governmental need to ensure that the person is paying for the transportation being consumed. Certain information could be justified by the need of the transit provider to obtain information useful for marketing or planning purposes, such as advertising or choosing the venue of future transit stations, lines, or vehicles. More intrusive information could be justified by a need to protect public safety and security. Given the broad sway afforded the need to protect public security in transportation in the post-9/11 world, one could even imagine a legitimate government need to have information correlated with the Smart Card on membership in extreme and radical political and religious organizations with a history of terrorism.

Therefore, it seems that quite a wide spectrum of personal information could be sought or correlated by transit providers in or related to the issuance and use of Smart Cards. However, personal privacy could be protected in other ways, such as the issuance of regulations by the transit providers establishing guidelines as to what information is to be collected and how it is to be stored, used, and disseminated, and whether the individual has the right to access and correct such information. In other words, the wide latitude given governmental institutions by the Constitutional jurisprudence could still be limited internally. So long as such limitations did not conflict with federal security laws or regulations, they likely would be upheld.

B. Federal Statutes

Since the 1970s, the U.S. Congress has passed several pieces of legislation attempting to protect individual privacy against governmental intrusions or dissemination. Yet in the post-9/11 world, the federal government has been given increased authority to monitor individual activity in the "war on terrorism."

[94] 538 F.2d 1264 (7th Cir. 1976).

[95] Amalgamated Transit Union v. Suscy, 538 F.2d 1264 (7th Cir. 1976).

[96] City of Indianapolis v. Edmond, 531 U.S. 32, 40, 121 S. Ct. 447, 453, 148 L. Ed. 2d 333, 342 (2000); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 450, 110 S. Ct. 2481, 2485, 110 L. Ed. 2d 412, 420 (2004).

[97] Steinbock, *supra* note 48, at 697, 724–25.

[98] *Id*. at 726.

[99] United States v. $124,570 U.S. Currency, 873 F.2d 1240, 1246 (9th Cir. 1989).

[100] 873 F.2d at 1245 (citing Davis, 482 F.2d at 910).

[101] *Id*. at 1243.

One source notes three overriding characteristics of U.S. privacy law that account for its diversity and complexity: "(i) the tendency of modern privacy law to divide into at least two main branches of privacy interests: privacy concerns about autonomy and privacy concerns about personal information; (ii) the variety of different types of privacy laws; and (iii) the specific, context-dependent nature of many privacy laws."[102]

The Fair Credit Reporting Act of 1970 limits the collection and sharing of credit histories by credit bureaus.

The Privacy Act of 1974[103] protects individual privacy with respect to federal agency operations and practices by regulating the government's collection, use, and dissemination of personal information. The Privacy Act applies to information maintained by a federal agency in a "system of records," defined as a group of any records from which information is retrieved via either the name of an individual or by some individually-assigned identifying number, symbol, or other particular.

The Privacy Act requires that a federal agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[104] It also requires the U.S. government to restrict disclosure of personally identifiable records maintained by federal agencies. A federal agency may withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information…could reasonably be expected to constitute an unwarranted invasion of personal privacy."[105] It may also withhold documents that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[106] Examples include "arrest records, discipline records, passport or Social Security numbers, job performance records, union membership cards, and the like."[107]

The Privacy Act structures how information is processed within the public sector through the regulation of recordkeeping and disclosure practices. Individuals have the right to gain access to agency records containing their personal information, and the right to request correction or deletion of information that is inaccurate, irrelevant, or incomplete.[108] The Privacy Act also regulates the use of computer matching by federal agencies when records are matched with those of other federal, state, or local government records. Federal agencies involved in computer matching programs must:

1. Negotiate written agreements with the other agency or agencies participating in the matching programs;
2. Obtain the approval of the matching agreement by the Data Integrity Boards (DIB) of the participating federal agencies;
3. Publish notice of the computer matching program in the *Federal Register*;
4. Furnish detailed reports about matching programs to Congress and the Office of Management and Budget;
5. Notify applicants and beneficiaries that their records are subject to matching; and
6. Verify match findings before reducing, suspending, terminating, or denying an individual's benefits or payments.[109]

However, the Privacy Act had several structural weaknesses. It failed to restrict the practices of private corporations or confer upon individuals standing to pursue a cause of action against state or local governments; only federal agencies could be held accountable, and then only for administrative injunctions and minimal damages. Moreover, the "routine use" exemption seemingly swallows the rule.[110]

The 1986 Amendments to the Electronic Communications Privacy Act of 1968[111] criminalize unauthorized access to electronic communications.[112]

---

[102] Glancy, *supra* note 12.

[103] 5 U.S.C. § 552.

[104] 5 U.S.C. § 555a(3)(1).

[105] 5 U.S.C. § 552b(7)(c).

[106] 5 U.S.C. § 552b(6).

[107] Lahr v. Nat'l Transp. Safety Bd., 453 F. Supp. 2d 1153, 1177 (2006).

[108] Norian, *supra* note 71, at 803, 818.

[109] 5 U.S.C. § 552a.

[110] Black, *supra* note 12, at 397, 416–17.

[111] 18 U.S.C. § 2701.

[112] (a) Offense. Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment. The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

The Computer Matching and Privacy Protection Act of 1988[113] amended the Privacy Act[114] by designating the manner in which federal agencies could engage in computer matching and by providing certain protections for those applying for and receiving federal benefits.

Section 7201 of the Omnibus Budget Reconciliation Act of 1990[115] amended the Privacy Act by providing certain protections for individuals receiving federal benefits.

The Health Insurance Portability and Accountability Act of 1996 provides privacy protection for electronically transmitted health information.[116]

The Children's Online Privacy Protection Act of 1998[117] requires parental consent for the collection of information concerning children under the age of 13.

The Financial Services Modernization Act of 1999[118] (also known as the Gramm-Leach-Bliley Act) protects the privacy of consumer information held by financial institutions. Every financial institution has a continuing obligation to protect the privacy of its customers and safeguard the confidentiality of their customers' nonpublic personal information.[119] Regulatory agencies are obliged to promulgate regulations to ensure that banks and other financial institutions adopt procedures and safeguards:

> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[120]

The E-Government Act of 2002[121]requires federal agencies to conduct privacy impact assessments before developing or procuring information technology that collects, maintains, or disseminates personally identifiable information. Agency officials must develop appropriate privacy measures when implementing Smart Card-based systems and ensure that privacy impact assessments are conducted.[122]

The Intelligence Reform and Terrorism Prevention Act of 2004[123] establishes an "information sharing environment" (ISE) among federal, state, and local intelligence gathering agencies and requires the President to ensure it is created "in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[124] The ISE shall incorporate protections for individuals' privacy and civil liberties.[125]

The Act also established a Privacy and Civil Liberties Oversight Board, consisting of five members appointed by the President.[126] Though established by Congress in 2004, the President did not appoint its members until 2006. The Board's mission is to advise "the President and other senior Executive Branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and Executive Branch policies related to efforts to protect the Nation against terrorism."[127]

C. Administrative Practice

On August 27, 2004, President George W. Bush issued Executive Order 13353 establishing the Board on Safeguarding Americans' Civil Liberties, in order to "strengthen protections for the rights of Americans in the effective performance of national security and homeland security functions…."[128]

On December 15, 2005, President George W. Bush issued a *Memorandum to Heads of Executive Departments and Agencies on Guidelines and Requirements in Support of the Information Sharing Environment*.[129]

---

[113] 100 Pub. L. No. 503, 102 Stat. 2507 (1988).

[114] 5 U.S.C. § 552a.

[115] 101 Pub. L. No. 508, 104 Stat. 1388 (1990).

[116] Health Insurance Portability and Accountability Act of 1996, 104 Pub. L. No. 191, 110 Stat. 1936 (1996).

[117] 15 U.S.C. §§ 6501–6506.

[118] 15 U.S.C. § 6801.

[119] 15 U.S.C. § 6801(a).

[120] 15 U.S.C. § 6801(b).

[121] Pub. L. No. 107-347, 115 Stat. 2899, codified at 44 U.S.C. § 101.

[122] See http://www.whitehouse.gov/omb/egov/g-4-act.html (Last visited Nov. 14, 2007).

[123] 108 Pub. L. No. 458, 118 Stat. 3638 (2004).

[124] 6 U.S.C. § 485(b)(1)(A).

[125] 6 U.S.C. § 485(b)(2)(H).

[126] 5 U.S.C. § 1601.

[127] 6 C.F.R. § 1000.3; 72 Fed. Reg. 17789 (Apr. 10, 2007). See also http://www.whitehouse.gov/privacyboard/ (Last visited Nov. 8, 2007). In 2004, Sen. Patrick Lahey (D-Vt.) characterized RFID tags as "barcodes on steroids…poised to become the catalyst that will launch the age of micro-monitoring." He continued, "The RFID train is beginning to leave the station, and now is the right time to begin a national discussion about where, if at all, any lines will be drawn to protect privacy rights." Brito, *supra* note 3.

[128] 69 Fed. Reg. 53585 (Aug. 27, 2004).

[129] On the issue of protecting the privacy rights of Americans, it provided:

> As recognized in Executive Order 13353 of August 27, 2004, the Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.
>
> (i) Within 180 days after the date of this memorandum, the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, shall (A) conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, (B) develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of

Certain functions were transferred to the Director of National Intelligence in 2007.[130]

IV. STATE PRIVACY LAW

An exhaustive compendium of all state privacy laws is beyond the scope of this project. This section instead summarizes several relevant state Constitutional provisions, laws, and regulations. Legislation has been introduced in a number of States, including California, Massachusetts, Missouri, and Utah to regulate RFID.[131]

A. Constitutional Law

Though the U.S. Constitution does not explicitly use the term "privacy," many state Constitutions do. Most address it indirectly, by protecting individuals from warrantless searches and seizures.[132] A few, like California, explicitly define privacy as an "inalienable right."[133]

B. Common Law

There are several cases involving Smart Cards and RFID technology in the context of satellite television piracy[134] or patent infringement.[135] However, no federal or state cases have addressed the issue of "Smart Cards" in the context of privacy, or indeed, in the context of transit usage.

In their seminal article in the *Harvard Law Review*, Samuel Warren and Louis Brandeis proclaimed what has become the fundamental principle of American privacy law: the "right to be let alone."[136] Dean Prosser used the Warren and Brandeis methodology to identify four separate "privacy" torts: (1) appropriation of another's name or likeness, (2) intrusion on personal seclusion, (3) public disclosure of private embarrassing facts, and (4) publicity that places an individual in a false light.[137] They all have been embraced by the Restatement (Second) of Torts,[138] and in most of the states' common law.

C. Statutory Law

Texas appears to be the only state to have explicitly addressed privacy requirements for Smart Cards. The Texas statute addresses the use of health information, not transit information. Still, it is instructive of how privacy concerns may be addressed. It limits the class of persons having access to gathered information and the type of information that can be accessed, and provides that storage and communication of information complies with privacy laws. Specifically, the Texas Health and Human Services Commission is authorized to consolidate a cost-effective method for recipient identification and benefit issuance, including the use of Smart Cards, provided that it:

> (2) ensure that all identifying and descriptive information of recipients of each health and human services program included in the method can only be accessed by providers or other entities participating in the particular program;
> (3) ensure that a provider or other entity participating in a health and human services program included in the method cannot identify whether a recipient of the program is receiving benefits under another program included in the method; and
> (4) ensure that the storage and communication of all identifying and descriptive information included in the method complies with existing federal and state privacy laws governing individually identifiable information for recipients of public benefits programs.[139]

However, a number of states have enacted public record laws modeled on the Federal Freedom of Information Act, which include exemptions for the dissemination of information that would constitute an unwarranted invasion of personal privacy.[140] The New York statute provides a detailed definition of what may constitute an unwarranted privacy invasion:

> i. disclosure of employment, medical or credit histories or personal references of applicants for employment;
> ii. disclosure of items involving the medical or personal records of a client or patient in a medical facility;
> iii. sale or release of lists of names and addresses if such

---

personally identifiable information, and (C) submit such guidelines to the President for approval through the Director of OMB, the APHS-CT, and the APNSA. Such guidelines shall not be inconsistent with Executive Order 12333 and guidance issued pursuant to that order.

(ii) Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B) upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

See http://www.whitehouse.gov/news/releases2005/12/20051216-10.html (Last visited Nov. 14, 2007), and http://www.pyramid-tech-eng.com/ISE%20Implementation%20Plan.pdf (Last visited Nov. 14, 2007).

[130] 72 Fed. Reg. 18561 (Apr. 13, 2007).

[131] Brito, *supra* note 3.

[132] For example, South Carolina's Constitution protects individuals against "unreasonable searches and seizures and unreasonable invasions of privacy." S.C. CONST. Ann. art. I, § 10 (2005).

[133] CAL. CONST art I, § 1 (2006).

[134] *See, e.g.*, Direct TV v. Ellebracht, 2002 U.S. Dist. Lexis 27260 (2002).

[135] *See, e.g.*, Leighton Technologies v. Oberthur Card Systems, 358 F. Supp. 2d 361 (2005).

[136] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Norian, *supra* note 108, at 803.

[137] William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[138] Restatement (Second) of Torts §§ 652A–652I.

[139] TEX. GOV'T CODE § 531.080, *et seq.* provides for the potential use of Smart Cards in the State Medicare program.

[140] *See, e.g.*, CAL. GOV'T CODE § 6254; FLA. STAT. § 119.01; 5 ILCS § 140/7; LA. REV. STAT. § 44.1; N.Y. CONSOL. LAW Pub. 0 § 87(2)(b); TEX. GOV'T CODE § 552.001; VA. CODE ANN. § 2.2-3705.7.

lists would be used for commercial or fund-raising purposes;
iv. disclosure of information of a personal nature when disclosure would result in economic or personal hardship to the subject party and such information is not relevant to the work of the agency requesting or maintaining it; or
v. disclosure of information of a personal nature reported in confidence to an agency and not relevant to the ordinary work of such agency; or
vi. information of a personal nature contained in a workers' compensation record, except as provided by section one hundred ten of the workers' compensation law.[141]

Some state statutes apply to information accumulated by public transit providers that may impact Smart Card adoption by them. For example, the State of Washington has enacted a Public Records Act that protects individual rights to privacy.[142] It requires state agencies to promulgate rules and regulations providing full access to public records.[143] Certain information is exempt from disclosure, however. Personal information of employees, appointees, and elected officials is exempt to the "extent that disclosure would violate their right to privacy."[144] Such privacy right is invaded if the "disclosure of information about the person: (1) Would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public."[145] Credit card and debit card numbers, bank and other financial account numbers, and other financial information are exempt from public inspection unless disclosure is required by law.[146] Certain intelligence information is exempt to the extent necessary for "effective law enforcement or for the protection of any person's right to privacy."[147]

The State of Washington has a specific provision exempting certain records held by public utilities and transportation entities. With respect to personally identifying information contained on, *inter alia,* "stored value smart cards and magnetic strip cards," the exemption from disclosure has three exceptions: (1) disclosure to an entity responsible for paying for the transit pass, (2) disclosure to news media when reporting on public transportation or public safety, and (3) disclosure to "governmental agencies or groups concerned with public transportation or public safety."[148] Exemptions from disclosure also exist for individually identifiable records collected for vanpool, carpool, or other ridesharing programs and paratransit.[149]

Georgia's Open Records Act requires that all public records of an agency be available for public inspection, except those exempt from inspection by law or an order of a court.[150] Numerous exemptions exist. One provision specifically exempts "the financial records or travel history of any individual who is a purchaser of a TransCard or Smartcards or similar fare medium." Such financial information includes Social Security Numbers; home and email addresses; telephone numbers; and credit, debit card, and bank account information.[151] Another exempts certain personal information compiled for carpooling or ridesharing programs.[152] Also generally exempt from disclosure in Georgia is information compiled for law enforcement purposes;[153] records that would "compromise security against sabotage or criminal or terrorist acts, and the nondisclosure of which is necessary for the protection of life, safety, or public property…";[154] Social Security Numbers;[155] and certain personal financial information.[156]

Note that both the Washington and Georgia statutes, though protecting privacy by limiting the dissemination of personal information to the public, are silent as to the information that can be acquired by its agencies or the internal use to which such information is put.

V. TRANSIT AGENCIES AND SMART CARDS: POLICIES AND PROCEDURES GOVERNING INFORMATION, ACCESS, AND USE

A. Transit ID Cards

The Washington Metropolitan Area Transit Authority (WMATA) adopted pre-pay magnetic-strip cards in its Metro transit system in the 1970s. In 1999, in a pilot program, WMATA became the first public transit system to adopt Smart Cards. The cards were about the size of a credit card, and their magnetic strips recorded what had been pre-paid and allowed deductions therefrom each time the card was "swiped" through the exit turnstile. By 2004, more than 800,000 Smart Cards (called SmarTrip®) had been sold. One-third of WMATA Metrorail riders use the cards regularly. SmarTrip® also has been expanded to cover Metro parking lots and bus transit.[157]

Since the inaugural launch by WMATA, Smart Cards have been adopted in a number of other cities, while a large number of transit providers are either planning to implement Smart Cards or are studying their implementation. The Chicago Card was the nation's first multi-agency, intermodal Smart Card system for public transit. As of 2004, more than 67,000 Chicago Cards

[141] N.Y. CONSOL. LAW PUB. O § 89.
[142] WASH. REV. CODE ch. 42.56.
[143] *Id*. § 42.56.100.
[144] *Id*. § 42.56.230(2).
[145] *Id*. § 42.56.050.
[146] *Id*. §§ 42.56.230(4), 42.56.270.
[147] *Id*. § 42.56.240(1).
[148] *Id*. § 42.56.330(5).
[149] *Id*. § 42.56.330(3-4).
[150] GA. CODE ANN. § 50-18-70(b).
[151] *Id*. § 50-17-72(a)(20).
[152] *Id*. § 50-18-72(a)(14).
[153] *Id*. § 50-18-72(a)(3), (4).
[154] *Id*. § 50-18-72(a)(15)
[155] *Id*. § 50-18-72(a)(11.1).
[156] *Id*. § 50-18-72(a)(11.3).
[157] http://www.apta.com/research/info/briefings/briefing_6.cfm (Last visited Nov. 9, 2007).

were in use. The system is seamlessly interoperable across the Chicago Transit Authority's (CTA) rail and bus networks, as well as the PACE suburban bus system.[158] Since then, seven Seattle-area transportation agencies have formed a regional intermodal fare collection program that enables customers to use a common interchangeable fare Smart Card (ORCA, or "one regional card for all") on transit, ferry, and rail systems throughout the four-county Central Puget Sound area.[159]

The Metropolitan Atlanta Rapid Transit Authority (MARTA) inaugurated a Smart Card system (named "Breeze") in 2005. The Breeze system allows commuters to use a single card to pay for rail, bus, paratransit, and park-and-ride fees.[160] In Boston, the Massachusetts Bay Transportation Authority (MBTA) is installing automated fare collection equipment at every subway station and on every bus, allowing riders to pay by swiping Smart Cards in their names. Each transaction will be recorded electronically, identifying where users were at a particular time on a particular day.[161]

Similar to the SmarTrip® issued by WMATA is the Maryland Transit Pass, which can be used on Maryland Transit Administration (MTA) local buses, light rail, and Metrorail. The MTA describes the Maryland Transit Pass as

> a rechargeable "smart card" embedded with a computer chip to keep track of the cash value stored on the card. Think of it as an electronic wallet that stores a cash balance directly onto your card. Fares are automatically deducted from the card each time you touch it to the Maryland Transit Pass target on a bus farebox, or on faregates and Ticket Vending Machines.[162]

In 1993, the Bay Area Rapid Transit (BART) and the County Connection (the Contra Costa bus system) tested a Smart Card system that proved unreliable. In 1999, a new system was installed by Motorola at a cost of $61 million. Twenty-six transit agencies in the San Francisco Bay Area began testing a universal transit ticket, known as "TransLink," in January 2002. Coins were replaced by the plastic Smart Card, allowing 4,000 riders a day to pay their fares by sliding the card over an electronic pad. The card was capable either of allowing monthly pass usage or of holding and deducting a stored value of money.[163]

In 2003, seven transit agencies in the four-county Puget Sound area—Community Transit, Everett Transit, Kitsap Transit, King County Metro Transit, Pierce Transit, Sound Transit, and the Washington State Ferries—created the Central Puget Sound Regional Fare Coordination Project, establishing a common Smart Card named ORCA, which began testing in 2006. The card allows seamless intermodal connections between rail, transit, and ferry modes of transport. It also allows each participant to expand its strategic marketing alternatives.[164]

In 2006, the Los Angeles County Metropolitan Transportation Authority, in cooperation with 11 other agencies, announced deployment of a Smart Card system for transit riders (the Regional Transit Access Pass program) for fare payment on all regional rail and bus systems, to be implemented over a 5-year period at a cost of between $32 million and $60 million. A private contractor will build and operate the regional service center to administer cardholder registration, card inventory and distribution, and point-of-sale network management, accessible to passengers through a Web site, interactive voice response phone system, customer service representatives, mail, and fax.[165]

A survey of transit providers disseminated by the Transportation Research Board in late 2006 revealed that, of those responding, 91 percent had not yet adopted Smart Cards.[166] Yet, of that group, 65 percent expected to adopt Smart Cards, many in the near future. One indicated it was evaluating the potential for accepting bank-issued contactless devices for the payment of transit fares. The questionnaire attempted to ascertain what financial, trip, and personal data is gathered; who has access thereto, how long the data is stored; and what privacy and identity theft protections are in place.[167]

---

[158] *Id.*

[159] http://transit.metrokc.gov/prog/smartcard/smartcard.html (Last visited Nov. 9, 2007).

[160] http://www.apta.com/research/info/briefings/briefing_6.cfm (Last visited Nov. 9, 2007).

[161] Thomas Caywood, *Charlie's Watching You*, BOSTON HERALD, Dec. 27, 2005, at 3.

[162] http://www.mdtransitpass.com/faq_transitpass.htm (Last visited Nov. 8, 2007).

[163] Michael Cabanatuan, *Public Transit 'Smart Card' to be Tested: One Ticket Will Pay for Bay Area Travel*, S.F. CHRONICLE, Nov. 30, 2001, reproduced at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2001/11/30/MN24612.DTL (Last visited Nov. 9, 2007).

[164] http://transit.metrokc.gov/prog/smartcard/smartcard.html (Last visited Nov. 9, 2007).

[165] William Welsh, L.A. County Awards Transit Smart-Card Deal, GCN, June 5, 2006, reproduced at http://www.gcn.com/online/vol1_no1/40938-1.html (Last visited Nov. 9, 2007).

[166] Thirty-four transit providers responded to the questionnaire, of which only three were using Smart Cards in late 2006/early 2007.

[167] Essentially, the questionnaire focused on the following issues:

> 1. Do you now use Smart Cards? If not, do you expect to adopt Smart Cards? If so, when?
>
> 2. If you have, or plan to, adopt Smart Cards, for what purpose(s) will they be used? Employee access to secured areas? Passengers? By rail? By bus? Both? Can the card be used for non-transit purposes? If yes, please describe?
>
> 3. If you have adopted Smart Cards, what are the economic benefits you have realized? Can they be quantified? Are there other non-economic benefits you have realized?

Of those transit providers indicating that they were currently using Smart Cards, the following benefits were identified: (1) customer convenience enhanced, (2) product distributed more efficiently, (3) progressive image enhanced, (4) more expeditious movement of passengers through the transit system, and (5) facilitation of innovative marketing and pricing approaches. The type of personal information collected included the passenger's name, address, and telephone number, but not his or her credit card number, checking account number, or driver's license number. Employers were identified if the customer was part of a transit benefit program. One transit provider indicated that it correlated trip data with personal information at the zip code level, but not at the personal level; the others did not correlate trip and personal data, but had the capacity to do so. None correlated personal information with data obtained from outside sources. All restricted the class of persons having access to Smart Card data, usually to database and IT administrators and customer service staff. The data collected by most of the transit providers using Smart Cards fell subject to state freedom of information or privacy laws; one had promulgated its own internal regulations and guidelines addressing these issues. Most noted that the data they collected would be subject to court subpoena.

The Smart Card Alliance lists the following transit providers as having implemented Smart Card systems as of 2007:

- Atlanta/MARTA.
- Boston/MBTA.
- Chicago/CTA (Chicago Card and Chicago Card Plus).
- Houston/Metropolitan Transit Authority of Harris County, Texas/METRO.
- Las Vegas/Monorail.
- Los Angeles/Los Angeles County Metropolitan Transportation Authority (LACMTA) Universal Fare System (UFS).
- Maryland Transit Administration (MTA).
- Miami-Ft. Lauderdale-Palm Beach/Miami-Dade Transit (MDT)/South Florida Regional Transportation Authority (SFRTA) (Universal Automated Fare Collection (UAFC)).
- Minneapolis/St. Paul/Metro Transit.
- New York/Metropolitan Transit Authority (MTA)/New York City Transit (pilot).
- Newark/Port Authority of New York and New Jersey (PANYNJ) and New Jersey Transit (NJT) (SmartLink).
- Orlando/Central Florida Regional Transportation Authority (LYNX)/ Orlando Regional Alliance for Next Generation Electronic Payment Systems (ORANGES).
- Port Authority Trans-Hudson (PATH).
- Philadelphia/Port Authority Transit Corporation (PATCO).
- San Diego/Metropolitan Transit Development Board (MTDB).
- San Francisco/Metropolitan Transportation Commission (MTC) (Translink®).
- Seattle-Puget Sound/King County (KC) Metro.
- Utah Transit Authority (pilot).
- Ventura County.
- Washington/WMATA.[168]

B. Transit Agency Procedures

As a creature of interstate compact not subject to state privacy or freedom of information laws, the multi-jurisdictional WMATA has adopted two policies of relevance by resolution of its Board of Directors: (1) a Public Access to Records Policy, and (2) a Privacy Policy. In them, the WMATA Board recognized the "competing policy concerns between the need to guarantee the public as much access to information as possible and the need to protect the privacy expectations of persons who are the subject of records…."[169] The Public Access to Records Policy is designed to make all official or public records generated in the regular course of business available to the public for inspection or reproduction to the greatest possible extent unless they fall within an exemption from disclosure.[170] A specific exemption exists for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwar-

4. If you have adopted Smart Cards, have you encountered any problems with them? If so, of what nature? Were the problems anticipated or unanticipated?

5. Do you gather personal data from Smart Card users? If so, of what nature?

6. Do you gather financial and trip data from Smart Cards? If so, for how long is it stored? Who can access the data?

7. Are you governed by the privacy laws or regulations of your State or local jurisdiction? If so, could you please provide a copy?

8. Have you adopted policies and procedures governing the collection, storage and dissemination of information from Smart Card users? If so, please provide a copy. What was the process by which such policies and procedures were developed?

9. Have you been asked by non-transit entities for information you have collected in the issuance of Smart Cards? If yes, by whom? By governmental institutions? By judicial institutions? By police or security agencies? By the press? By commercial institutions? How often? Is data collected by you subject to acquisition under FOIA or state public record laws?

10. What procedures and practices have you adopted to protect the privacy and to protect against identity theft of Smart Card users?

[168] http://www.smartcardalliance.org/pages/smart-cards-applications-transportation (Last visited Nov. 9, 2007). See also the Web site of the American Public Transportation Association, http://www.apta.com/research/info/briefings/briefing_6.cfm (Last visited Nov. 9, 2007).

[169] WMATA, Resolution of the Board of Directors of the Washington Metropolitan Area Transit Authority (May 19, 2005).

[170] *Id*. Exhibit A (Public Access to Records Policy) §§ 1.0 and 3.0.

ranted invasion of privacy."[171] WMATA issues SmarTrip® Cards. Identifiable personal information obtained for such cards is exempt from release unless the request is made pursuant to a court order, by a law enforcement official, or by the registered user of the card.[172] Financial and transactional information of WMATA customers is also exempt, but is also subject to these same three exception as cards.[173]

The WMATA Privacy Policy: (1) prevents the disclosure of information about a person without his or her permission; (2) provides the individual with an opportunity to access information about him or her in WMATA records; and (3) gives the individual an opportunity to request amendment of those records.[174] WMATA is authorized to maintain only those records concerning an individual that are "relevant and necessary to accomplish its purpose in accordance with the WMATA Compact."[175] The Federal Privacy Act,[176] specifically prohibits the retention of information of "how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute, by the individual about whom the record is maintained, or pertinent to and within the scope of an authorized law enforcement activity."[177] The names and addresses of passengers may not be sold or rented unless specifically authorized by law.[178] A general rule prohibits the dissemination by WMATA personnel of information obtained by WMATA and not generally available to the public except in the performance of official duties or in connection with judicial proceedings. Moreover, "Any applicable statute, regulation or WMATA policy providing greater privacy protection controls over this policy."[179] Certain records maintained by the Metro Transit Police involving criminal law enforcement are exempt from release.[180]

Dan Grabauskas, MBTA General Manager, insists that MBTA will guard personal travel information collected by the CharlieCard system. "We are doing more to protect the privacy of the card holders than any other transit agency in America," Grabauskas said. MBTA developed a privacy policy after a series of public hearings and meetings with civil rights and privacy watchdogs. The Smart Card automated fare system will record where a passenger boards the system and at what time. It will not record any data on the rider's destination. The information will be archived for 1 1/2 to 2 years.[181] Procedures and policies regarding the collection, storage, and dissemination of information from Smart Card users also are under development at the Metropolitan Atlanta Rapid Transit Authority.

A random search of transit Web sites revealed that virtually no transit providers address privacy concerns associated with Smart Cards. Many do have a "privacy policy" link that addresses privacy concerns associated with visiting their Web sites, but that is an entirely different issue. One exception was the Web site of the University of Washington, which has this entry on a page of "frequently asked questions":

> I have seen a great deal in the news lately about security and privacy issues with smart cards and I am concerned about the security of my personal information. How will this be addressed?
>
> There will be no personal information stored on the smart chip. The chip will simply be a number in the transit system that either has the U-PASS activated or not. The UW will send files to the transit agency "clearing house," which identifies which smart cards are active, valid U-PASS holders. These files will have the serial number of the active U-PASSes but will contain no names.
>
> Transportation Services will be the office that maintains the information on who has a valid U-PASS, and will keep this information private in accordance with the UW privacy policy, "UW Electronic Information Privacy Policy on Personally Identifiable Information."[182]

Public confidence surrounding privacy issues with Smart Cards would be enhanced if transit providers would, first, adopt a privacy policy on the subject (identifying the type of information collected, how it is to be stored, who will have access to it, and under what circumstances it will be released outside the agency), and second, post that policy on their Web sites. Transparency is a fundamental component of good government.

C. Suggestions for Access to Collected Information

Although governmental agencies are given wide latitude in collecting information from transit users and then using that information in their operations, there is a widespread belief that it would be prudent for transit providers to protect individual privacy in designing their ITS:

> In the first place, recognition of privacy as a value seems worthy of concern in designing ITS systems, because in the long run public acceptance and use of ITS services will depend on public confidence in the technology as not predatory or harmful. Respecting privacy fosters public confidence in ITS and will add to the consumer appeal of ITS services. Second, taking account of privacy is mandated under the federal organic act, which created the

[171] *Id*. Exhibit A (Public Access to Records Policy) § 6.1.6.

[172] *Id*. Exhibit A (Public Access to Records Policy) § 6.1.8

[173] *Id*. Exhibit A (Public Access to Records Policy) § 6.1.9.

[174] *Id*. Exhibit B (Privacy Policy) § 1.0.

[175] *Id*. Exhibit B (Privacy Policy) § 7.6.1.

[176] 5 U.S.C. § 555a(e)(7).

[177] WMATA, Resolution of the Board of Directors of the Washington Metropolitan Area Transit Authority (May 19, 2005). Exhibit B (Privacy Policy) § 7.6.6.

[178] *Id*. Exhibit B (Privacy Policy) § 7.6.9.

[179] *Id*. Exhibit B (Privacy Policy) § 6.2.

[180] *Id*. Exhibit B (Privacy Policy) § 9.4.

[181] Caywood, *supra* note 161.

[182] http://hfs.washington.edu/husky_card/default.aspx?id=953 (Last visited Nov. 9, 2007).

federal ITS program. Third, a variety of existing privacy laws will constrain how ITS can be operated.[183]

The threshold question is what personal information is really necessary to obtain and maintain. To answer that, one must ask for what the information will be useful. If the only thing the transit provider views as essential is simply monitoring financial payment, then an anonymous debit card will do nicely. If, however, the transit provider would like to enhance its marketing data, then a correlation of travel patterns with personal demographic information, including such things as age and income, frequency of travel, and proximity of home vis-à-vis work, may be quite useful. Additional information, including biometric identifiers correlated with TSA and law enforcement information, may enhance transit security.

In the 1970s the U.S. Congress developed "Fair Information Standards" to address the question of protecting privacy. These principles to date have not been codified; however, they have been used by Congress and federal and state agencies as the framework for privacy-related legislation and regulations. [184] These guidelines have been widely used in the assessment and implementation of the guidance for Homeland Security Presidential Directive 12[185] and TSA privacy regulations. [186]

The U.S. Department of Justice has incorporated the Fair Information Principles as follows:

1. *Collection limitation principle*. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. *Data quality principle*. Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

3. *Purpose specification principle*. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. *Use limitation principle*. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with Paragraph three except (a) with the consent of the data subject or (b) by the authority of law.

5. *Security safeguards principle*. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

6. *Openness principle*. There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. *Individual participation principle*. An individual should have the right to (a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) have communicated data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; (c) be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8. *Accountability principle*. A data controller should be accountable for complying with measures which give effect to the principles stated above. [187]

The State of California transportation agency (Caltrans) issues broad privacy guidelines that can be used by state agencies to design policies specific to each operation. The text below reflects general requirements for State departments.

Pursuant to Government Code Section 11019.9, all departments and agencies of the State of California shall enact and maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 (Civil Code Section 1798 et seq.), that includes, but not necessarily limited to, the following principles:

(a) Personally identifiable information may only be obtained through lawful means.

(b) The purposes for which personally identifiable data are collected shall be specified at or prior to the time of collection, and any subsequent use of the data shall be limited to and consistent with the fulfillment of those purposes previously specified.

(c) Personal data may not be disclosed, made available, or otherwise used for a purpose other than those specified, except with the consent of the subject of the data, or as required by law or regulation.

(d) Personal data collected shall be relevant to the purpose for which it is needed.

(e) The general means by which personal data is protected against loss, unauthorized access, use, modification, or disclosure shall be posted, unless the disclosure of those general means would compromise legitimate agency objectives or law enforcement purposes.

Each department shall implement this privacy policy by:

[183] Glancy, *supra* note 10, at 151, 170.

[184] *See* MARK MCNULTY, TREATMENT OF PRIVACY ISSUES IN THE PUBLIC TRANSPORTATION INDUSTRY (Transportation Research Board, Transit Cooperative Research Program, Legal Research Digest No. 14, app. A, 2000).

[185] http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html (Last visited Jan. 24. 2008).

[186] http://www.tsa.gov/assets/pdf/rt_standards_v3_0.pdf.

[187] See Justice Information Privacy Guideline, app. A (2002), available at http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf (Last visited Jan. 24, 2008).

- Designating which position within the department or agency is responsible for the implementation of and adherence to this privacy policy;
- Prominently posting the policy physically in its offices and on its Internet website, if any;
- Distributing the policy to each of its employees and contractors who have access to personal data;
- Complying with the Information Practices Act (Civil Code Section 1798 et seq.), the Public Records Act (Government Code Section 6250 et seq.), Government Code Section 11015.5, and all other laws pertaining to information privacy, and
- Using appropriate means to successfully implement and adhere to this privacy policy.[188]

The Smart Card Alliance recommends the following policy objectives:

- Smart card-related databases of personal information should be encrypted and should transmit only encrypted information.
- Transactions between smart card and reader should be offline only, and any information captured by a reader or other intermediate system should be deleted as soon as a transaction is complete.
- Organizations should set up checklists to show who is authorized to see or change information in each data field.
- Cardholders should be required to authorize, via password, personal identification number or biometric permission, the extraction of any data from their smart cards.
- Applications should be structured so that transaction records can't be used as surveillance tools. [189]

Further, the Smart Card Alliance recommends:

- The organization must have a privacy and security policy that clearly defines what personal information is to be collected, how the information will be used, who can access the information, how the information will be protected, and how the individual will control its use and provide updates to the information over time.
- The enrollment and identity proofing process must verify that the information presented is accurate and protect the confidentiality and integrity of that information.
- The system must protect each individual's information at all times, including while the information is being stored and while it is being used.
- The ID an individual carries must protect its contents from being copied, altered, or hacked, to prevent unauthorized use, misuse, or disclosure of the personal information it carries.
- The exchange of data between the ID and whatever device reads the ID must be protected to prevent unauthorized capture and use of data to impersonate an individual.
- Access to the personal information should be granted only after an issuer-defined authentication process. Only necessary information should be released and only to authorized systems or individuals.
- All personnel involved in using the system must be carefully trained and monitored to ensure strict conformance to the system's policies and practices. Compromising these policies and practices means compromising the identity management system itself. [190]

Each transit provider would be well advised to closely examine these fair information standards and policies if it has not already done so. Further, each transit provider can determine which principles and guidelines suit its particular objective, protect the transit users' privacy, and are legally defensible.

VI. CONCLUSION

Smart Cards have many potentially valuable uses. They may facilitate more expeditious, efficient, and economical fare collection, easing passenger access to and through the system. They may allow the collection of more useful data that can be employed to make better marketing and planning decisions, including types of fare stimulation packages or when and where new or different services should be offered. They also have the potential to add a layer of security to the transit system so as to ban dangerous patrons or terrorists from the system or apprehend them if they commit a criminal act, particularly if biometric identifiers and more powerful RFID card readers are incorporated into them. The more the information collected and correlated with other databases moves across the spectrum from mere fare collection to market data collection to security and surveillance, the greater the privacy concerns.

The fundamental challenge of transportation security is to be highly effective in protecting the public against terrorism, while not intruding unnecessarily upon personal privacy, convenience, and civil liberty, nor burdening unduly the efficiency of public transportation. The public would be well served if careful thought and analysis was given to where to draw the line between these conflicting policy objectives.

As we have seen, transit providers enjoy a wide Constitutional latitude in which to collect observable information in public areas such as transit stations and vehicles. They have a legitimate governmental interest in the collection of information concerning fares, and probably such additional data as the identity and address of the card holder. They probably also have wide discretion to acquire information necessary to serve the compelling governmental interest in protecting public safety and security, such as biometric identifiers, and correlate that data with law enforcement information, particularly in a post-9/11 world—a world in which London and Madrid subways have been bombed, and

[188] http://www.dot.ca.gov/privacy.html.

[189] http://www.gcn.com/online/vol1_no1/21158-1.html (Last visited Jan. 24, 2008).

[190] http://www.smartcardalliance.org/alliance_activities/identity.cfm (Last visited Jan. 24, 2008).

Tokyo subways have been gassed, by terrorists. In such an environment, there may be a compelling governmental interest in the protection of public safety that may allow a wide berth of information acquisition and user monitoring. Moreover, the courts have already given governmental institutions wide latitude in monitoring individual conduct in public places, as transit facilities clearly are. However, the acquisition of information not legitimately related to security (such as a patron's race, religion, political affiliation, or sexual preference), or the imposition of intrusive security measures or procedures (such as strip searching suspect patrons) would not likely survive Constitutional scrutiny.

Absent Constitutional restraint, the issue becomes one of what sorts of local legal, regulatory, or institutional restraints may be imposed. As we have seen, some state statutes and transit agency regulations do attempt to protect privacy. Sometimes, the statutes work at cross purposes, as when on the one hand a state attempts to enhance governmental transparency by promulgating a Freedom of Information Act, while on the other it attempts to protect individual privacy by limiting its dissemination. A transit provider also can further protect privacy through its internal regulations or procedures. Though the Constitutional latitude may be wide, local governmental institutions and transit providers may voluntarily seek to provide privacy protection beyond that mandated by federal law.

Transit agencies' regulations or procedures can protect privacy in various ways. They may limit the type of information that is gathered. They may circumscribe the universe of persons who may have access to it. They may protect information against external dissemination. Information collected can be encrypted, and firewalls built against external access. The information collected can be prohibited from distribution except by court order. Transit providers, however, must determine the extent of that privacy protection and how it will be legally implemented.

ACKNOWLEDGMENTS

This study was performed under the overall guidance of TCRP Project Committee J-5. The Committee is chaired by **Robin M. Reitzes**, San Francisco City Attorney's Office, San Francisco, California. Members are **Rolf G. Asphaug**, Denver Regional Transportation District, Denver, Colorado; **Darrell Brown**, Transit Management of Southeast Louisiana, Inc., RTA New Orleans, New Orleans, Louisiana; **Dorval Ronald Carter, Jr**., Chicago Transit Authority, Chicago, Illinois; **Dennis C. Gardner**, Ogletree, Deakins, Nash, Smoak & Stewart, Houston, Texas; **Clark Jordan-Holmes**, Joyner & Jordan-Holmes, P.A., Tampa, Florida; **Sheryl King Benford**, Greater Cleveland Regional Transit Authority, Cleveland, Ohio; and **Alan S. Max**, City of Phoenix Public Transit Department, Phoenix, Arizona. **Rita M. Maristch** provides liaison with the Federal Transit Administration, and **James P. LaRusch** serves as liaison with the American Public Transportation Association. **Gwen Chisholm Smith** represents the TCRP staff.

These digests are issued in order to increase awareness of research results emanating from projects in the Cooperative Research Programs (CRP). Persons wanting to pursue the project subject matter in greater depth should contact the CRP Staff, Transportation Research Board of the National Academies, 500 Fifth Street, NW, Washington, DC 20001.

Transportation Research Board
500 Fifth Street, NW
Washington, DC 20001