



February 14, 2006

Request for Proposals: TCRP J-5, Study Topic 9-01, Privacy Issues with the Use of Smart Cards

Dear Attorney:

The Technical Activities Division of the Transportation Research Board (TRB), as part of its work with the Transit Cooperative Research Program (TCRP), plans to award a contract for a study and report. The research Problem Statement is enclosed for your consideration.

TRB anticipates an estimated 400 hour level of effort, and compensation in the \$24,000.00 to \$36,000.00 range for this study topic.

Research reports sponsored by this project are published in TRB's Legal Research Digests (LRD) series. LRDs are distributed to some libraries and to approximately 4000 transportation lawyers and officials through the TRB distribution network.

After reviewing the enclosed statement, if you are interested in being considered as the researcher and author, you should reply by mail or before March 10, 2006 to:

James B. McDaniel
Counsel for Legal Research Projects
Transportation Research Board
500 5th Street, NW
4th Floor
Washington, DC 20001
Tel: (202) 334-3209
Fax: (202) 334-2003
Email: jmcdaniel@nas.edu

Your reply should include: a statement of interest; a resume; a list of your prior publications (you may enclose one or two publications); a statement of resources you will allocate to this project; any additions, deletions, or changes you may wish to suggest for undertaking the work; and your requested compensation.

Offerors are evaluated by Project Panel members and TCRP staff consisting of individuals collectively knowledgeable in the problem area. Evaluations are based upon the offerors': 1) experience in the subject area; 2) understanding of the work (demonstrated by the commitment of resources); 3) prior relevant publications (including briefs); 4) schedule for completing the work; and 5) price.

Feel free to call me at (202) 334-3209 if you have any questions.

Sincerely,

James B. McDaniel
Counsel for Legal Research Projects

Enclosure

JBM/jlc

TCRP J-5 STUDY TOPIC 9-01

PRIVACY ISSUES WITH THE USE OF SMART CARDS

Problem Statement

Smart cards are credit card-sized plastic cards with an embedded antenna and computer chip. They have become quite widespread among U.S. public transit agencies. The contactless Smart Card uses an electronic link between card and reader equipment that allows for a very fast interface that is needed by mass transit.¹ Using Smart Cards to replace traditional transit tickets or tokens reduces cash handling, equipment maintenance, and security costs; and holds 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.² Collection of ridership data leads to more targeted services by allowing transit agencies to keep track of ridership patterns and preferences. Representatives of the Dallas Area Rapid Transit (DART), while in the process of procuring a smart card system, heralded the data collection capabilities as one of the biggest advantages of smart card technology.³

In March 2000 TRB issued TCRP, LRD Number 14, *Treatment of Privacy Issues in the Public Transportation Industry*. This publication represents 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. The article noted the beneficial use of a Smart Card data collection system to transportation planners. However, such information may also reveal specific information about a transit customer; thus raising corresponding privacy questions.⁴ Subsequent to this publication, particularly after the terrorist events on September 11, 2001, public consciousness regarding privacy as it relates the use of Smart Cards has changed. The plea for a higher level of security has supported the rapid growth in technological enhancements of the Smart Card. Government agencies now use Smart Cards with identification tools to ensure the secure ingress and egress of employees and contractors to government facilities. The Department of Homeland Security and the Federal Transit Administration plan to further augment the use of their agencies' Smart (ID) Cards by allowing them to be used as public transit fare cards.⁵

State and local transit authorities also engage in Smart Card multi-application programs. The Chicago Card is interoperable across rails, buses and PACE, a regional commuter bus service. The Massachusetts Bay Transportation Authority (MBTA) "Charlie Card" system incorporates a reduced fare program for senior citizens, persons with disabilities, and blind persons. The Washington Metropolitan Area Transit Authority (WMATA) rechargeable SmarTrip® card doubles as a rail and bus fare card that can also be used to access Metro parking lots.⁶ WMATA now offers a SmarTrip® MasterCard® that allows a customer to store Metro value directly on the credit card.

¹ Smart Card Alliance RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities, http://www.smartcardalliance.org/alliance_activities/rfidvscontactless.cfm.

² Smart Cards and US Public Transportation APTA: Transit Resource Guide, Number 6 – Revised May 2005. http://www.apta.com/research/info/briefings/briefing_6.cfm.

³ See, Amy Carter, *Smart Card Technology Just Got Smarter*, Metro Exchange, 2001, http://www.metro-magazine.com/t_featpick.cfm?id=90503020.

⁴ Mark McNulty, *Treatment of Privacy Issues in the Public Transportation Industry*, TCRP, Legal Research Digest, N0. 14, p. 7, March 2000,

⁵ Responding to the White House directive: *Policy for a Common Identification Standard for Federal Employees and Contractors*, the federal government has launched over 64 Smart Cards programs in various agencies. The Transportation Security Administration has issued cards to approximately 15 million government and non-government transportation workers. DOD has issued in excess of 1.6 million smart-card ID's to military and civilian employees. Privacy advocates worry that security badges may be a first step toward national identity cards that contain masses of personal information. The data-storage capability of the cards continues to grow as the industry expands, and governments and companies have found wide uses for the cards including fare card and other transportation privileges. See, Sara Kehaulani Goo, *Smart Cards' In Demand As Concerns About Security Rise; Privacy Issues Loom*, The Washington Post, Wednesday, February 26, 2003.

⁶ See Washington Metropolitan Area Transit Authority (WMATA) <http://www.wmata.com/riding/smartrip>.

Regional authorities also use this technology to ease traffic congestion at toll facilities. The Maryland Transportation Authority is considering the elimination of all toll booths on the Bay Bridge to ease summertime traffic jams via the use of its EZPass and Express Toll Lane systems.⁷

The technological innovation that makes the Smart Card data collection possible is the radio frequency identification (RFID) system. The purpose of the RFID system is to identify and track people, animals, and goods. RFID systems have two main components: a transponder and a reader. Transponders are the data-carrying device in an RFID system and are affixed to the object to be identified, for instance a contactless smart card key. The reader is a radio transceiver that communicates with the transponder via radio waves.⁸ At some later point the information on the reader is uploaded to a central computer. In many cases this is an agency computer. On others such as with TransLink® in the San Francisco Bay Area it is a regional computer. In many cases a private company under contract with the local or regional agency operates the computer. That computer may contain the name, address, driver's license number, automobile tag number, or financial data (such as credit card or checking account numbers) from the cardholder.⁹

Generally, most transit agencies only ask for and compile personal information that is needed to provide the customer with the service that is sought. For fare media that provide a high level of functionality, a greater amount of information is required and broader scope of its use is probable. Smart Cards can be purchased over the counter or online. In either circumstance, transit agencies are required by law to post or publish information concerning privacy and confidentiality.¹⁰

⁷ <http://www.baybridgeinfo.com/overview.html>. With an E-ZPass account, drivers get an electronic tag with account information that attaches to the windshield of their cars. When drivers go through a toll that offers E-ZPass, an antenna reads the vehicle and account, and the toll is paid electronically. The technology used to read tags in cars is just one part of E-ZPass. Toll plazas are equipped with cameras to snap pictures of the license plates of drivers who fail to pay. Character recognition software reads the tags and connects with other systems to mail out violation notices and fines. This month the Maryland Department of Public Works launched its new Express Toll Lane. This program allows automobiles carrying min-transponders to maintain speed while proceeding through toll plazas. The theory is much the same as the new HOV+ lanes in the State of Virginia and the technology is similar to that of the E-ZPass. Maryland's Intellectual Property and Economic Budget Privacy Policies are incorporated into its public transportation information gathering policies. Other states with similar technology include the San Diego Fastrak and the Lee County, Florida, Queue Jump.

⁸ Jerry Bitro, *Relax Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature*, UCLA J. L. & Tech. 5 (2004).

⁹ Brian W. Smith, Ramsey J. Wilson, *The Electronic Future Of Cash: Article: How Best To Guide The Evolution Of Electronic Currency Law*, 46 Am. U.L. Rev. 1105, 1997; Richard T. Preiss, *The Consequences of Anonymous Access to the Financial Payment System*, 16 Dick. J. Int'l L. 619, 1998; Sarah N. Welling, Andy G. Rickman, *Cyberlaundering: The Risks, The Responses*, 50 Fla. L. Rev. 295, 1998; Heather C. Alston, *ELECTRONIC BANKING: Will That Be Cash, Credit, or E-money?*, 1 N.C. Banking Inst. 225, 1997.

¹⁰ San Francisco Bay Area TransLink License Agreement Provision (License agreement is included in the "Welcome Package" and registrant certifies the reading of it when signing registration form.)

12. CONFIDENTIALITY OF INFORMATION

- 12.1 All information and data relating to the Cardholder collected by the TransLink® FPS shall be used by MTC and the Service Providers for the purposes of the operation and management of the FPS and shall serve as a source of information and data for transit and/or related services in general but shall otherwise be dealt with in a confidential manner by MTC unless:
- (a) the express written consent of the Cardholder has been obtained; and/or
 - (b) there is legal requirement to the contrary.
- 12.2 You retain the right to review all personal information pertaining to your account, whether stored electronically or on paper. Any inquiry or request to obtain information, in accordance with the above provisions, should be directed in writing to the TransLink® Customer Service Center. MTC may adopt procedures for your review of such information, including but not limited to charging a fee for processing requests for access to personal information.

This project should examine 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 long should the information be stored.¹¹ In what way, if any, is the use of the data monitored and protected. Other issues emerge with the commercial application of the technology in for example, the Exxon Mobile SpeedPass system, which is similar to the technology used by the EZpass system or the SmarTrip® MasterCard®. Do the protections afforded credit cards and check cards remain available? Also, would use of travel information to market customers be appropriate in transit?

It would be useful to include additional research such as a compilation of current state laws, and what information regarding privacy protection is made available to potential or actual cardholders with current or proposed Smart Card systems. Of further use would be a compilation transit agencies' policies regarding registration and protection against invasion of privacy and identity theft and a legal memorandum detailing strengths and weaknesses. Include privacy and security issues and thru-ticketing implications under federal railroad laws. Also, it would be useful to discuss to what extent smart card information would or should be available to the following: requestors under FOIA or state public records laws; federal or local governmental agencies for police or security investigations; taxing authorities; litigants through discovery requests or subpoenas.

The law is clear that there exists no reasonable expectation of privacy associated with the use of public transportation services. However, the success of public transportation is directly affected by the use that the public makes of it. Query whether the public is aware of privacy limitations associated with the use of transit and whose responsibility is it to make them aware. How does such information impact public trust? How, if at all, are civil rights threatened? Surveys could be conducted on what different jurisdictions are doing to educate the public both in a general fashion and in association with registration for Smart Cards and other such electronic intellectual devices. The study should also examine how privacy concerns of the public transit customer have changed historically, especially in light of an increased security awareness of the nation.

Primary data is needed on the extent to which transportation agencies are participating in Smart Card identification management systems.

Task 1. Research Implementation. Research Plan and Detailed Report Outline.

Consultant will conduct background research and develop a complete research plan. The final step of this task will consist of a work plan, a proposed questionnaire to state agencies, and a detailed outline for the report (8-10 pages). This material will be submitted to TRB for approval.

Estimated Length of Time: 60 days

Estimated Work Effort: 60 hours

Task 2. Collect primary data by sending the questionnaire to state agencies. Collect and analyze the data.

Estimated Length of Time: 90 days

Estimated Work Effort: 60 hours

¹¹ Focus groups of potential riders have shown that transit riders are also concerned about privacy when using the card (Dinning and Collura 1996). The most critical issue in this case is how agencies will use and who will have access to the transaction database. Precedents in other industries suggest that it will be fine for transit agencies to "mine" the database for their own use, particularly for determining what incentive offers to give users. Norren Mc Donald, Multipurpose Smart Cards in Transportation: Benefits and Barriers to Use, University of California Transportation Center, Research Paper, No. 630, Spring 2003, <http://www.uctc.net/papers/630.pdf>, citing Dinning, Michael and John Collura, "Electronic Payment Systems in Public Transit," in *6th ITSA Annual Meeting Proceedings*, Houston 1996.

Task 3. Draft report in accordance with the approved outline (including modifications required by TRB).

Estimated Length of Time: 90 days
Estimated Work Effort: 200 hours

Task 4. Revise report as necessary. Offeror should estimate that 2 revisions will be necessary. One revision may be required after review by the Principal Investigator and members of a subcommittee. In addition, revisions may be required after the full committee has reviewed the report.

Estimated Length of Time: 60 days
Estimated Work Effort: 80 hours

Total Effort Estimated Length of Time: 300 days*
400 hours

Estimated Compensation: \$24,000 - \$36,000.00
If an offeror's estimation on Length of Time and Estimated Work Effort differs from those above, the Offeror should use his/her estimates.

* The successful offeror can expect committee review time to consume as additional 90-150 days.

Submit Statements of Interest on or before March 10, 2006 by mail to:

James B. McDaniel
Counsel for Legal Research Projects
Transportation Research Board
500 Fifth Street, NW, Room 426
Washington, DC 20001
202/334-3209
FAX: 202-334-2003
Email: jmcdaniel@nas.edu