Privacy, SmartCards and the MBTA

A Policy Analysis of the MBTA's New Automated Fare Collection System

Ian Brelinsky
Brian Myhre
Jennifer Novosad
Chris Suarez

6.805 – December 10, 2004
Massachusetts Institute of Technology

Table of Contents

Acknowledgements

We would like to wholeheartedly thank the following people for their contributions to our project. It would not have been possible without you:

Professor Hal Abelson

Keith Winstein

Danny Weitzner

Senator Jarett Barrios

Dalie Jimenez

Dan Michaud

Steven Berrang

Josh Martiesian

Leslie Caplan

Thomas Komola,

Pat Saccoia

Mary Simonowicz

Marvin Sledge

Anita Chan

Executive Summary

The MBTA aims to provide a safe, available, and inexpensive service to its customers while respecting its customers' basic rights to privacy. Currently, the MBTA is pursuing a plan of automated fare collection that will entail the use of RFID smartcards. Other metropolitan areas have implemented or are in the process of implementing this technology into their public transit systems. To date, however, no public authority has developed or integrated a privacy policy directed towards RFID. A privacy policy developed by the MBTA can serve as a model for these other systems. In this paper we will outline guiding principles for a privacy policy, including openness, choice, and security. These principles are critical to maintaining personal and institutional security while maintaining the trust of citizens; failing to address them could unnecessarily subject riders to breaches of their personal privacy. These include risks of being stalked, profiled, or victimized by targeted advertising or theft. We specify what characteristics any fare-collection infrastructure would need to meet these policy principles; these include provisions for the collection, access, and storage of data, in addition to informing users of these data practices and providing a choice to ride the T at the same cost without providing personal information. We also provide a possible technical implementation for fare data collection in accordance with the principles. Our recommendations will address any privacy issues MBTA customers may have while enabling the MBTA to fulfill its goals of increased efficiency, reduced costs, and improved customer service.

Our original work in several areas served to support our claims. By studying other RFID implementations and interviewing several transit officials we were able to gain perspective on the choices that are made by outside authorities. By reviewing and analyzing the recommendations of privacy organizations such as EPIC and CASPIAN, we were able to gain an understanding of the privacy principles necessary for preserving the public trust. And by meeting with local, state legislative, and MBTA officials, we could relate to the local issues faced by the MBTA and the Massachusetts resident. These broad perspectives gave us a balance of opinions necessary to make well thought-out, realistic recommendations to the MBTA.

Section 1 – History of the MBTA

Massachusetts and the city of Boston have a long and venerable tradition of excellence in providing public transportation. These many systems reflect a historic commitment to customer service and constant advocacy for progress in their best interest. Boston is considered the birthplace of mass transportation in America, and this pioneering and progressive spirit lives on today with the current Massachusetts Bay Transit Authority (MBTA).[1]

Source: http://www.mbta.com/insidethet/taag_history.asp

Long before America declared independence from the British, Bostonians were experimenting with early versions of mass transportation. The Legislature of Massachusetts offered a charter in 1630 for a ferry service from Boston to Charlestown, since Boston was a narrow peninsula. Thomas Williams accepted their offer in 1631 and introduced a water ferry across the Boston Harbor, including stops in Chelsea, Charlestown, and Boston. This service was family owned and operated for most of its history, establishing a continuing precedent for personal attention to the customer and a strong connection to the surrounding community.[2]

Section 1.1 – Early Public Stagecoach Service

Following the American Revolution, bridges were constructed to connect the Boston peninsula to the mainland, including Cambridge, but the flourishing commonwealth still required more land transportation services to meet the personal and commercial demands of its citizens. Regular stagecoach service arrived between Boston and Cambridge in 1793, and the system quickly expanded to reach the other numerous outlying areas, traveling over the many new bridges.

With an ever increasing interest to meet the needs and demands of customers, variations of this traditional form of stagecoach service soon appeared on the Boston landscape. The most notable was the daily omnibus service, with the "omni" meaning "all." Similar to the current network of MBTA buses, the omnibuses had several assigned stops along a published route. Seats were

[1] "T History: The Chronicle of the Boston Transit System." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history.asp>.
[2] "T History: The Ferry." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history2.asp>.

lengthwise inside the horse-drawn vehicles, and doors at both ends allowed for much more rapid and efficient loading and unloading of passengers. They represented a monumental step forward in acknowledging the necessity for public transportation to increase the scope of its availability and accessibility to the citizens of Boston. If the stagecoaches are analogous to today's taxis, the omnibus foreshadows the incredible public promise embodied by the MBTA.[3]

Section 1.2 – Passenger Comfort and Reliability

Having begun to address the challenge of accommodating large numbers of passengers, the mass transportation of Boston then set out to address passenger comfort and the reliability of service. Especially as a result of cold Boston winter, the streets were perpetually marred by ruts and mud, and streets covered by ice and snow presented an even more immediate hazard to horse-drawn vehicles. Boston turned to an idea New York had experimented with since 1832 of running the horsecars on two parallel metal rails permanently fixed in the streets. This created a much smoother ride for the passengers, and allowed for operation through adverse weather conditions. The rails also enabled the much faster transportation more weight as a result of the reduced surface friction on the wheels.

The first horsecar on rails began running March 26, 1856 between Central Square and Bowdin Street. The created an atmosphere of healthy competition with the rail and omnibus services that brought about even greater levels of customer satisfaction and attention. However, this time period also illustrated the need for public administration of mass transportation, as many routes were largely overlapping yet fares varied widely. Laying a foundation for the public-interest minded MBTA, the General Court of Massachusetts passed the West End Consolidation Act, which formed a single transportation system on the rails lining many Boston streets called the West End Street Railway. It was remarkable accomplishment as one of the largest such networks in the America at that time.

The next problem tackled by mass transportation pioneers following these significant improvements to comfort and reliability was public health. The West End Company maintained a fleet of 8,000 horses for pulling the street railway cars, which were prone to disease and frequently injured from overloaded cars. The combination of sick animals and incredible amounts of waste were particularly a problem in the already crowded city streets of Boston. This motivated the search for alternative means of locomotion for the transit vehicles.[4]

---

[3] "T History: The Omnibus." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history3.asp>.

[4] "T History: Horsecard on Rails and the West End Street Railway Company." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history4.asp>.

Cable cars had gained popularity and acceptance in other US cities during the late 1800s, and Boston also entertained plans for two cable car lines stretching across the city. However, the West End Company, which was scheduled to assume management, had apprehensions about their success in the rough Boston weather. In no rush to pursue the cable car plan, the transportation decision-makers decided to visit Richmond, VA and preview another mass transportation design installed by the Union Passenger Railway Company. These cars ran on rails but were powered by electricity supplied from an overhead copper wire.[5]

Source: http://www.mbta.com/insidethet/taag_history7.asp

The West End Railways executives were amazed at the speeds achieved by the electrified cars, but they still questioned the ability of primitive American power systems to handle the load. Late one night, Union Passenger ran the entire fleet of 21 cars simultaneously on the overhead copper wires. The Bostonians were thoroughly convinced and took an incredible step of faith in bringing electrified rail cars to the entire metropolitan area. And once again the citizens of Boston ruled the day. Developers saw the potential of connecting underdeveloped areas by rail car, and soon Massachusetts had more track per square mile than any other US state. Boston mass transit was continuing its long tradition of delivering more service to more people with greater reliability.[6]

Section 1.3 – The First Subway in America

Boston winters present a challenge to all aspects of life, and as mentioned before, establishing reliable mass transportation is no exception. However, in 1897 an infrastructure addition was unveiled that redefined the ability of city dwellers to travel largely unhindered by Mother Nature and other vehicle traffic. This was the year Boston opened the first subway system in America, and it paved the way for similar systems in urban centers across the country.[7]

The next half century was especially hard for the mass transportation systems as war, depression, and other economic challenges jeopardized the very existence of

[5] "T History: The Cable Car." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history5.asp>.
[6] "T History: Electrification." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history6.asp>.
[7] "T History: The Rapid Transit Commission and the BERY." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history7.asp>.

many railcar and subway routes. On August 3, 1964, the state of Massachusetts acknowledged the imminent situation and responded by forming the current Massachusetts Bay Transit Authority (MBTA) as a taxpayer supported public service. The new organization initiated an aggressive and rapid strategy of expansion, extending transportation links far into the suburban communities around Boston, including bus service, commuter rail, and subway. The MBTA also contributed by consolidating numerous small, struggling railways into its expanding system, including the Eastern Massachusetts Street Railway on March 30, 1968 and the Middlesex and Boston Street Railway complex on July 1, 1972. These proactive responses ensured the availability and affordability of affordable mass transit to Bostonians for generations to come.[8]

Source: http://www.mbta.com/insidethet/taag_history11.asp

Today the MBTA is the 4th largest transit system in America, and the letter 'T' has special meaning for all who have come to know and love this city. Yet despite its rich heritage and continual progress, the MBTA finds itself now standing at a critical crossroads. The current token-based fare collection system is 30 years old, and most of the associated station infrastructure has become burdensomely costly to maintain. At the same time, law enforcement authorities are eager to develop frighteningly intrusive and evasive methods of passenger tracking and control. Fares only cover a small fraction of operating costs, yet customers are growing increasingly dissatisfied with the quality of service.[9]

The challenges are real and demand immediate attention. This paper will highlight the MBTA's incredible opportunity to step confidently into the future while preserving the public trust, enhancing customer satisfaction, and protecting the privacy of every citizen. Other urban transportation networks have had similar experiences in upgrading their fare collection technology, but their responses have largely failed to address these critical issues of customer service, which have long set the MBTA apart as a leader in public transportation. Through this transition process, the MBTA can set an example to be emulated by the rest of the world and reestablish itself as first in mass transportation.

---

[8] "T History: Public Control and the MTA." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history9.asp>.

[9] "T History: New MBTA." 2003. MBTA. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history11.asp>.

Section 2 – History of RFID

A substantial component of the current MBTA system upgrades is the introduction of RFID technology as part of an Automated Fare Collection system to replace the existing antiquated machines. RFID technology allows contact-less reading of information stored on a small chip inside a plastic card. The technology, however, is far from a new idea. In October 1948, Henry Stockman wrote what was perhaps the first scholarly paper on RFID, titled "Communication by Means of Reflected Power." It appeared in the Proceedings of the Institute of Radio Engineers (IRE), a forerunner to the highly respected Institute of Electrical and Electronics Engineers (IEEE). Unfortunately for Stockman, the technology required to practically build the necessary components, including the transistor and microprocessor, would not be widely available for several decades. Even so, less sophisticated implementations of the central ideas behind what we understand as RFID technology were well under development in the 1950s. A radio transponder system to identify aircraft as friendly or foe was among these ambitious projects. [10]

Research in the field of RFID gained steam in the 1960s, when a significant number of scholarly papers established and documented founding principles of the field. Titles from this time period included "Field measurements using active sensors," "Theory of loaded scatters," "Remotely activated radio frequency powered devices," and "Interrogator-responder identification system."[10]

Section 2.1 – The Commercialization of RFID

The major commercial interest at this point was theft prevention of expensive merchandise. Two corporations still in existence today that formed in response to this market demand were Sensormatic and Checkpoint. Both companies have diversified greatly since their inception but maintain expertise and a strong standing in the field of RFID enabled asset tracking and supply chain management. The equipment was called electronic article surveillance (EAS) and simply detected the presence or absence of a tag in a defined vicinity. [10]

The 1970s witnessed a dramatic increase in attention to RFID technology, with major development projects at Los Alamos Scientific Laboratory and Northwestern University. Large corporate systems integrators entered the scene as well, including Raytheon with its "Raytag" and similar efforts by RCA, Fairchild Semiconductor, General Electric, Westinghouse, Philips, and Glenayre.

---

[10] "Shrouds of Time: The history of RFID." 1 Oct. 2001. The Association for Automatic Identification and Data Capture Technologies. 11 Nov. 2004. <http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf>.

Europe was particularly keen on the idea of tracking animals and industrial products, while America saw more potential in human and corporate resource management. Transportation monitoring was introduced in the Port of New York and New Jersey on large ships, and personnel access control followed in line with this application. The Association of American Railroads and Container Handling Cooperate Program were leading advocates for these developments.[10]

The first RFID implementation to experience true commercial viability and success was automated toll collection. Dallas North Turnpike introduced RFID payment in 1989, sparking a decade of remarkable progress and proliferation. Oklahoma opened a toll highway in 1991 that could read from the car's RFID unit as it traveled through the toll plaza at full speed. Other states in that region implemented compatible systems, so a single RFID device could interact with multiple reader networks or a single billing agency was responsible for collecting payment on behalf of multiple jurisdictions. This latter model was embraced by seven northeastern toll collectors who joined together as the E-Z Pass Interagency Group.[10]

Section 2.2 – Mult-Purpose RFID Cards

The RFID card scheduled for release with the MBTA's new Automated Fare Collection implementation is named the "CharlieCard." An idea very attractive to the MBTA as they progress with CharlieCard implementation is leasing space on the card. The customers could include other government entities that require identification and record keeping on patrons, such as the public library, or commercial entities where consumers spend money on a regular basis, such as Starbucks or Dunkin Donuts. This is a potentially lucrative source of supplementary revenue for the cash-strapped MBTA, and it is embraced as a great convenience by many customers. In reality, multi-use cards are far from a new idea. The North Dallas Tollway again led the way in this innovation with its novel TollTag®, a standard vehicle mounted RFID device that could also pay parking lot fees and gain access to gated communities.[10] A concern with this arrangement is that personal information is shared among groups subject to different regulations, which significantly increases increased risk of data misuse.

Today RFID appears more prevalent in our everyday lives than ever before. The Federal Communications Commission (FCC) has aggressively provided more bandwidth for RFID applications in the 5.9 GHz range, representing a huge opportunity for proponents and those with a commercial interest. Transportation systems and business around the country have had extensive experience and grown comfortable with many forms of RFID technology, and now is the critical time to draw lessons learned and chart the course forward.[10]

Section 3 – Benefits to the MBTA

The MBTA has identified a number of tangible customer benefits associated with this overall system upgrade, and particularly with the introduction of RFID technology. Customer service is prominent among these claims. Most T stations currently vend tokens primarily from a small, metal booth, staffed by a single MBTA employee who collects money, distributes tokens, and returns change to customers. Some stations also feature mechanical vending machines, but these are frequently inoperable and have limited ability to offer change on the transactions. The result of this situation is very lengthy lines to purchase tokens, which slow down busy travelers and create problematic congestion in station entrances. This congestion not only impedes customer movement, but large crowds create a serious law enforcement liability and danger to public safety. This is particularly a problem when large events take place downtown Boston.[14]

Section 3.1 – Personnel Cost Savings

Since such a large number of personnel are required to staff fare vending booths, the MBTA is unable to provide employees in the stations devoted to customer service. With the elimination of human-vended tokens, these Fare Booth Personnel at each station would become Customer Service Agents. The agents would provide assistance with using the RFID card technology, quickly identify malfunctioning technology and immediately notify the maintenance department, provide directions to tourists and other visitors, and give subway riders a greater peace of mind regarding their safety when riding the system. It is certainly possible for the current Fare Booth Personnel to fulfill many of these functions, but they are less approachable when seated behind bullet proof glass, and the fixed booth position greatly limits their view of activity in the station.[12]

A RFID card-based fare collection system allows the MBTA to easily implement customer-friendly payment methods and lower the customer transaction cost. A credit card may be linked to the MBTA card, allowing for automatic refill of the balance when it drops below a certain predefined level. Another option is automatic deduction for monthly or other long-term purchase options. This is particularly attractive to those who use the T for transportation to work or school on a regular basis. The ability to associate personal information with a particular card also enables loss-protection and recovery of remaining card balance if a card is lost or stolen, since the customer can now prove his identity and be associated with a particular card. This possibility is a source of great concern for privacy advocates who worry about the potential to track and monitor individual customers, which will be explored later in great detail.

The opportunity to introduce online fare purchases and online account monitoring are further benefits of the RFID card-based system. A user can add card value from the comfort of his home or office, before even arriving at the transit station. Further, it might be possible to give a customer limited access over the Internet to recent account activity, so he can guard and monitor against malicious or unwanted use and errors in the MBTA collection technology.

Section 3.2 – Maintenance Advantages

The MBTA also identifies a number of maintenance advantages associated with installation of this new system. The current token turnstiles and magnetic reader machines are old technology, and the represent assets that are increasingly more costly to service and maintain. Replacement parts are hard to come by, and finding entire "new" units is an even greater problem.

New fare collection technology will also enable more rapid identification of hardware failures. Since every card reader is linked to a central database and control center, remote monitoring stations can work with the Customer Service Agents to efficiently dispatch repair team, order replacement parts, and redirect customer traffic when needed. The current system has limited connectivity between the individual system units, and debugging almost always includes sending maintenance personnel to the site instead of more efficient remote monitoring

Section 3.3 – Financial Benefits

With rising costs and a relatively static fare structure, paramount among the benefits of this system to the MBTA is potential cost savings. At present, farebox collected money only covers around 22% of operating expenses, and the long-term financial concerns are very real.[9] The T is almost entirely dependent on outside cash flows to maintain its operation, with 20% of state sales taxes and an assessment on each jurisdiction it services going directly to MBTA operations. The Authority derives the remainder of its funding from local and federal grants.[11] As a result, working to finance the T is an endlessly frustrating task, and the possibility of automated fare collection to increase revenue beyond its cost is alone very convincing.

Although many of the Fare Collection Personnel will be transformed into Customer Service Agents, the MBTA will likely be able to reduce its overall number of employees as a result of the new system, and employees currently represent a huge portion of its operating expenditures. The MBTA will at the

[11] Davis, Jonathan. "Balancing Debt & Pay-As-You-Go Financing." 10 Oct. 2002. MBTA. 10 Dec. 2004. <http://gulliver.trb.org/conferences/Fin3/Track2_Davis_10-28-02.pdf>.

same time need to hire skilled personnel to service and administer the automated system, this is a relatively small number, and they will simply be replacing the teams of people currently devoted to working on the current machines.

Token handling, management, and distribution represent another substantial and potentially reducible cost to the MBTA. Fleets of armored trucks with multiple agents on board are employed to ferry tokens from subway stations to sorting stations and back again. Mechanical counting and sorting technologies are required in all these facilities, and a huge number of people are involved in the money and token handling process, as a result of proliferation of passenger entry and exit points, including those on the buses and commuter rail vehicles. Since so many transactions involve cash and token exchange, this is a massive and costly responsibility. Additional law enforcement challenges surrounding these same four concerns are highlighted later in this section. Greatly increased payment by credit card, more robust automated vending machines, automatic card refill capabilities, online payment alternatives, and the elimination of tokens will all contribute to substantial savings in this area.[12]

Fare evasion is a major source of lost revenue to the MBTA. A business case study performed by the MIT Auto-ID sets the amount at 1.5% of total revenue, based on numbers provided by the MBTA.[13] MIT Detective Thomas Komola, who served previously as MBTA Chief of Police, estimated based upon his personal experience overseeing station law enforcement and security that a true representation of the cost associated with fare evasion is even higher.[14] Komola pointed out that the turnstiles are very easy to circumvent, the accuracy of bus-based fare collection boxes in counting coin payment and identifying invalid monthly passes is very questionable, and especially on the buses, payment is entirely dependent on the ability of a single, unarmed driver to enforce the fare regulations. Furthermore, unlike most other jurisdictions around the country, fare evasion is not an offense subject to arrest in Boston. The MBTA's only recourse in dealing with those who abuse the system in this way is asking them to leave. An automated system would eliminate the interaction with a human operator, who can be more easily intimidated and manipulated than a machine. A report prepared for the Seattle Monorail on fare collection alternatives for their green line found typical evasion rates between 2% and 6% for inspector verified payment systems around the country, including the bus and commuter rail operations within the MBTA. In contrast, the number was 1-2% for what they call

[12] Berrang, Steven and Josh Martiesian. Interview with Brian Myhre and Chris Suarez, 15 Nov. 2004. Written Notes. Massachusetts Bay Transit Authority.
[13] Bean, Brandon, Robert Dudley, and Hideaki Tomikawa. "Business Case Study: Auto-ID Fare Collection at the MBTA." 1 Feb. 2003. MIT Auto-ID Center. 10 Dec. 2004. <http://www.autoidcenter.cn/solution/download/Auto-ID%20Fare%20Collection%20at%20the%20MBTA.pdf>.
[14] Komola, Thomas. Interview with Brian Myhre, 25 Oct. 2004. Written Notes. MIT Police Department.

"self-verification" systems such as turnstiles and RFID.[15] The advanced card technology would allow for more sophisticated verification of valid payment, and the new turnstiles can be designed to make jumping or otherwise bypassing them much more challenging.

An automated fare collection system with RFID technology can also process large volume much more easily and efficiently than is currently possible. Eliminating the inherent complications associated with people directly vending the tokens is the first potential source of huge consumer benefits. Employees expect a consistent number of working hours each week, which scheduled and unscheduled leave thrown in with relative regularity for good measure. They need breaks throughout the work day, and environmental factors greatly hinder or enhance their ability to serve customers effectively. Furthermore, most T stations are unable to afford more than one fare vending employee because of high personnel costs. In contrast, machines have substantially lower life-cycle costs than an actual employee. According to an acclaimed study of the current MBTA spending patterns "Labor costs, driven by high pay scales, growing headcounts, antiquated work rules and the state's anti-privatization statute are the T's most serious challenges. To date most of the Authority's significant efforts to bring costs under control have been stymied by political resistance."[16] With the automated fare collection system contributing to substantial savings in this area, even small stations should be able to afford multiple card vending machines. The machines have no preference in their working hours, refuse to take coffee breaks, and are designed for optimal speed of operation.

In addition to daily demand fluctuations, there are particular instances during the year with the rider traffic far outpaces the MBTA's ability to vend individual fare. Examples include the downtown Fourth of July festivities and large concert events in the city. In these instances, huge numbers of people simultaneously enter a T station and overwhelm the distribution system. In some instances, the MBTA will simply unlock all the turnstiles and allow everyone to pass through without paying the fare, to avoid a potentially very dangerous situation with hundreds of tired and perhaps impaired customers clogging the entire entrance to buy tokens.[13] The CharlieCard first allows people to easily load money in advance, so they can be carrying fare and avoid fare vending lines without the need to keep track of cumbersome, heavy, and easily misplaced tokens. Secondly, the increased vending machine capacity will accommodate more customers simultaneously, and the ability to pay with a credit card at the machines should immediately speed up the fare payment process. Customers will appreciate the

[15] "Green Line Fare Collection Alternatives." May 2003. Multisystems, Inc. 10 Dec. 2004. <http://www.elevated.org/_downloads/Meetings/05-05-03_Fare_Collection_Alternatives.pdf>.
[16] Tepke, Glen. "MBTA Capital Spending: Derailed by Expansion." Feb. 2002. Pioneer Institute for Public Policy Research. 10 Dec. 2004. <http://www.pioneerinstitute.org/pdf/mbta.pdf>.

convenience and find themselves more inclined to place additional value on the card.

Section 3.4 – Law Enforcement Considerations

The law enforcement communities connected to the MBTA and the metro-Boston region also see incredible value and potential in the CharlieCard and Automated Fare Collection. It will be easier to build safe and secure stations, given the introduction of entirely new turnstiles, methods of fare vending, and attitudes on paying for transit services. The fare vending booth, a central fixture in every current T station, would no longer be a huge customer bottleneck.[13] Since the system will come with new turnstiles, the MBTA has an opportunity to completely resign the restraint mechanism. The new turnstiles may feature 5' tall swinging glass doors, as are already found in the New York City subway.[11]

One particularly important and dangerous function of the MBTA police force is protecting, securing, and monitoring the huge amount of cash that passes through the system every day. The fare booth operator often has tall stacks of money on his desk, and although he is seated behind a layer of bullet proof glass, the lure is no less real for the criminal mind. Even rolls of tokens have huge cash value, both inside and outside the legitimate distribution channels. Whenever the fare booth operator takes a personal break from his post, steps outside to help a customer, or responds to an emergency situation, his safety is in great peril because the open door exposes the money inside the booth. It is not possible for an armed law enforcement officer to be present at every station, and even when a police presence does exist, the proximity of innocent bystanders and the constraints of a small maneuvering area hinder his ability to fully respond in a timely manner with appropriate and effective force, should this situation escalate. Furthermore, the money must be transported between stations, and this operation is conducted by a fleet of armored trucks, as was mentioned earlier. The driver and his assistant hand carry the money from the station to the truck, as well as empty out money from the vending machines and other revenue sources inside the T station. The money is then trucked off for counting and deposit, under the close supervision of MBTA police and armored transport personnel. However, this is a huge drain on law enforcement resources and maintains significant stress on everyone involved in the process.

The current challenge comes from the sheer quantity of cash moved around the system every day. The Automated Fare Collection system enables people to pay with a credit card, which would drastically reduce the human handling of money at the many disparate stations throughout the MBTA system. In addition, the ability to automatically reload a CharlieCard and purchase from on the Internet also reduce the likelihood of a passenger paying with cash. The result is fewer large money transfers on a schedule less predictable and observable by those

who would disrupt the system. It is a great financial risk to have so many individual parties handling money with little to no direct supervision.

Similar to the current situation with large amounts of cash in the system, the antiquated tokens also present a huge financial and security liability, since they have a real cash value within the T. The tokens must be trucked around in armored vehicles, counted, sorted, rolled for redistribution, replaced when they wear out, and handled by many different and loosely connected parties, just like the cash. Despite the nostalgia and classic feel of token payment, the T should be excited to offload this cumbersome and grossly inefficient system.

Another benefit to the MBTA of Automated Fare Collection is the safety and well-being of its employees who interact directly with customers on a constant basis, particularly the safety and well-being of the bus drivers. There is no physical barrier between the bus drivers and passengers the way it exists with the fare booth personnel and subway drivers. The driver is somehow responsible for ensuring that every passenger pays the correct fare, MBTA rules are properly enforced, and emergency situations are quickly addressed, all while safely and skillfully maneuvering the huge city bus. Correctly marking and handing out transfer slips when requested is also expected of the bus driver, effectively establishing him as not only a driver, enforcement officer, and emergency first responder, but a fare agent as well. An automated fare collection system would wisely move the driver further away from direct interaction with the passenger while he is paying, which is a time the driver should not need to be closely involved.

The train conductors have their own set of unique challenges as a result of the current payment arrangement. A passenger boards the train without paying, because the conductor does not have time to collect fare upon entry. While the train is in en route, the customer pays with cash or shows a pass. This requires the conductor to make change and carry large amounts of money on his person. It is also relatively easy for a person to pay less than the correct fair or evade the fair entirely, since it is not collected until later in the trip. One idea for the new automated system is handheld RFID reads for the conductors to carry, which would facilitate much more efficient and secure fair collection.

The law enforcement community also finds the ability to identify patterns of irregular activity very attractive to its mission. A sudden shift in ridership, either a significant increase or a significant decrease, can be a valuable signal for law enforcement to proceed with particular vigilance and attention to detail. Decreased traffic at a certain station might suggest a pervasive source of harassment, station equipment particularly prone to failure, or inconsiderate MBTA employees. Increased traffic might signal a need for more police

patrolling, heighten awareness of insidious plans among a group of people, and provide information that enables a generally more optimal distribution of law enforcement resources in the future.

Data collected by people riding the T could also provide critically important evidence for criminal proceeding in which it is properly and legitimately subpoenaed. Any data use along these lines would most certainly demand strict and closely monitored privacy policy implementation. However, law enforcement entities believe they could appropriately manage their use for purely legitimate and beneficial purposes.[14] Our concerns on law enforcement use of the data are addressed throughout the remainder of this paper.

Returning to financial concerns, another important advantage of the CharlieCard is the potential for much greater flexibility in farebox revenue generation. The automated system easily facilitates charging different rates for peak and off-peak travel. The T could increase revenue with higher rates during the always busy rush hour period. Another alternative is assessing different fares based upon distance traveled. Washington DC has a system along these lines, and since the card can record the entry location, that could be a determinant in the fare charged to the customer. Confirming and correctly charging reduced fare customers, including children and seniors, is also much easer with the CharlieCard, since the driver is not longer required to discern legitimate reduced fare cards and monitor proper payment.

Automated Fare Collection is a great service to handicapped customers. No longer will they need an assistant to help them make payment and deposit fare, but a simple wave of the plastic card in the direction of the reader will do the trick. These represent a handful of reasons from among the variety offered by the MBTA for switching to Automated Fare Collection with the CharlieCard.

Section 4 - Technical Basics

RFID is an automatic identification system which uses tags that communicate wirelessly with readers to transfer identifying information that is then used to help a server make a decision. There are three parts to an RFID system: tags, readers and middleware. Tags are devices that are affiliated with an external, movable object. Middleware is composed of servers and infrastructure that acts as the brain and nervous system of the RFID system. Readers are the system's mouth and ears – they ask tags questions which allow the server to know what tag has been presented. In all, the three devices compose a powerful system which can manage enormous amounts of data with very little human interaction.

Tags come in many flavors. There are "active" tags and "passive" tags. Active tags are like over-caffeinated gifted children – they yell to readers whenever they want, despite a reader's presence. They are capable of doing many things at the same time, such as performing advanced calculations, taking measurements of temperatures, etc. Passive tags, on the other hand, are sluggish and talk back often. They do not speak to readers unless asked a direct question and rarely do anything other than repeat themselves over and over until they are pulled away from the reader. Passive tags lack the power to do advanced calculations and typically, they are a buck a dozen (whereas active tags cost more).

How far a tag can "yell" is determined by how much energy it has. Active tags can be "heard" much farther away than passive tags and some passive tags can be "heard" a bit father away than others. The distance a tag can be read from depends on how much other noise is present and how loud and in what direction the tag "yells." Given a large enough and sensitive enough "ear" a tag can be heard much farther away than the specs dictate.

Active tags are safer than passive tags. Active tags can answer intelligently to questions posed to them and (sometimes) know better than to talk to strangers. Passive tags learn one saying and will say it to everyone who passes by and says "hello!" Active tags are surely more trustworthy with secrets, but they cost more, which is a definite tradeoff.

Active tags are better at word games, since they can do more computations faster. Generally speaking, obfuscating a word or sentence so only the intended listener knows the meaning is called Encryption. Tags with more power and bigger "brains" (i.e. more transistors [which cost more]) can play word games better and thus are more secure.

There is far more to an RFID system than over-caffeinated children and yelling. For a more technical discussion (but hopefully still understandable), please check out appendix A, Technical Information.

Section 5 – Cautionary Anecdotes

5.1 – A story says 1,000 images.

There is a lot of talk about privacy, especially in this paper, and there are two ways of viewing the issue. If you consider yourself pragmatic, you most likely declare that you have nothing to hide and anyone who wants to take the effort to watch you or look at where you go is more than welcome. If you claim to be a privacy advocate, you might think that it's nobody's business where you go or what you do and there should be laws banning them from doing that.

Both sides have merit and there are tradeoffs in choosing to enforce one or the other. Generally, implementing more secure systems requires more testing and thought. Even with a well-thought plan, an implementation might not satisfy the needs of everyone. For example, law enforcement would like ubiquitous access to movements of civilians and far more tracking and logging of transit. Society has a need for dangerous and intimidating behavior to stop; however, the importance of creating a safe environment must be weighed against people's need for freedom, and privacy. We do not believe that there is one solution to the problems we mention concerning the MBTA's new automated fare collection system. We hope through some cautionary anecdotes, we can share our vision and worries with you in an illustrative manner. Perhaps, by reading about poor Charlie, the ol' sap we place in precarious situations, we can give emotional reason to our suggestions and make them seem like the natural decision.

Without further ado, here's Charlie…

5.2 – Trust Your Data to People Who Manage Data [Not Trains]

Charlie, an old time Boston resident, recently acquired a new RFID card so he could ride the T. Charlie was an average guy; he lived single in a modest apartment, worked a modest job, traveled to see his family on holidays, and had a fairly average life. Charlie was a good person; he was honest and expected others to be as well. He never thought twice about the privacy concerns of his new CharlieCard because he figured that if anyone wanted to know what he was

up to, he would tell them – he reasoned that since he had no secrets, if this could make his life easier, let him start living better!

Charlie enjoyed his new card. He never had to worry about buying tokens again. His checking account was linked to the Charlie Account so whenever he was low on fare, the MBTA would automatically transfer $50 onto the card and he was set to go. He loved the ease of use of the card and especially liked not to having to touch the grubby tokens ever again. Life was good for Charlie – for a few months that is.

Charlie was sitting at work when it happened. He was sitting at his computer just as the hacker sat at hers. He typed e-mail after e-mail as she tried a recursive brute force attack on the MBTA's servers. Just as he got up to go get money from the ATM for lunch, she finally cracked into the MBTA's servers and was now logged in as "administrator." She could do anything now.

Charlie was content with his financial state, he had several thousand in the bank and was saving for retirement – he was planning to transfer ten thousand to his stock portfolio, but didn't have time. Eve, the hacker, was counting on this. She was now logged into the main database – it was beautiful. There, before her eyes, lay unencrypted databases with over a million people's checking account numbers, credit card numbers, addresses, "secret key words," and other personal information. She set the file to download as she, too, grabbed lunch. Then, she edited the main access log and wiped her traces. To the naïve system administrator, she was never there.

Charlie walked back to his cubicle, oblivious to what had just happened with the information he thought was safe with the T. He trusted the T with his checking account number, as they promised to only use it to top-off his account. He didn't care if they knew his address and phone number, he even gave his social security number so he could "verify" his identity, a precaution they insisted upon to ensure that his checking account really belonged to him. All was good.

Eve, looking for some cash to buy that new Red Mustang she always wanted, found a buyer for her newly acquired information. Mwambano Mustavuff from Nigeria was the ex-secretary of the treasury and was looking for some American checking account numbers. He bought the information for $5 a name, $7 if they had socials listed. In all, Eve sold only a small fraction of the names to Mwambano, but made over $200,000 from the transaction. She got that new Mustang and had enough cash to live off of for a few years. She was quite happy -- she had left no paper trail, and she could not be traced back to the transaction from the MBTA servers or from the use of the numbers.

Two months later, Charlie's credit card was denied. He tried another card and it too was denied. He didn't understand why, as he had plenty of credit, but called the company to inquire. Turns out "he" had refinanced his house and bought plenty of good stuff on credit in the past month. "His" debauchery was now catching up with him – his checking account was empty and his credit cards sky high in debt. His trusting attitude and the MBTA's poor attempt at maintaining security for their customer's data had led to a disastrous situation he would never forget (or recover fully from).

What's the moral? The MBTA should not have kept all that data in one place. They shouldn't have put all their faith into a weak system. Redundancy in protection would have stopped Eve. Eve also wouldn't have gotten Charlie's information had he not given it so trustingly to the MBTA. He won't forget this lesson for as long as he lives.

5.3 – Insider Abuse Has Major Risks

Charlie lay on the pavement gagging on his own blood. He had heard a loud explosion and before he could think what happened, he was cold and staring at the sky. The man stood over him, a grimace on his face, shouting something about Charlie deserving what he got. Everything got dark as Charlie took his last breath – the man's shouting was Charlie's last experience.

Just one week earlier, Ryan Marcus, the man who shot Charlie, had learned that his 17 year old daughter had been assaulted by a man named Charlie M. Cardier. Charlie M. was not a nice person -- he had just been released from prison and wanted to assuage his sexual desires. Miss Marcus was walking alone in an alley; Charlie M saw that she was alone and took advantage of her. In the act of assulting her, he dropped his credit card and Miss Marcus picked it up before going to the hospital.

Mr. Marcus was understandably angry about his daughter. He fell into a fit of rage and promised to get back at Charlie M.

Working as low level system administrator at the MBTA, Mr. Marcus knew he had access to the travel logs and knew just the way to find Charlie M. He searched the records for "Charlie Cardier" and low and behold, one entry came up. He did a bit of research and found where Mr. Cardier typically traveled. He had paid for his Charlie account using a CeltCo account (CeltCo was a company in Boston) and entered the T at exactly 10:35 every morning at Porter and got off at 10:58 at Park Street. Mr. Marcus traveled to Porter to wait for his prey. He spotted a man who was wearing a CeltCo polo shirt and followed him onto the

train. The man removed his CharlieCard to exit the T and Mr. Marcus noticed that his driver's license said Charlie Cardier on it. Mr. Marcus was in luck – he had located the man, he though, who had raped his daughter.

He followed Charlie off the T and into the Common. He waited for Charlie to get to the middle of a clearing and took out his gun. Charlie didn't see it coming.

Sadly for Charlie, his name was Charlie T Cardier, not Charlie M Cardier. He hadn't assaulted anyone, nor would ever. Our star had been slain because he shared a name with a criminal.

Sadly, there have been real cases like this one. In New Hampshire, a woman is suing an ISP for invading her daughter's privacy and enabling a stalker to murder her.[17] The court in this case decided that information brokers who store personal data have a responsibility to the person indexed. If the MBTA does not implement safeguards to prevent internal abuse of personal information, they are liable and our citizens are at risk.

5.4 – Holey Matrimony

Charlie is an ordinary guy and like any ordinary guy he had some issues. For Charlie, it was his sex life – his highly successful wife, Beth, wasn't around nearly enough and his love life was running on empty. He tried to take things into his own power, and make due without her, but only loneliness sprung from his attempts. Veronica, the tall, slender blonde from HR was always giving him good vibes and he was desperate.

Every day after work, Charlie hopped on the Blue Line and rode to Wonderland hoping to forget his frustrations. Beth worked late and the kids had soccer practice, so nobody noticed that he wasn't home. Charlie and Veronica had fun together, but it was only for one purpose: recreation.

Beth, noticed that Charlie seemed more relaxed and didn't want sex nearly as often as before. She was happy that Charlie was managing his desires, but didn't give him that much credit – she suspected something. On Charlie's birthday, Beth decided to come home early to surprise her husband. Four o'clock rolled around, five o'clock came, six approached and at six thirty, Charlie ambled into the house pretending that he had just come back from the gym.

[17] http://www.courts.state.nh.us/supreme/opinions/2003/remsb017.htm

Frustrated and distraught, Beth filed for Divorce a week later. Her lawyers subpoenaed Charlie's T logs and found that Charlie had been a naughty boy. He had traveled from work to Wonderland and then from Wonderland back home every day. From these logs, the court found that there was enough evidence that he was having an affair. His wife got custody of the kids and also got a nice alimony check. Charlie was up the creek.

While it was nice for Beth that the travel logs were available, Charlie did not commit a crime. Moreover, the MBTA collected logs on his movements before he was suspected of guilt. Collecting travel logs on people not suspected of crime, and using these logs in court, in a sense, makes Charlie guilty until proven innocent.

He was naïve for many reasons, but as far as our story goes, Charlie should have known better than to trust his movements to a huge database at the MBTA. If he had known the precedent of the EZ Pass system, he might have thought twice. The New York Throughway System received 128 subpoenas from 1998 to 2003 – they delivered information on about half of those. Subpoena's ranged from divorce cases (very similar to Charlie's) to murder cases (US Attorney Luna). Also, EZ Pass logs were used to discipline 30 narcotics detectives for claiming false charges in NY – they were logged driving through tolls where they were not claiming to be working.[18]

Databases have changed how Americans live their lives. Our credit record is a big database, as are our transactions from credit cards and banks. Our travel is logged, as in an EZ Pass system and potentially on the T. Our recreation is surely logged, as Blockbuster Video most likely tracks which customers watch what films, etc. If all these databases were linked in an intelligent form, the administrator of this uber-base would know almost everything. It would be easy to see what someone's interests were by seeing what they do for fun. It wouldn't be tough to see what they eat regularly by looking at grocery purchases, it wouldn't be tough to search for purchases at a Jewelers to predict whether the person was engaged and a public records search would determine if he or she was married. All in all, information is encroaching on the once sacred private sphere of our private lives. As a society, we need to determine what safeguards, if any, we wish to place on this information. We need to determine who we want to see it, how long it lasts, what can be done with it, and if it even exists. If you're not willing to tell a total stranger your social security number, date of birth, amount of hemorrhoid cream purchased in a year, sexual orientation, and yearly salary – you might wish to change your perspective on database access controls and the lifetime and breadth of data collected about you.

[18] AP, Dec 11 2003

5.5 – Tracking Customers is Bad Business

Imagine Charlie is a 25 year veteran of the Boston area FBI. Charlie is getting ready to retire. Since he has been on the job for so long, he is good at what he does and can accomplish a lot in a day. He recently got into the habit of getting his hair cut and paying his bills and such over lunch – essentially adding half an hour to his lunch period. He figured that since he was a pro at his work, he could finish everything he needed and have time to run errands, take a longer lunch and leave a few minutes early. He was paid for a 40 hour work week but ultimately did a 40 hour job in 35.

Charlie knew that he was technically supposed to work five more hours every week, but figured that since he accomplished what he was expected to do he needn't worry about being a stickler for the rules. Perhaps that's why Charlie was so surprised when his boss informed him that he'd been fired for time fraud.

Charlie demanded to know what evidence they had against him and learned that his travel logs on the T had been obtained. The times on this time-card were inconsistent with the times that had been predicted based on logged T usage data. While he claimed to leave at 5:00, he was logged entering the Government Center T stop at 4:15. Obviously, he couldn't be in two places at once. The T's records were trusted over his story.

This is what happened: HR had acquired access to the MBTA's ridership logs, which contain a rider's personal information (i.e. identifying info) and a list of relevant account information (date and time of entry into a station, etc). They wrote a script which compared their employee list and time database to the MBTA database. The script checked for matches in name and compared the time employees left work to the time they entered the T. If there were inconsistencies, they would investigate. Unfortunately for Charlie, he was working 35 hours of a 40 hour week and got caught red handed.

As a society, we recognize and value people's differences. Charlie happened to be especially good at his job and could finish his work early and effectively. He is now paying the price for a database society. If we want a society where people maintain a criminal mindset – constantly wondering if what they are about to do is wrong of if they can get away with it – we can easily implement systems which will accomplish that goal. If, on the other hand, we value our freedom and realize that people are only human, we need to impose restrictions on technologies which could infringe on the very essence of what a free society means to us.

Section 6 - Case Studies of RFID Smartcards in Transit

The final goal of this paper is to make policy recommendations to the MBTA based on its proposed RFID smartcard implementation. In making these recommendations, we must examine what other transit authorities using RFID smartcards have already done to combat privacy concerns. In our research, we found that no major transit authority with a full-scale RFID smartcard implementation (London, Chicago, Washington DC) has provided sufficient safeguards for consumer privacy. This section examines each of these three authorities, identifying the key areas where the authority either does an effective or ineffective job in addressing privacy concerns. Through a case study of Metro Transit in Minneapolis, this section also discusses other issues – reduced fare smartcards and incentive programs – that can potentially provide customers with an incentive to opt-in when they may not have otherwise wanted. The issues that are discussed vary by case so as to minimize redundancy of the section. We hope that the MBTA will be able to use the provided information and suggestions to reflect on its own privacy practices, and that, in addition, other transit authorities that currently have or are considering having RFID smartcard implementations will reflect on them in creating or modifying their practices as well. We provide a summary of the practices of these other implementations along with the variables this section considers in Figure 6.4 at the end of this section.

Section 6.1 - A Foreign Case – Transport for London (Oyster Card)

Transport for London (TFL, UK) has a major implementation of automated fare collection with an associated smartcard called the "Oyster Card." Although TFL has taken some important measures to address privacy and data use concerns for this card, we found that its policies often neglect consumer privacy. Despite this, the Oyster Card was given a publicly nominated award for its "world class ticketing system."[19]Like the CharlieCard, the Oyster Card affords users the opportunity to go through turnstiles quickly and easily, is rechargeable, and is available to both adults and students. It records the time, date, and location of riders at entry (and sometimes exit) of stations. Finally, there are two options for riders: Oyster and Oyster pre-pay.

[19] "Oyster card wins public nominated award"
http://www.oystercard.com/files/press/Oyster_wins_award_July_04_FINAL.doc

Section 6.1.1 – Opt-out Availability for the Oyster Card

Having two distinct options (regular and pre-pay) effectively adds an opt-out provision[20] to London's RFID implementation. This is because the pre-pay card has an option to be unregistered, whereby the card is not linked to a credit card or name. Instead of paying a fare that is automatically reloaded by the credit card, riders using pre-pay cards can recharge their cards with cash within London transit stations. They also can be recharged on-line or over the phone using a credit card. Having distinct choices for both those who do and do not want to reveal their identity while traveling is a significant step. Nevertheless, this opt-out choice is not available for all individuals interested in using some form of the Oyster Card.

Reduced Fares and Student Registration

It is frustrating that any student who wishes to use an Oyster Card that provides student discounts must register. Under the current system, students who have a valid "Student Photocard" may get reduced rates without having an Oyster Card, but they must wait in lines and purchase their tickets on a per-ride basis. The Oyster Card alternative allows students to receive these special fares via a 7 day or monthly pass, both of which require registration. Given the relative ease of using an RFID smartcard, students will be inclined to want the Oyster Card regardless of their privacy concerns. The convenience of the Oyster Card does not necessitate registration for passengers in general; it is thus foolish to apply this double-standard to students. If a student is relies on the discount when going to class each day, he well may register regardless of the privacy implications or individual concerns. The time saved by not having to wait in line may be the difference between arriving late or on time to a final exam.

One argument that can be made in support of forced registration for students is that it makes TFL certain that an actual student or senior is receiving the card; however, this argument neglects that someone can just as feasibly sign up for a *pre-paid card* that subtracts discounted rates. Indeed, there can be a screening protocol that students go through before they receive this card, and this may require the collecting of some personal information. However, screening information can be gathered and put into a database of students that *have received* cards; this would be totally unrelated to any master databases that may track rider movement or associate credit card numbers with riders. This way, cases of student attempts to receive multiple discounted cards can be prevented, but

[20] When referring to an opt-out provision, we specifically reference the ability to opt-out of an RFID smartcard option that associates a customer's name with data collected from using a smartcard.

students will be able to opt-out of releasing additional information about both themselves and their future travel patterns. If a student refuses to register, a field that identifies the *unique card* given to a student can be left blank.

Limiting Unregistered Card Use Geographically

Another opt-out restriction problem is created outside of London, where TFL users are unable to use the untracked Pre Pay card option on approximately 16 separate bus routes. Thus, an individual who travels on these bus routes is only able to purchase the standard Oyster card if he expects to use an RFID smartcard during his trip to and from work each day. Less-frequent users of these routes are also affected. An individual from London, for example, may have relatives who live near these bus routes. Otherwise not very intent on obtaining a registered card, these individuals may get one anyway to avoid the inconvenience of switching from RFID to a standard ticket when making their trips on these bus routes. Therefore, if a transit infrastructure provides an option to use a registered card in a given area, it should always provide an option to use an unregistered card in that area as well. This will minimize the potential for cases like this to occur, where people will be forced to make a difficult choice between maintaining their privacy and convenience.

Section 6.1.2 – Oyster Card Privacy Communications

The level of detail of the Oyster Card website is impressive.[21] The site allows plenty of opportunities for card registration, card recharges, and customer service inquiries. It even has its own internal search engine. Referring to figure 6.1, we see references to all of these opportunities on the main page of the Oyster site. After initially examining the site, therefore, we were fairly certain that something in the privacy realm would be mentioned on the site. But upon typing the word "privacy" into its search engine, *zero* results were returned. In a comprehensive eleven page "Guide to Oyster," moreover, no information about rider privacy or data collection is mentioned. Someone could easily go to the Oyster site, register, and have no notion of their privacy or data collection rights. Making a policy that is easy to locate and widely available is undoubtedly in the public interest.

[21] The Oyster Card website is located at www.oystercard.com

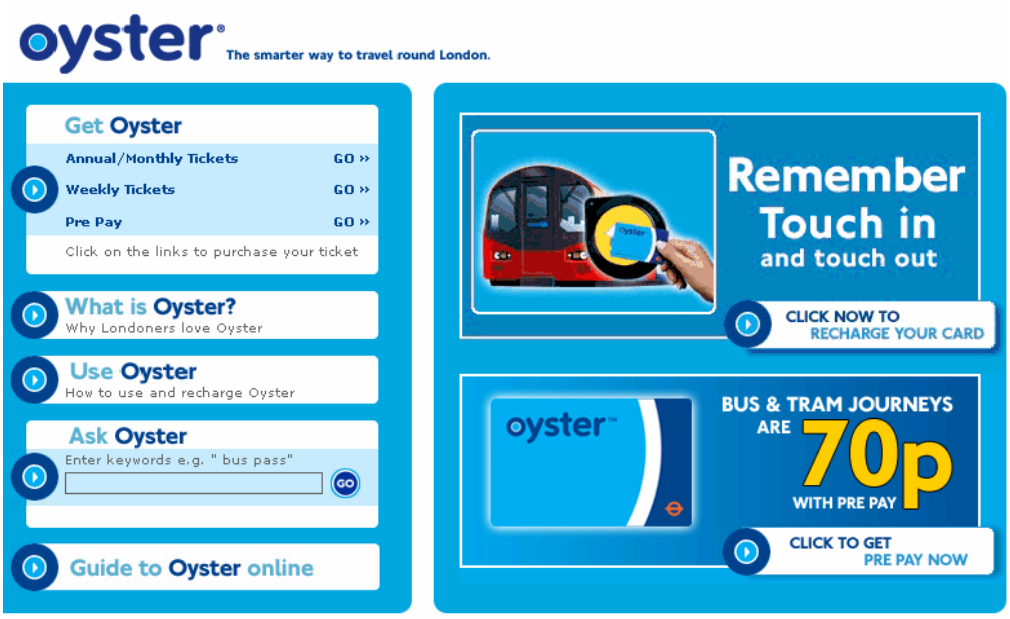


Figure 6.1. Screenshot of Oystercard Website

An Alternative to a Privacy Policy – London's Ticketing Data Protection Policy

Admittedly, TFL is unique in that it offers a "Ticketing Data Protection Policy.[22]" This is a very significant adaptation for a transit system, and its existence alone should be commended. Questions answered in the document include what personal information is collected by TFL, what personal data is used for, what is disclosed to third parties, and which third parties information can be disclosed to. Unfortunately, however, the data protection statement makes no direct reference to the Oyster Card. In fact, the only thing resembling a reference to the card in the entire document is where it states "we may collect information when you use our services." But when will they collect that information? What TFL services does this apply to? Reading the TDDP statement does not fully inform the TFL rider.

Besides failing to answer these questions, the TDPP presents a problem to the concerned customer by announcing a fairly liberal data disclosure policy. First, information can be disclosed to law enforcement and regulatory authorities. This could cause an individual to be implicated in a crime based primarily on circumstantial evidence. The fact that Charlie entered Station X at 1 PM with his Oyster Card does not necessarily imply that he was a criminal in many

[22] Transport for London Ticketing data Protection Statement - http://www.londontransport.co.uk/tfl/nftt_dataprotection.shtml

circumstances. What if someone's card is stolen (or found) and a crime is committed? How would we know if the person who registered the card is lying or telling the truth? Circumstantial evidence provided at the level of an RFID smartcard that is so easily lost or stolen can be unreliable. Although we realize that transit authorities can be bound to release their information from a legal standpoint, the amount of information released to law enforcement would decrease dramatically if transit authorities stored the data for very short periods of time.

Oyster Card information could also be disclosed when it is "in the public interest." This is a very vague and general statement that leaves plenty of room for TFL to determine innovative ways to justify disclosing data. As we will show in our discussions of recommended policies, we are not in support of these sorts of unclear statements in privacy or data use policies.

It would seem dangerous to consumers to allow TFL to make such broad statements in its data collection policy or in any other policy. By instead defining and clarifying the public interest for consumers in its statement, TFL can fairly justify its data collection. And, at the point the justification is defined, the consumer will at least be able to make the decision of whether to opt-in or opt-out upon being fully informed. Under the current system, someone who may disagree with one form of data collection that is "in the public interest" may have opted-in with the assumption that data would not be collected for that case in which data is *actually collected*. We do not want riders of the T to experience the same confusion. At a basic level, we think that it would clearly be in the public interest for the public to know the specific instances when data is disclosed (or at, minimum, be given a definition that allows people to understand applicable instances of what the public interest *could be*).

The TDPP also does not state how long TFL will store information that is attached to a particular person's name. Instead, it says that information will be retained "as long as necessary" to fulfill TFL's purposes. As with disclosing information that is in the public interest, retaining information as long as necessary presents an ambiguity to the consumer that should be made clearer. How long is it held for exactly? Why does holding the information for this amount of time necessary to "fulfill the goals?" Unless this justification is made in the policy, TFL is not doing enough. We also need to ask if the goals of TFL are necessarily legitimate to begin with. Should the TFL, for example, be a law enforcement agency? These are all tough questions that will need to be addressed in the MBTA's privacy policy. Due to the issues listed above, it is clear that the TDPP only represents a reference point for that policy.

Section 6.2 - Fully Implemented Domestic Cases – The CTA and WMATA

In the United States, the Chicago Transit Authority (CTA) and Washington Metropolitan Area Transit Authority (WMATA) have instituted their own RFID Smartcard transit implementations. Both have fallen far short of the ideal privacy goals we propose. Nevertheless, like London, both have unique practices that protect privacy concerns.

Section 6.2.1 - Chicago Transit Authority (Chicago Card and Chicago Card Plus)

Chicago's RFID smartcard implementation is in the form of two cards called the "Chicago Card" and "Chicago Card Plus." The Chicago Card (CC) is the more basic option; customers can add value (up to $100) to a CC by depositing cash into vending machines within stations. Value can be checked at vending machines, and registration is optional. Conversely, the Chicago Card Plus (CCP) requires the use of a credit card to add value, requires registration, and does not allow the user to check the card's value at vending machines within stations. Instead, customers need to check the amount of value on their CCP online. Finally, whereas the CC only allows for a pay-per-use option, the CCP gives users the option to apply 30 day passes to the card as well.

Clearly Indicating the Differences between Cards with and without Registration

The differences between the two cards as explained on the CTA website are highlighted in figure 6.2.[23] This figure serves as a good model of what a transit authority could produce that makes a viable comparison between its multiple smartcard options. The figure is color coded to distinguish between the cards, and the key differences are clearly stated for the customer. Notably, the announcement is neutral; it does not express any preference for the card that requires registration. This is something that can be posted in a station for customers to look at as they consider making switches from anonymous magnetic stripe cards (these are also an option in the Chicago system) to RFID smartcards that may or may not be anonymous. We think it is important that transit authorities ensure that their customers understand all available RFID

[23] http://chicago-card.com/ - The chart is referenced off of a section on the main page called "Which Card is Right For You?" The link references a COM file, and a direct link is thus unavailable.

smartcard options, and diagrams like this posted in stations or on websites serve this purpose well.

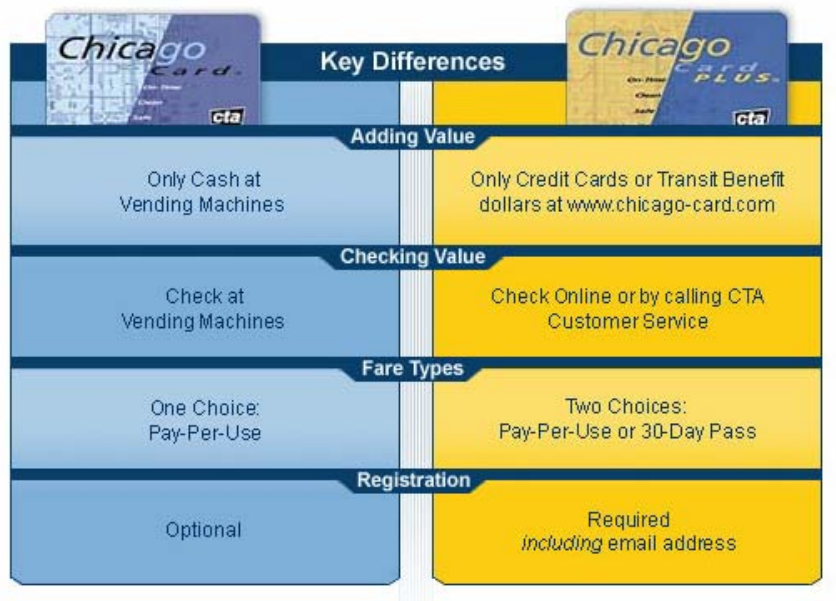


Figure 6.2. Comparison of Chicago Card and Chicago Card Plus

It is unfortunate that users are not told data can be collected and used after the point of sale when we consider that the CTA does indeed collect data on the times and places the card is used by individuals.[24] As with other RFID smartcards, those that are registered can easily be traced back to a particular person using this data. The CTA, as we were told in our interview with them, does not release this specific information to third parties or outside sources. Riders should know that this pertains to both the CC and CCP. They should also know that the data on a particular customer's riding patterns can be subpoenaed by appropriate legal authorities. Further, they should know that their rider data is stored on one CTA database for 90 days, while it can be held on another for as long as a full year. All of these could be mentioned in a privacy policy and/or TDDP.

In illustrating the differences between smartcard options, moreover, we also believe that transit authorities should clarify the implications of having a registered versus an unregistered card. In this regard, Figure 2 could be improved. A customer may not necessarily understand that, in addition to automatic fare recovery, "Registration" also implies that there will be data collection that is associated with the customer's name while he travels. Thus, we advise transit authorities to do the following when indicating the differences between their smartcard options:

[24] CTA Interview with Marvin Sledge, Customer Service Manager 12/6/2004

1. Place an asterisk next to "registration" on a diagram like Figure 6.2, and indicate that by registering, the transit authority will be able to collect travel data and associate with it with the individual who registers.
2. Provide a reference to the appropriate privacy and/or data collection policies (a URL, customer service agent, or brochure that can be looked at)

By doing this, we feel that customers will be given ample opportunity to understand the potential for privacy limitation and decide which card they want based on that. That is, they will be able to opt-out. In all likelihood, many people will not be swayed by taking these additional steps. Nevertheless, at the point some people do alter their thought calculi based on these measures, we feel that it is the obligation of the transit authority to take them.

Maintaining Fare (Fair) Incentives[25]

Chicago's fares are independent of distance traveled. Thus the time, date, and location of an access is only recorded at entry. An incentive is provided to use the RFID smartcards, as users receive a $1 bonus for every $10 that is added to the card. Both the Chicago Card and the Chicago Card Plus provide riders with the bonus. This bonus creates a disincentive to use magnetic stripe cards as a mode of transportation. Nevertheless, given the cost-effective nature and efficiency of an RFID smartcard implementation, it makes sense to provide incentives to use smartcards. Because the bonuses the CTA gives are uniform for both the Chicago Card and Chicago Card Plus, we believe that the bonuses are beneficial. Thus, we encourage transit authorities to have these incentive programs. However, in creating the programs, transit authorities must provide the bonus equally in both registered and unregistered versions of the card.

The CTA's Need for Clearly Defined Privacy Measures

We believe that the opt-out choice and privacy provisions of the CTA aren't codified well or specified for RFID smartcards. This problem was shown to exist in our discussion of the CTA's chart indicating the differences between its card options. While the differences between the cards were presented well, the privacy-related issues were essentially left on the backburner. The CTA's privacy policy has similar problems. In essence, it is a general statement about website privacy. It specifically states that information may be collected and that cookies

[25] "Chicago Card FAQs Page." <http://chicago-card.com/ccplus/faq.aspx>.

may be used as an individual browses the CTA's web site; that information collected when one purchases a *Chicago Card* will not be divulged to third party businesses; and that personal information of children under that age of 13 will not be collected by the authority.

It may be good that the CTA takes these privacy steps in its policy, but the unfortunate reality about the CTA's privacy policy is that it does not mention the relevant privacy concerns that arise when a rider uses a smartcard. The introduction of the CTA's privacy policy states:

> This statement provides the CTA's privacy policy on information that is collected through this web site, and the Chicago Card™ and Chicago Card Plus™ programs and the use of that information.[26]

After having said this, one would expect a sustained effort throughout the document to draw distinctions between the relevant privacy issues that arise from the smartcard as compared to those from the website. Instead, however, the only major references to Chicago Cards within the policy concern the information that is collected at points of transaction. Yes, we learn that credit card information, names, and addresses obtained at the point of sale will only be used for billing purposes and to fill orders. But there is no indication that, with a registered Chicago Card, data can be collected subsequent to the initial transaction and attached to a customer's name. The CTA, moreover, has no policy like London's TDDP that explains why and how data is used that is specifically collected from usage of the smartcard. Thus, besides adding provisions about the privacy of users who use the smartcards, the CTA may also want to consider creating a policy like the TDPP in the near future.

Releasing Information to Individuals – Security Protections for Registered Cards

A final issue for the CTA is how it deals with the release of information to customers. Based on the Freedom of Information Act, all customers using registered cards have a right to see their own travel histories. They also have the right to examine the personal information held on file by a transit authority to ensure that it is up to date and accurate. We feel as strongly as anyone else that all customers should have the right to view and correct personal information and rider histories stored by a transit authority. But, in giving this right, transit authorities must ensure that that information is only released to the actual

[26] Chicago Card Privacy Statement - https://www.chicago-card.com/cc/privacy.aspx

person who registered the card. Otherwise, the rights of the cardholder would clearly be infringed upon.

To this end, we support that the CTA associates PIN numbers with each registered CCP. These 5-digit PIN numbers are chosen by users at the point of registration. An individual should not have the ability to call a customer service representative, tell the representative a card number, and receive personal information of the cardholder or the cardholder's travel history. Having a PIN number in addition to a standard card number adds an extra layer of security that helps avoid cases of unreasonable data disclosure.

Section 6.2.2 - Washington Metropolitan Area Transit Authority (SmarTrip)

The Washington Metropolitan Area Transit Authority (WMATA, Washington D.C.) has another implementation of an RFID smartcard. The WMATA implementation uses a smartcard called the "SmarTrip," and users can store as much as $300 on the card at any given time. Users have to touch the card to fare-boxes upon entry and exit of stations (and only upon entry of buses) because the WMATA MetroRail system charges fares based on the distance traveled. There is only one type of SmarTrip card, and it can either be registered or unregistered. The system does not provide any incentives in the form of bonuses or discounted fares. Based on this, we feel that the WMATA provides its customers with a flexible system that is neutral between registered and non-registered users.

Best Information Practices: Logging Employee Interactions with Data

In our interview with the WMATA, we were able to gain some insight on other relevant issues. First, we learned that the ride history of individuals is collected by the WMATA upon both entry and exit of each station. Like London and the CTA, the time, date, and location of a card touch is stored. Data is stored in databases for a minimum of one year, and the data turnover usually occurs every two years. The access to the databases is limited to those who work in the WMATA's customer service department, along with some upper-level management, technical representatives, and treasury department members. Significantly, the WMATA's system logs each time someone accesses data within their systems. This allows managers to do periodic checks to ensure that their employees are not abusing the system. Ideally, these systems could be designed so that unusually high rates of access by employees can be flagged. Managers informed of these flags can then address internal abuse issues quickly and easily.

At the WMATA, the customer service representatives are also limited in that they are only allowed to view a cardholders name, address and daytime telephone number. The personal information is in a separate database from rider histories, and the customer service representatives are therefore very limited in their ability to abuse it.[27] We also support this idea of isolating personal data from travel data because it makes associating one's identity with a travel history much more difficult.

The WMATA's Need for Defined Privacy Measures

If we examine the privacy policy of the WMATA, we once again see little mention or specifics regarding smartcard privacy.[28] Unlike the CTA privacy policy which at least acknowledged the existence of the Chicago Card, the "Metro Privacy and Data Use Policy" fails to specifically reference the SmarTrip card *at all*. And meanwhile, like Chicago's policy, it puts primary emphasis on information stored and collected from websites. The privacy policy explains that personal data is collected "only if you buy from us online, subscribe to our e-mail subscription service, or apply for a job online." While it is true that these are the only instances in which *personal information* is collected, personal data goes much beyond that. Personal data includes the travel histories of riders, and the fact that the WMATA collects this information should be indicated. The record of a particular individual's travel is as personal as anything else. Just as a name or address helps someone to infer the identity of a particular person, a person's travel history can also be used in determining someone's identity, albeit with more difficulty. Personal data provides the link that allows someone to determine personal information.

Because the WMATA does not discuss the SmarTrip card in its privacy policy, it is clear that the WMATA does not explain the data that is collected on individuals' as they use the card. It, like the CTA, should consider a TDDP policy. On its privacy policy, the WMATA does say that information it collects can be released if it is subpoenaed by a court or a grand jury. It should make this fact clear to its customers that this is the case for both personal information *and* travel histories. The WMATA should also explain its other motivations for tracking rider entry and exit, and justify why it needs to retain its travel history data for such a long period of time (1 to 2 years) in the policy.

[27] Pat Saccoia, WMATA Representive, Interview 10/18/2004
[28] Metro Privacy and Data Use Policy - http://www.wmata.com/about/datause.cfm

Section 6.3 - A Domestic Case in Development – Metro Transit (Minneapolis/St. Paul, MN)[29]

In May 2003, Royal Philips Electronics announced that its MIFARE technology would be implemented by Metro Transit (Minneapolis/St. Paul, MN). This made Metro Transit the first transit authority to enter into a contract to use the MIFARE card.[30] A year and a half later, Metro Transit is currently nearing its final phases of testing and will soon be ready to launch its RFID smartcard into a pilot stage. Like the MBTA, Metro Transit has not yet decided its privacy policy or finalized its implementation plans. Considering this, and the fact that both Boston and Minneapolis will be using the MIFARE implementation, this case study is particularly relevant to the MBTA's privacy policy.

A Blurry Line between Registered and Unregistered Cards

Currently, Metro Transit's RFID smartcard system is modeled to be similar to existing systems. The implementation, like the MBTA's and London's, will only require one physical card. The technological capabilities of the MIFARE card are such that many different options can be carried out on a single card. Reduced fare cards for seniors and youth, 31 day passes, and standard adult fares can all be indicated on separate "purses" programmed into the card. Because there is only one physical card, the line between a card that is registered and unregistered is more nebulous than in the case of the CTA, where there were two distinctly defined cards. Thus, we recommend that Metro transit be particularly vigilant in giving its customers an understanding of the differences between choosing to register and choosing not to. Since this was also the case for London, we recommend this measure for their implementation as well.

Integrating Use Incentives in an RFID System - The Ride to Rewards Program

Metro Transit currently administers a "Ride to Rewards" program. The purpose of the program is to encourage transit users in the greater Minneapolis area to use public transit as a consistent alternative to driving. By encouraging the use of more public transportation, the program generates increased tax revenues for Minnesotans, and, in addition, reduces local pollution due to auto emissions. Currently, the program is run on the honor system. Customers who ride Metro

[29] All specific information discussed in the Minneapolis implementation comes from:
Mary Simonowicz, Transit Store Supervisor (Distribution of Farecards), Interview, 12/7/2004
[30] "Minneapolis / St. Paul becomes first U.S. transit authority to implement Philips' contactless smart card technology." Smart Card Alliance Industry News. 5/20/2003

Transit at least three times a week are encouraged to sign up for the program. The Ride to Rewards Program webpage tells riders, "If you already ride transit three or more days a week, enroll and simply keep doing what you're doing!" The program currently has free registration, and participation has large incentives. Those who register can be entered into prize drawings for airline tickets, hotel stays, tickets for college and professional sports teams, gift certificates, and more. Providing the program an email address will allow the customer to receive information about service updates and promotions. [31]

In the context of Metro Transit's Go2Card implementation, the "Ride to Rewards" program could pose a problem. This problem arises because, upon launch of the Go2Card, Metro Transit may impose a smartcard registration requirement for all "Ride to Rewards" program members.

Admittedly, requiring registration does make some sense. At the point Metro Transit is able to track individual riding patterns, it could have the ability to more equitably distribute the rewards given by its program. Instead of having people illegitimately sign up for the program and ride Metro Transit less than three times per week, smartcard registration will verify that participants are actually fulfilling the minimum standards to receive a reward. Nevertheless, we also want to maintain a passenger's right to make an informed decision on smartcard registration. When the choice is given to people in a world of unequal incentives, we firmly believe that the program inhibits the thought calculus a person undergoes in choosing whether to opt-in or opt-out.

Currently, the Ride to Rewards program collects information from its participants in the form of names, addresses, phone numbers, and primary routes used when traveling. All of this information is currently stored in its own database. Therefore, post-implementation, Metro Transit can easily maintain a database of registered users of the *program* that is completely independent of a database that keeps track of registered users of the *smartcard.* This alternate database can thus be used for Ride to Rewards without limiting privacy.

We know that the main privacy concern with collecting travel data is that this data generally contains the locations and time stamps of the various travels of a particular customer. However, the ride to rewards program is not trying to provide incentives for traveling *to or from* certain places at certain times of the day. Rather, its intent is to provide incentives for traveling to or from places *more often*. Thus, the Ride to Rewards program (and others like it) can also be run without requiring smartcard registration.

[31] Metro Transit Ride to Rewards Program - http://www.metrotransit.org/riderPrograms/rideToRewards.asp

Because the MIFARE card can store multiple purses,[32] another purse can simply be added to the card that keeps track of the "number of times traveled." If Metro Transit wishes to reward passengers who travel more than ten times a month, this purse can be used to verify that this occurred and then be reset to "0" on a monthly basis to allow for long-term participation in the program. When a person desires to opt-out of smartcard registration but wishes to participate in Ride to Rewards, the person's name will *only* be associated with this purse that keeps track of *travel frequency*. Additionally, employees working within the Ride to Rewards Program headquarters can be restricted to access the travel frequency data *only*. If someone did not choose to register the smartcard, that person would not be listed as a registered smartcard user within those other portions of customer service that may have the ability to access travel data (times and locations).

If either of these measures were to be taken, the rewards program could be successful without attributing travel times and locations to persons using the card. Unfortunately, keeping track of travel frequencies may still be undesirable for some people, but the frequency data is necessary to provide the minimum information required to run the Ride to Rewards program.

Reduced Fares and Registration Requirements Revisited

Per our discussion with Metro Transit, one more pertinent issue came up in conversation. Specifically, they are still determining whether they would like to require registration for seniors and students who will be receiving reduced fare Go2Cards. Based on our discussion of required student registration in London, we are highly against required registration in these cases. The opposing argument we were given was that, if passengers are getting reduced fares, they should do something in return to receive them. That something in return, at least for Metro Transit, is smartcard registration. However, saying that the students and seniors need to do something in return is absurd. Transit authorities need to take a step back and look at the principles behind giving reduced fares to students and seniors in the first place. These principles had nothing to do with the seniors or students giving something in return; rather, they were based on the reality that students and seniors are disadvantaged members of society, who need to be given something in return *by the state*. Bearing this in mind, we ask Metro Transit to consider our proposals suggested to TFL in creating a reduced fare option for students and seniors using unregistered smartcards.

[32] For the MIFARE card, a "purse" is simply a separate area on the card designated for a different purpose. A MIFARE card can have separate purses for 30 day passes and cash fares, for example.

Section 6.4 - Comparing RFID Smartcard Implementations

To give the MBTA and other transit authorities of some idea of the features of current RFID smartcard implementations, we have compiled this chart (Fig 6.3) summarizing some of the key points of each major system.

	London (TFL)	Chicago (CTA)	Washington D.C. (WMATA)	Minneapolis (Metro Transit)
Name of Card	Oystercard	Chicago Card/Chicago Card Plus	Smartrip	Go2Card
Opt-out Alternative (for RFID, other than magnetic stripe card)	Oystercard (Pre-pay)	Unregistered Chicago Card	Unregistered Smartrip Card	Unregistered Go2Card
Reduced Fares on Smartcard	Yes; Students can receive discounted farecard (registered Oystercard)	No discount cards available at this time	Student cards are issued	Yes; Will offer reduced fares for students and seniors; not yet sure of registration requirement
Maximum Value on Card	n/a	$100	$300	$200, or two 31 day passes
Privacy Policy?	Yes; And have TDDP focused on oystercard	Yes; But no Chicago Card data collection policies discussed	Yes; But not specific mention of SmarTrip	n/a
Transit Data Protection Policy?	Yes	No	No	n/a
Standalone Website?	Yes; oystercard.com	Yes; chicago-card.com	No; will run through main WMATA website	No; will run through main metro transit website
Data Collection	Time, Date, and Location of each touch	Time, Date, and Location of each touch	Time, Date, and Location of each touch	Time, Date, and possibly Location
Data Retention	n/a	90 days-1 year	1 year-2 years	Not yet determined
Direct Access To Data	Customer Service and Management	Customer Service and Management	Customer Service and Management	Customer Service and Management
Times of Collection (Rail)	Sometimes entry and exit; Sometimes only entry	Entry only	Entry and exit always	Entry only
Times of Collection (Bus)	Entry only	Entry only	Entry only	Entry only
Bonus for RFID Card Use?	Yes; Users can continue paying 2003 fare rates for an indefinite period of time	Yes; $1 Bonus for every $10 added to Chicago Card	None	Bonuses given for all farecards; may apply Ride to Rewards
Other Amenities/Possible Uses	None at this time	None	None	Under Consideration
Fee to obtain card	3 pounds	$5	$5	$5
MIFARE Card?	No	No	No	Yes

Figure 6.3. Comparison of London, Chicago, Washington D.C., and Minneapolis Smartcard Implementations

Section 6.5 - Other Implementations on the Horizon

These are some of the other smartcard implementations that are currently in pilot or implementation phases. Additional research into these cases should provide further insight into the approaches that should be taken in an RFID smartcard implementation.

- *Bay Area Translink*[33]
  - *Limited Availability to Bus Users in October, 2004*
  - *Full Implementation in 2005*
- *Central Puget Sound Regional Fare Coordination Project*[34]
  - *Seven agencies will allow linked trips between bus, transit, ferries, and rail by 2006*

[33] O'Connor, Mary Catherine. "Transit Moves Ahead with RFID." *RFID Journal*. Oct. 27, 2004.
[34] Central Puget Sound Fare Coordination Project - http://transit.metrokc.gov/prog/smartcard/smartcard.html

    - *Connects Washington, Idaho, and Oregon*
- *Los Angeles County Metropolitan Transit Authority*[35]
    - *To be implemented by Summer, 2005*
- *Metropolitan Atlanta Rapid Transit Authority – Breeze*[36]
    - *First system in the U.S. to deploy a low-cost, limited use smartcard to be used for ALL fare purchases*
    - *System will feature 6-foot "jumper proof" gates*
    - *Can read any smart card that meets ISO standards (more flexibility)*

Section 6.6 - General Reflections on Interviews and Case Studies

Common themes arose from our conversations with the representatives of the various transit authorities. Most, for example, seemed shocked that privacy was even an issue with smartcards. One representative of the CTA, for example, cited that 96% of CTA riders have chosen the registered version of the CTA's Chicago Card.[37] She thus seemed compelled to believe that users did not care about their privacy. However, when consumers are not told about the privacy implications of registration, why wouldn't they register? If consumers were more informed, we believe that this number would be reduced. Certainly, many transit users wouldn't care about the data collection practices of the WMATA or CTA, but we need to acknowledge those who may change their mind based on being more informed.

In addition to those concerns presented in the body of the case studies, there are two other points that should be addressed based on the information in figure 6.4. First, the length of time data is held is generally too great. Holding data for years at a time while keeping it associated with a person's name is unnecessary. A cross-application to our privacy recommendations in section 7 will help to explain that. We also encourage the maximum value stored on cards to be lowered. In the WMATA's case, $300 in value can be stored on the card. Since transit authorities have given users the right to recoup their losses from a registered card if it is lost or stolen, users who see a higher maximum may be more inclined to register it. Although this point is low-impact, and users can just put lower amounts of money on the card themselves, it is important to avoid practices that may encourage registration.

Most of the transit representatives we talked to knew of no laws that regulated their RFID data collection practices (besides regulations against selling

[35] Metro Short-Range Transportation Plan - http://www.mta.net/projects_plans/shortrange/SRTP.htm
[36] Brenner, Kimberley. "Atlanta's Transit Authority, MARTA, is taking the Georgia City Contactless." *RFIDNews*. February 1, 2003. – Other source http://www.itsmarta.com/
[37] Interview with Leslie Caplan, Chicago Transit Authority, 12/8/2004

information to third parties), and acknowledged the new and developing nature of the laws in the RFID world. When the transit representatives acknowledged their general lack of acquaintance with any aspects of law regulating smartcards, they were often willing to make concessions and appreciate some of the suggestions we made. At this point, laws relating to RFID privacy and information collection practices are only beginning to be filed. Transit authorities need to acknowledge that the potential for these laws is real, and that it is never too early to begin taking steps to address them. Based on our review of the transit authorities in this section, it is clear that many steps still need to be taken to comply with laws that even minimally require transit authorities to explain the privacy implications of RFID smartcards.

Section 6.7 - The MBTA's Privacy Action Plan[38]

As London, Chicago, Washington D.C., Minneapolis, and other transit authorities are asked to reflect on the privacy issues relating to their present and future RFID smartcard endeavors, the MBTA is utilizing a privacy action plan throughout its process of determining an ideal privacy policy. While our paper and analysis provide tips and suggestions for creating a privacy policy, we encourage all transit authorities to create an action plan of a similar form and do their own independent analysis. As smartcard implementations change and new privacy issues arise, it is important to remain up to date on any relevant information.

The plan, as reprinted in Figure 6.4, includes several useful steps in making a privacy policy. These include researching comparable policies, consulting an outside attorney for feedback and guidance on privacy, drafting a new policy, utilizing customer focus groups and feedback, and creating a formal "privacy officer" position. All of these steps are useful, especially the ones that consider consumer feedback. An attorney is also necessary to ensure that data collection and other RFID implementation aspects do not violate local laws. However, this list is not exhaustive. Transit authorities should consider new and innovative ideas to place in their privacy action plans.

[38] Davis, Jonathan R. MBTA Privacy Action Plan to Senator Barrios, October 13, 2004.

Task	Responsible Party	Description	Approximate Duration	Comment
Research comparables	• MBTA	Compare current MBTA Privacy Policy to other agencies/companies with electronic payment systems and analyze potential changes. Compare policies of: • Transit agencies (smart cards) • Highway authorities (electronic toll collection) • Financial Institutions.	4 weeks	
Consult Outside Attorney	• MBTA	Obtain feedback/guidance regarding privacy.	3 weeks	
Draft new policy	• MBTA • Outside attorney	Utilize comparable analysis to draft new Privacy Policy.	Concurrent with above item	
Review of draft policy	• Industry Review • Public Officials	Consult with others regarding draft new Privacy Policy and update draft policy as needed including, where appropriate, elected officials.	4 weeks	
Focus groups	• MBTA	Solicit feedback from community.	1 week	
Public Comment Period	• MBTA	Post draft new policy on web site (www.mbta.com) and hold Public Comment Period.	3 weeks	
Privacy Officer	• MBTA	Assign MBTA employee as Privacy Officer to ensure privacy compliance, resolve issues and continually improve privacy policies and procedures.	TBD	
Publish new policy	• MBTA	Complete updates and publish new policy.	8 weeks	
Implement new policy	• MBTA • Others TBD	Develop/enforce any new procedures and controls required to adhere to MBTA Privacy Policy for transaction data. Ensure applicable MBTA customers are aware of privacy policy.	Ongoing	

Figure 6.4. MBTA Privacy Policy Task List

Section 7 – Legal Considerations

In this section, we focus on some of the legal discourse that exists regarding privacy and data protection concerns relevant to the MBTA's smartcard implementation. Unfortunately, law that specifically governs the use of RFID smartcard data collection is quite limited, despite the wealth of general privacy law that exists. We first examine the relevant law in Massachusetts, including recently filed legislation. We will then address an individual's Constitutional right to travel anonymously. Finally, we will examine the Data Protection Act of 1998, the law in Britain that requires entities to abide by strict data protection practices. These legal considerations represent the synthesis of what implementers of RFID should be considering

Section 7.1 – Chapter 66A

Currently, Massachusetts has one statute that restricts the information practices of entities in Massachusetts. This law, formally known as the Fair Information Practices Act, specifically regulates the use of personal data by entities in Massachusetts in Chapter 66. In section 1 of Chapter 66A, "Personal Data" is defined as follows:

> ""Personal data", any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual; provided, however, that such information is not contained in a public record, as defined in clause Twenty-sixth of section seven of chapter four and shall not include intelligence information, evaluative information or criminal offender record information as defined in section one hundred and sixty-seven of chapter six.[39]

Upon close reading, it is clear that the MBTA's collection of data in its smartcard implementation would fall well within this definition of personal data. Specifically, registered cards can clearly be associated with a particular individual. We know this because all transit authorities with RFID have emphasized that registered cards allow individuals to recover their lost or stolen fares. And, unless the transit authority knows who holds a particular card, it is impossible to return the fare on a lost or stolen card to its rightful owner.

Section 7.1.1 - Chapter 66A Requires Reasonably Minimal Data Collection[40]

Since registered CharlieCards will be subject to this law, we begin to see that smartcard data collection, in reality, is already quite regulated. In section 2(l) of Chapter 66A, we are told that "Every holder maintaining personal data shall not collect or maintain more personal data than are reasonably necessary for the performance of the holder's statutory functions." This codifies a recommendation we make relating to the storing of "reasonably minimal personal data," where this law is also mentioned (Sections N.2.1.1, N.2.2.3). The MBTA will be required by this law to confirm that it is not exceeding the minimum of data to perform its functions. By clearly explaining why the data

[39] Mass State Code, Chapter 66A Section 1, Definitions, http://www.mass.gov/legis/laws/mgl/66a-1.htm
[40] Mass State Code, Chapter 66A Section 2, *Fair Information Practices*, http://www.mass.gov/legis/laws/mgl/66a-2.htm. This document is referenced in the rest of this section.

collection is reasonably minimal in its privacy policy, we believe that the MBTA can help itself avoid legal challenges grounded in this section of the law.

Section 7.1.2 - Chapter 66A Constrains the feasibility of a Multi-Use CharlieCard

Because the function of the MBTA is to provide transit services to residents of Massachusetts, we do not believe that the MBTA should make the CharlieCard a multi-use card. As mentioned in our history section, there are personal privacy issues that could arise if a single card is used for transit, state identification, library use, and grabbing a cup of coffee at the local Starbucks. Moreover, we see from this law that the MBTA cannot centrally administer such a card legally; otherwise, the MBTA would need to collect data unrelated to its statutory function. Thus, if the CharlieCard became a multi-use smartcard, each agent that provides card functions will need to maintain an independent database for any data collected beyond the MBTA's statutory functions. From the MBTA's standpoint, this would be a logistical nightmare that is incredibly inefficient. In sum, unless the MBTA's statutory functions were expanded to serve a more general government purpose, the MBTA is not allowed to collect data that is unrelated to riding the T. And, even if its *government* functions were expanded in this way, the MBTA would not be able to collect data that may be necessary for Starbucks' *commercial* interests.

Section 7.1.3 - Chapters 66A Requires Advance Notice of a Subpoena

Even though the MBTA may sometimes be forced to release data requested via a subpoena, it should do so with complete regard for the customer. Simply put, the MBTA should take care in releasing its data to third parties, taking into account whether the customer has been duly notified of any impending release. We believe in this concept in principle, but it is also established in law. According to chapter 66A, section 2(k) of the Massachusetts State Code, personal data should not be made available in response to a subpoena unless a data subject is notified in advance and has an opportunity to quash the subpoena. To comply with this law, we recommend that the MBTA should send a written letter to any registered user of the CharlieCard whose personal data may be involved in a subpoena. Each user should be given at least 30 days to respond in some legal form to the subpoena request. Most people don't even understand their right to quash a subpoena; MBTA riders should understand that it is their right to do so.

Requests to quash RIAA[41] subpoenas have been moderately successful, and customers can make compelling arguments to have them quashed. The right to travel anonymously, an issue discussed in a subsequent section, is an example of something that can provide sound grounds for quashing a subpoena.

Section 7.1.4 - Chapter 66A Provides Customers a Right to Access Their Data

Another relevant section of Chapter 66A is section 2(j), where the law discusses the rights of individuals to both contest and correct their own personal data. The right of receiving a hard-copy of the data, moreover, is also bestowed on individuals by the Freedom of Information Act passed by Congress in 2001. These provisions require the MBTA to set up a framework in which riders will easily be able to collect their data if requested. We therefore reaffirm our prior suggestion that people should have secure methods through which they can ensure that only they themselves are given this opportunity to correct and contest their data. Our suggestion in this area was to associate a PIN number or password with each registered smartcard. Therefore, when Charlie calls MBTA customer service to obtain Johnnie's personal data, he will promptly be denied the right to view or correct it. If a protection framework is not set up, the MBTA may have instances in which third parties obtain data unlawfully. And, since the MBTA has to make its data available to consumers anyway, the time for it to act is now.

Section 7.2 – The Personal Information Protection Act

The implications of Chapter 66A are strong for the MBTA. However, recently filed legislation could provide an even greater impact. This legislation, called the Personal Information Protection Act, would create a new section of law called Chapter 66B that would add several new provisions that would restrict the information practices of the MBTA. While chapter 66A more generally covered public records, Chapter 66B specifically references the MBTA. It creates a definition of "ridership data" to demonstrate that the privacy practices in the law are to apply to the MBTA as much as any other entity. As defined, ridership data is the information that details the time and location at which a rider utilized services. The particular section of interest is section 8, which adds two major provisions that will govern the MBTA.

[41] The RIAA is the Recording Industry Association of America. It has issued hundreds of subpoenas requesting information about individuals who download music from the internet illegally.

First, the law would require that personal data not be capable of being linked to ridership data. If this law is passed, it will severely limit the MBTA's flexibility in providing registered cards. The registered card can still be tied to a person under this law, but the MBTA will be constrained in that it would only be able to associate the *amount of money* on the card with an individual. If registered cards were not tied to personal information *at all,* the MBTA would be hard-pressed to refund money from lost or stolen cards. Luckily, the law does not restrict associating fare collection data with a person. This law would require the MBTA to isolate the databases that keep track of ridership data from those that keep track of fare deductions. Thus, this law would pose some challenges to the T, but would essentially guarantee full privacy rights for all of its riders.

Section 7.3 – A Constitutional Right to Travel Anonymously

"The right to travel anonymously through our T system is a right that all customers have enjoyed throughout the T's history."[42]
–Massachusetts State Sen. Jarrett Barrios

If there was a point at which the MBTA, a public provider of transportation services, compelled all individuals to register an RFID smartcard in an all-RFID transit system, it would completely remove this right to travel anonymously. This would set a bad precedent that goes against basic principles of Constitutional law and American social norms.

Our team feels very strongly about maintaining this right. A right to travel anonymously is grounded in Constitutional Law. This right is based on the precedent established in *Griswold v. Connecticut,* which provided the first explanation of a basic right to privacy in the United States.[43] Referring to Justice Douglas' now famous opinion, he told us that "the First Amendment has a penumbra where privacy is protected from governmental intrusion" (481). Furthermore, these penumbras extend to the Bill of Rights more generally. The Fourth Amendment is also grounded in privacy. It protects against unreasonable searches and seizures of ones papers and effects. In fact, as applied by the Court, the primary focus of Fourth Amendment cases has been to protect privacy.[44] And, in *United States v. Kroll,* a Federal court found that "Compelling the defendant to choose between exercising Fourth Amendment rights and his right to travel

[42] Memo from Senator Jarrett Barrios to the MBTA, *Automated Fare Collection and Privacy Guidelines*, December 2, 2004.
[43] *Griswold v. Connecticut*, 381 U.S. 479
[44] Solove, Daniel J., "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" Southern California Law Review, Vol. 75, July 2002 http://ssrn.com/abstract=313301

constitutes coercion."[45] Another case, *McIntyre v. Ohio Elections Commission*, further recognizes one's constitutional right to speak anonymously.[46]

While speaking is not traveling in the literal sense of the word, speech is a broadly defined concept that has been extended to travel. For example, if Charlie traveled on the T to attend a protest rally, he would be exercising his free speech rights during his trip. From *McIntyre,* it would be clear that Charlie had a right to take this trip anonymously. The MBTA shouldn't have the opportunity to suspect and determine that Charlie, a well-known protester, decided he wanted to go to the rally based on the record of his departure at "Park Street."

With respect to travel, the only instance in which government interests have forced individuals to reveal their names has been in airline travel, where the government argues that a national security interest necessitates knowing the identity of every traveler. Thus, people on the whole understand why the Transportation Security Administration checks IDs at airports. Conversely, since there is no compelling national security interest in knowing the identities of all riders of urban transit, people would not understand why people should be required to utilize a card that is linked to a person's identity. Outside of cases in which there is an unusual justification for limiting privacy, people in our society are used to having the ability to travel freely and with all deliberate speed.

Section 7.4 – The Data Protection Act of 1998

In England, the Data Protection Act of 1998 governs the fair use of data by government entities.[47] It is the most comprehensive data protection law that exists right now, although other laws are sure to follow suit. This law necessitated Transport for London's Ticketing Data Protection Policy. Specifically, it indicates that individuals are entitled to be fully informed about data that is collected by an agency. The law requires that data controllers describe personal data that is processed, the purposes for which they are being processed, and the recipients to whom the data may be disclosed. It also allows individuals to submit written requests to receive their own data. The law contains an opt-out provision, and, maybe most significantly, allows individuals to take legal recourse and receive "just compensation" for any inflicted damages.

A similar law may be useful within the United States. Data collection can be conducted in a multitude of ways, and it would be useful to have a standard that

[45] *United States of America v. Gerald Frank Kroll.* 481 F.2d 884; pg. 885
[46] McIntyre v. Ohio Elections Commission. 514 U.S. 334
[47] 1998 Data Protection Act (Britain)
<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

forces entities to clarify what, why, and how data is collected. Currently, people do not understand why so much data is collected. As we move towards an Internet enabled society, the necessity for this law increases as we become more and more surrounded by information collectors. By establishing a law like the Data Protection Act of 1998, we feel that collectors will be forced to give more thought into their collection of data. After individuals collecting illegitimate data are found to have not disclosed their rationales for collecting, they will finally be subject to a law that is clearly defined. Unfortunately, the law has yet to catch up in the United States, but, once it does, we will finally be able to confidently say that people will have the opportunity to fully consider the privacy implications of the choices they make regarding RFID and data collection.

Section 8 - Our Recommendations

Because of the possible security risks in the relatively new RFID technology, and a desire to respect the rights of citizens, the MBTA and other transit systems should work to build community trust, and provide a safe and secure service. To reach this goal, we recommend that the MBTA follow the recommendations given in the outline below.

1. To build community trust
    - 1.1 The MBTA should be open about its data use policies
        - To accomplish this, we recommend that the MBTA post within T stations and on their web page:
            - That the MBTA collects data about its travelers
            - The specific data that it collects
            - How the data is collected
            - The storage lifetime of the data
            - The kinds of ways this data will be used
            - When the data can be given to an outside agency
            - How to opt out of providing data
    - 1.2 The MBTA should offer travelers the choice not to provide personal information
        - To accomplish this, we recommend that the MBTA create an opt-out policy which:
            - ▪Allows users to ride the T without providing personal information
            - ▪Has the same fare for travel as the default option
            - ▪Does not physically segregate opt-out passengers from others
            - ▪Minimizes additional frustration
            - ▪Allows for any discounts offered with the default card such

as senior citizen discounts

2. To provide a safe and secure service

2.1 The MBTA should take measures to prevent internal abuse

To accomplish this we recommend that the MBTA

2.1.1 Store a reasonably minimal amount of data

- Acceptable examples include information which is directly related to system administration or customer service such as name, credit card information, and short travel histories.
- Unacceptable examples include gender, race, and sexual orientation. These should not be stored.

2.1.2 Create data use policies and guidelines specifying

- what data uses are acceptable
- what data uses are unacceptable
    - Including sale of personal information and tracking people not under investigation.
- what to do in the case that a use is not included in the policy
- A policy for automatically recording when employees access data, what data they accessed, and for what purpose.

2.1.3 Create policies for response to a data request from law enforcement

- inform customers in writing if their data is requested by a law enforcement agency.
- give the customer 30 days to respond
- respect the customer's right to quash

2.1.4 Be able to demonstrate that the MBTA has followed its guidelines via yearly audits

2.2 The MBTA should work to prevent external abuse of data

To accomplish this we recommend that the MBTA

2.2.1 Actively encrypt all places of data transfer

- If active encryption is not possible, transferred data should not directly contain personal information, and the amount of data transferred should be minimal.

2.2.2 Keep its database separate from other networks

2.2.3 Store only a reasonably minimal amount of data

2.2.4 Keep up to date security and have regularly scheduled system security checks and updates.

In the following sections, we elaborate on the reasons for each of the above recommendations. To look for the reasoning on a particular recommendation, go to the section with the same number. For example, if you are interested in recommendation 2.2.1, please look at 8.2.2.1.

Section 8.1 - Gaining Citizen Trust

1. The MBTA should work to build community trust
    1.1 The MBTA should be open about its data use policies
        To accomplish this, we recommend that the MBTA post within T stations and on their web page:
        - That the MBTA collects data about its travelers
        - The specific data that it collects
        - How the data is collected
        - The storage lifetime of the data
        - The kinds of ways this data will be used
        - When the data can be given to an outside agency
        - How to opt out of providing data

    1.2 The MBTA should offer travelers the choice not to provide personal information
        To accomplish this, we recommend that the MBTA create an opt-out policy which:
        - Allows users to ride the T without providing personal information
        - Has the same fare for travel as the default option
        - Does not physically segregate opt-out passengers from others
        - Minimizes additional frustration
        - Allows for any discounts offered with the default card such as senior citizen discounts

Gaining citizen trust helps to increase the number of people who use the T, and reduces the amount of scrutiny aimed at the T.

To gain the trust of citizens, we recommend that transit systems follow measures to be open about their policies of data collection, storage, processing, usage, and distribution[48]. By being open and clear about polices, consumers have the option of knowing what is going on behind the scenes. This knowledge will help create a feeling of security and trust between the users and the transit system.

Transit systems should also provide a reasonable amount of choice in the amount of personal data stored and the way that the data is used. There should be an option for users who wish to remain anonymous to still ride the T without extra monetary cost or significant additional hassle.

Section 8.1.1 - Openness

1.1 The MBTA should be open about its data use policies
    To accomplish this, we recommend that the MBTA post within T stations and on their web page:
    - That the MBTA collects data about its travelers
    - The specific data that it collects

[48] 1980 Organization for Economic Cooperation and Development Guidelines

- How the data is collected
- The storage lifetime of the data
- The kinds of ways this data will be used
- When the data can be given to an outside agency
- How to opt out of providing data

To maintain trust between the T and its riders, any customer using the T should know how the T uses his or her personal data. This information might comprise a privacy policy or be incorporated into the "Customer Bill of Rights" currently on the MBTA webpage. [49]

Notifying customers of how the T uses their data will help inform people of what improvements the T is making. This notification will also highlight the efforts the T is making to improve service, cost, and safety through use of travel data. It will also give customers a sense of understanding and knowledge about how their data is being used. For openness to be effective the information must be complete and widely distributed.

To ensure that people see information on the T's collection, storage, and use of data, we recommend that this information be posted inside T stations where it will be visible to all users. If posted next to route maps or near ticket vending machines it would not need to take up a large amount of wall space. It is important that the information is in an area that the majority of customers will notice and have the opportunity to read. Posting this information on the MBTA website would be a good supplemental action, but alone would be incomplete to distribute information. Not enough T riders look at the website for posting it on the website to properly distribute the information. T riders should not have to actively seek this information out to be informed -- just like the signs about proper T etiquette and what individuals are expected to do while riding the T, what the T is expected to do for users should be widely understood by anyone riding the T.

We propose that all T riders know the following information[50],[51]:

- That the MBTA collects data about its travelers
- The specific data collected
- How this data is collected (via Charlie Card, Website, Paper Application, et)
- The storage lifetime of the data
- The kinds of ways this data will be used
- When the data can be given to an outside agency
- How to Opt-out of Providing Data

[49] Reference: http://www.mbta.com/contact_us/customerbill.asp
[50] 1977 Privacy Protection Study Commission, "Personal Privacy in an Information Society"
[51] "EPIC" - http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf

Section 8.1.1.1 - Example Privacy Statements

These examples are to demonstrate the level of depth we recommend in a transit system statement of data use. Their purpose is not to recommend an exact statement of intent or policy. While the MBTA's statement of intent should be specific, it does not need to give any implementation details or elaborate on the exact uses of the data. A short statement is more likely to be read and understood.

The first example would be placed in T stations next to the maps of the T route. The second example[52] would be linked from the front page of the MBTA webpage, and the Charlie Card web page if it exists.

MBTA Use of Customer Data

The MBTA feels strongly about the privacy of its customers. To ensure that your privacy rights are met, we would like you to know the following information.

The MBTA collects information on its travelers in order to improve customer service, improve transit times, and reduce cost. The data that the T collects enables it to provide services such as automatic Charlie Card payment via credit card, reissuing of lost Charlie Cards, and other customer service benefits. Aggregated travel data also allows the T to reduce delays and coordinate train schedules.

To accomplish these improvements, the T collects some personal and travel information. Personal information is collected via the website or paper application and includes name, birth date, home address, and credit card number. The T also logs travel data (time and location of entry and exit) via the Charlie Card. This data is stored for one month.

The MBTA does not sell or otherwise distribute your personal information to any outside agencies, except in the case of subpoena or other legal process. Should you wish to not provide your personal data, you can purchase a magnetic stripe card.

If you have any questions or concerns, please call xxx-xxx-xxxx

[52] Example based on "Oystercard – Explanation of Pre Pay Tickets."

Customer Privacy and Travel

The MBTA feels strongly about protecting the privacy of its customers. To ensure that your privacy rights are met, we would like to answer the following questions about our collection and use of customer's personal information.

What information do we collect?
We collect three kinds of information: identifying information, credit card information, and travel information. The identifying information we collect includes your name, birth date, home phone, and home address. We collect your credit card company and credit card number if you elect to pay via credit card. We also collect your travel patterns, including time of entry, time of exit, and which stations you traveled through.

How is this data collected?
Personal and credit card information is collected via our website or paper application for a Charlie Card. Travel information is collected when ever a customer enters or leaves a station with a Charlie Card, via an RFID chip inside the card.

How long is this data stored?
Personal and credit card information is stored for two years. Travel information is connected to personal identification for 30 days. Travel information older than 30 days cannot be connected to an individual.

What do we use the information for?
Information we collect is used
- to improve customer service
- to reduce travel times
- to reduce cost
- to bill customers
- for administration purposes
- for statistical analysis including travel patterns
- in response to legal measures such as subpoena

Will this information be shared with outside agencies?
We will provide information to the government in response to subpoena or other legal procedures. We will NOT give your personal information to any other agency.

We do sell statistical travel information to advertisers buying space within T stations; however, your personal information is not connected to this data in any way.

Do I have any options?
The MBTA provides an opt-out option for users who do not wish to have their personal information be connected to travel data. These users can ride the T at the same cost by purchasing a magnetic stripe card. Users do not need to present any personal information to buy this card. However, unlike the Charlie Card, the magnetic stripe cards do not have an automatic credit card payment option, nor can they be reissued if lost.

Where can I find more information on the MBTA's policies?
If you have any questions or concerns, please send an email to privacy-help@mbta.com, or call xxx-xxxx.

Section 8.1.2 Choice

1.2 The MBTA should offer travelers the choice not to provide personal information
To accomplish this, we recommend that the MBTA create an opt-out policy which[53],[54]:

- Allows users to ride the T without providing personal information
- Has the same fare for travel as the default option
- Does not physically segregate opt-out passengers from others
- Minimizes additional frustration
- Allows for any discounts offered with the default card such as senior citizen discounts

A partial opt-out policy enables users to feel that they have control over their personal information and privacy. This feeling of control and choice is critical to creating an atmosphere of trust. As an opt-out choice, most users will probably still choose the default option of providing their personal data. This is not a bad thing -- the data will be used to improve T service. What is valuable is that all users feel that they have the option of controlling their information, and that those users with concerns can alleviate them by opting out.

In order to make users feel that they have choice, they must not feel coerced or strongly encouraged to not opt-out. The choice should also be equally possible for all people, independent of their economic status. For this reason, there should be no monetary incentive to provide personal data. The fare for an opt-out customer should be exactly the same for a customer who opts in.

In particular, advantage programs, like senior citizen or student discounts, should have an opt-out option. Because these discounts lower the cost of the fare, they should be available to individuals who do not wish to have personal information in the MBTA database.

Additionally, opt-out users should not have to pay penalty in additional time or frustration. The opt-out program should minimize the additional lines or waiting that the opt-out customer must endure. Customer Service representatives should have knowledge of the opt-out program and be able to help confused customers. Opt-out customers should in no way be segregated or made to feel inferior.

[53] "EPIC" - http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf
[54] 1973 U.S. Department of Health, Education & Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973)

Section 8.1.2.1 Functionality not required for an Opt-out Program

It would be technically complicated, and sometimes impossible, to provide the exact same services for an opt-out customer as one who provides personal data. For example, it would be impossible to mail a card to someone who had not provided an address. For this reason, we refer to the opt-out policy as a partial one. The transportation time, cost, and method should be nearly equivalent between an opt-out and an opt-in user; however, extra customer service benefits do not need to be offered to opt-out users if they are complicated to implement. In this section, we explicitly cover some of the customer service functionalities which would not be necessary to implement in an opt-out program.

One customer service benefit that requires personal information is automatic reloading (automatically charging a credit card company when the account reaches a minimal balance). An opt-out policy which does not require personal information could not implement this feature because it requires credit card data and personal data to verify ownership of the credit card.

Reissuing lost cards is another benefit which might be only offered to customers who provide personal data. Via a login ID and password, it is possible for a user who has provided no personal information to have a lost card reissued. However, implementing this functionality could require major changes to an existing database, and may require substantial additional efforts on the part of the T's customer service department to implement. Most importantly, this functionality is not necessary for T users to get the main benefit of the T: transportation. It would be nice if reissuing lost cards was implemented for opt-out customers; however, it is not fundamental to protecting customer privacy rights, nor fostering trust because it does not pertain to the main service of the T: transporting people in a cost effective and timely manner.

While some functionality may not be offered to opt-out customers, an opt-out option should exist which provides equal speed of travel, access, and cost. This opt-out policy would allow users who are uncomfortable providing personal information to ride the T, and give all users a sense of control over their personal data.

Section 8.2 - Providing a Safe, Secure Service

For the MBTA to strive to provide a safe, secure service:

2.1 The MBTA should take measures to prevent internal abuse

To accomplish this we recommend that the MBTA

2.1.1 Store a reasonably minimal amount of data

- Acceptable examples include information which is directly related to system administration or customer service such as name, credit card information, and short travel histories.
- Unacceptable examples include gender, race, and sexual orientation. These should not be stored.

2.1.2 Create data use policies and guidelines specifying

- what data uses are acceptable
- what data uses are unacceptable
  - Including sale of personal information and tracking people not under investigation.
- what to do in the case that a use is not included in the policy
- A policy for automatically recording when employees access data, what data they accessed, and for what purpose.

2.1.3 Create policies for response to a data request from law enforcement

2.1.4 Be able to demonstrate that the MBTA has followed its guidelines via yearly audits

2.2 The MBTA should work to prevent external abuse of data

To accomplish this we recommend that the MBTA

2.2.1 Actively encrypt all places of data transfer

- If active encryption is not possible, transferred data should not directly contain personal information, and the amount of data transferred should be minimal.

2.2.2 Keep its database separate from other networks

2.2.3 Store only a reasonably minimal amount of data

2.2.4 Keep up to date security and have regularly scheduled system security checks and updates.

In addition to fostering a sense of trust in its customers, the MBTA wants to provide a safe service[55]. With regard to the RFID cards and databases, our recommendations emphasize creating a secure database, which it is difficult to steal information from, and easy for internal abuses to be tracked and identified.

Some of the possible effects of data abuse are given in Section 5. Misuse of data is becoming more prevalent as more databases are being made of personal information. A common example of internal abuse is illegal release of medical records. External abuse of databases includes selling lists of names and social security numbers for identity theft. With the growing rate of crime in these areas, the MBTA should take precautions to avoid internal and external abuse of data. In the case that it occurs, the MBTA will be able to show that it made a good effort to prevent this crime.

[55] Reference: http://www.mbta.com/contact_us/customerbill.asp

Section 8.2.1 Preventing Internal Abuse

2.1 The MBTA should take measures to prevent internal abuse

To accomplish this we recommend that the MBTA

2.1.1 Store a reasonably minimal amount of data

- Acceptable examples include information which is directly related to system administration or customer service such as name, credit card information, and short travel histories.
- Unacceptable examples include gender, race, and sexual orientation. These should not be stored.

2.1.2 Create data use policies and guidelines specifying

- what data uses are acceptable
- what data uses are unacceptable
    - Including sale of personal information and tracking people not under investigation.
- what to do in the case that a use is not included in the policy
- A policy for automatically recording when employees access data, what data they accessed, and for what purpose.

2.1.3 Create policies for response to a data request from law enforcement

2.1.4 Be able to demonstrate that the MBTA has followed its guidelines via yearly audits

Preventing internal abuse of data helps to reduce the chance of stalking or theft caused by a T employee. Internal abuse prevention also helps to ensure that due process is being carried out, and shows an effort on the part of the T to respect the rights of citizens and ensure their safety.

To prevent internal abuse of databases, we recommend that the MBTA store a minimal amount of data, create policies surrounding acceptable data use, and create methods to enforce accountability. Storing minimal data will reduce the possible damage that can occur from an employee abusing their access to data. To provide organization and clarity, we recommend that the MBTA create policies that outline what uses of data are acceptable, how acceptable uses can be carried out, what data uses are unacceptable, and who can access the data the data. To help locate abuses after they have occurred, we recommend that the MBTA store when employees access the database and what portion. Finally, we recommend that the MBTA have some form of yearly audit to demonstrate accountability.

Section 8.2.1.1 Storing Reasonably Minimal Personal Data

2.1.1 Store a reasonably minimal amount of data

- Acceptable examples include information which is directly related to system administration or customer service such as name, credit card information, and short travel histories.
- Unacceptable examples include gender, race, and sexual orientation. These should not be stored.

To prevent internal abuses of data the MBTA should limit stored data by storing reasonably minimal information which is required for system functionality (like billing or travel), not aggregating databases from other sources, and separating user information from identifying information (not reconstructible, or reconstructible only via cryptography following a special circumstance like a court order).

Internal abuses of user data would be impossible if the user data did not exist. Moreover, the more data which is stored, the more severe the abuse could be. However, taking no data eliminates all of its potential uses. A careful balance should be struck between use and security when storing data. As required by Ch. 66a, section 2 of Massachusetts State Law, government agencies must

> "(*l*) not collect or maintain more personal data than are reasonably necessary for the performance of the holder's statutory functions [56]"

.We recommend that a reasonably minimal amount of data (such as travel data) be stored which could be connected to personal information through a unique ID number. Additionally, we recommend that a reasonably minimal amount of personal data be stored, such as name, contact information, and credit card information. We take this to mean that data which serves a function can continue to be stored; however, data with little or no potential use must be deleted.

For instance, data concerning a customer's name, home address, credit card, and verification information are all useful; however gender, sexual orientation, and race are not necessary for billing or transportation and should not be stored at all. Storing excess amounts of data make identity theft easier.

In addition to reasonably minimal, we strongly recommend that data is not cross linked from other sources. In addition to quality control issues, cross linking data poses large risks for abuse via stalking, pre-preemptive legal action, and targeted advertising.

Fortunately, the statistical data needed for T usage studies, and even some

[56] "Chapter 66A Section 2, *Fair Information Practices.*" Massachusetts State Code.

advertising purposes does not require any personal information. Travel data for statistical studies remains useful over long periods of time; however, the individual who made that journey is not needed for these studies. The value of personal information being attached to travel information usually dies out over time. Periodically separating travel data from personal information only slightly reduces the usefulness of the data, while greatly increasing the security of the users.

For example, if a data base stores the following information:

Recent Data:
(John Smith (11-29-2004 SouthStation) (12-1-2004 SouthStation))
(Abby Flecher (11-28-2004 Wonderland) (12-1-2004 ParkStreet))

Old Travel Data:

Then, after a period of time, the information could be separated:

Recent Data:
(John Smith)
(Abby Flecher)

Old Travel Data:

((11-28-2004 Wonderland) (12-1-2004 ParkStreet))
((11-29-2004 SouthStation) (12-1-2004 SouthStation))

After separation, it is still possible to do a statistical usage study of the T; however, it is not possible to figure out if John or Abby traveled to Wonderland on November 28th, 2004.

The amount of personal travel data stored should not allow accurate prediction of where an individual will be on a given day of the week at a given time. To prevent this, separating personal information from travel data would need to be done at least every two weeks. Data separation of this frequency would mean every day of the week would have at most two records of personal travel data. For travelers who are consistent across days of the week, even this amount of data would be enough to determine movement patterns to a reasonable accuracy. However, it would be difficult to predict travelers with some variety of travel times with only two weeks of data.

However, data has important uses up to one month, including law enforcement and audit reasons. If a crime occurs or a missing person is reported, it is reasonable to expect that law enforcement could request data within one month of the event. Also, if a traveler wants to dispute a bill, it is reasonable to require that they notice the problem and bring it to the MBTA's attention within a

month.

Because data is still useful within a month's time, we recommend that the MBTA separate personal data from travel data at least monthly[57]. We would prefer that the seperation occur every two weeks. Note that storing any identifying number with both travel records and personal records will not effectively separate travel and personal information because the connection between travel information and personal information can be reconstructed.

In summary, to prevent internal abuses of data the MBTA should store a minimal amount of data by not cross linking databases from other sources, storing only information pertaining to travel and billing, and separating user information from identifying information.

Section 8.2.1.2 - Data Use Policies

2.1.2 Create data use policies and guidelines specifying
- what data uses are acceptable
- what data uses are unacceptable
  - Including sale of personal information and tracking people not under investigation.
- what to do in the case that a use is not included in the policy
- A policy for automatically recording when employees access data, what data they accessed, and for what purpose.

In addition to storing a reasonably minimal amount of data, we recommend that the MBTA create guidelines for data access and use. We also recommend that the MBTA create logs of when employees access data, what data they accessed, and for what reason. Creating data use policies and logging employee data will help the MBTA explain to employees what practices are acceptable and what are not. The employee logs will provide the MBTA with a method to verify that it has followed its policy. Finally, the logs will enable the MBTA to do business and customer service studies to improve its business model.

The MBTA should create employee user names and passwords to allow employees to access the database. These user names will allow the MBTA to record when employees access data. In the case of legal dispute, the MBTA could reference these logs to demonstrate innocence or to investigate which employee violated company policy. The size of system logs of this kind would be a minor in comparison to the size of travel data of T users, and help the T maintain its policies.

[57] Also recommended by Michaud, Dan. Interview with Jennifer Novosad. 27 Oct. 2004. MIT Card Office.

The MBTA should also limit the number of people who have access to the data. With data access requiring a log in name and password, the implementation would be fairly simple. The difficulty would be in deciding which people have access to the data, and how much of it they have access to. Ideally, access to the entire database should be restricted to as few people as possible (on the order of 10)[58]. Information that is not tied to personal or identifying information could be available to many more people (on the order of 50 to 100), or by request. Reducing the number of people with access to sensitive information such as personal identifying information reduces the likelihood of internal abuse.

In order for the MBTA to publish what it uses data for, and for employees to be knowledgeable of acceptable data practices, the MBTA should create a policy listing what data uses are acceptable and what are not. Examples of allowable uses include

- any statistical studies using travel data completely stripped of personal information
- providing a travel log to the government in response to subpoena
- system maintenance or improvement
- customer service or billing
- customer request to look at their record

Important examples of unallowable uses include:

- Selling personal data (addresses and names, or names and travel information) to companies for advertising or other purposes.
- Tracking individuals not suspected of crime.

For each example of allowable data use, the MBTA should provide a procedure or policy by which the data should be accessed for that use. These formal procedures are particularly important when an outside agency such as a police department or company wishes to access data for allowed purposes like usage studies.

Of course, it is impossible to predict all possible uses for data in advance. The MBTA will also want to create a policy for who will decide if a use is allowable or not, should the use under consideration not fall into the written guidelines.

[58] Recommended by <Michaud, Dan. Interview with Jennifer Novosad. 27 Oct. 2004. MIT Card Office.> based on his experiences in the card office.

Section 8.2.1.3 Response to Government Request for Data

2.1.3 Create policies for response to a data request from law enforcement

Other travel data collection agencies have been asked for information to help in court cases. The MBTA should decide on clear guidelines for how to respond to these requests.

We recommend that the MBTA

- Inform customers in writing if their data is requested by a law enforcement agency.
- give the customer 30 days to respond
- respect the customer's right to quash

Section 8.2.1.4 Accountability

2.1.4 Be able to demonstrate that the MBTA has followed its guidelines via yearly audits

We recommend that the MBTA undergo yearly audits to analyze if the practices of MBTA employees are in agreement with the data use policies[59]. By allowing yearly audits, the MBTA will improve internal data security, catch abuses and locate dangers that would otherwise not be found. Audits will also increase outside trust in the system. If the audit could be done by an outside agency, it would be more effective in finding errors and increasing system trust. If this is not possible, an internally conducted audit would still be useful. Auditors should receive the system logs about employee data access, and be assisted by an employee with full data access.

Section 8.2.2 - Preventing External Abuse

2.2 The MBTA should work to prevent external abuse of data

To accomplish this we recommend that the MBTA

2.2.1 Actively encrypt all places of data transfer

- If active encryption is not possible, transferred data should not directly contain personal information, and the amount of data transferred should be minimal.

2.2.2 Keep its database separate from other networks

2.2.3 Store only a reasonably minimal amount of data

2.2.4 Keep up to date security and have regularly scheduled system security checks and updates.

We recommend that strong encryption be used at every point of data transfer or access, that data is difficult to retrieve from remote systems, and that the amount of data be reasonably minimal.

[59] Recommended by Michaud, Dan. Interview with Jennifer Novosad. 27 Oct. 2004. MIT Card Office.

Section 8.2.2.1 - Encryption

2.2.1 Actively encrypt all places of data transfer

- If active encryption is not possible, transferred data should not directly contain personal information, and the amount of data transferred should be minimal.

To prevent adversaries from accessing data by eavesdropping on communications between parts of the system, we recommend that data be encrypted whenever it is transferred. Examples of transfer points include between the card and the reader, between the reader and the database, and between the database and any other computer or network. Sensitive data like credit card numbers should remain encrypted while in storage, using a different encryption system. This is a safeguard in the event of security breach.

Because RFID cards can be read remotely[60], it is particularly important that data on them is actively encrypted (equivalently, the card should send out a variety of signals, rather than just one signal). If the card only sends out one kind of signal, and unfriendly agent could read the signal remotely, and then send out that signal to impersonate that card. The unfriendly agent would not need to break the encryption, only be able to read the card. Since handheld readers can be purchased or built, cards should be carefully encrypted.

Passively encrypted cards simply emit the same data over and over again with the same encryption applied to it. This is completely ineffective if our fear is about cloning cards; a clone card might have no idea what it is broadcasting, but can access restricted items regardless. For more information, please see Appendix A, particularly the subsection concerning encryption.

If cost prevents cards from being actively encrypted, it is crucial that cards are not rewritable and contain only a number. While this number will relate to personal information in the database, an unfriendly agent with a handheld reader could only learn a number from reading cards of passerby. Though this number can be used to steal money from T rider's accounts, it could not be used to impersonate them in any other way, like a name, social security number, or address could.

Additionally, particularly sensitive information such as credit card numbers may need to have a second layer of encryption for storage. This encryption layer should be particularly difficult to break without the key, such as public key encryption. Decryption could occur as the data is needed, such as for billing purposes.

[60] CNETnews.com - http://news.com.com/RFID+tags+become+hacker+target/2100-1029_3-5287912.html

Section 8.2.2.2 - Separation from other Networks

2.2.2 Keep its database separate from other networks

To improve security, the number of places data can be accessed from should be minimized; equivalently, data should be connected to the smallest network possible.

For example, the server that holds the user data might have a protocol to accept incoming information, virus check it, and store it. The server would never execute incoming files, to reduce the possibility of virus attack. However, removing data from the server might require being in physical proximity to the server, or physically connected through a local network.

We recommend that user information not be accessible from the internet. Rather than attempting to guess a password through internet protocol, a hacker would have to know which physical machines stored the data and hack into them. This creates one more barrier to data access.

Keeping user information off of the internet has the disadvantage that T travelers cannot use an online account to view their information or register for a Charlie Card. Instead, they would need to mail requests or make them in a physical location like a T station. We feel that this disadvantage is necessary to protect users from the dangers of data breach such as stalking or credit card theft.

Section 8.2.2.3 Minimal Storage of Data

2.2.3 Store only a reasonably minimal amount of data

The value of the data contained in the database will relate to outsiders desire to hack in. By storing less data, the value of the database can be decreased to make it a less attractive target.

Of course, a certain amount of data will need to be stored for normal functioning of the system. Storing a reasonably minimal amount of data would help prevent identify theft, while still allowing for system functionality.

Travel data connected to user profiles should have a limited lifetime. We recommend no more than one month lifetime, and would prefer no more than two weeks so that data could not be used to create consistent travel pattern models (See section 8.2.1.1). The purpose of removing the personal information

from the travel data is to reduce the possibility of stalking that could occur if an unfriendly agent hacked into the data base. Fortunately, travel data can still be useful without a connection to any personal information. Travel information without personal information can still be used in statistical studies such as T station usage over the day, finding traffic between two stations, and looking at statistical movement patterns. To separate travel data from personal information, a database would only need to create tables with lists the times and locations of travel of anonymous users to store what movements were made over a month long period.

In accordance with storing a reasonably minimal amount of data, the data base should not be cross-linked with other data bases or contain unrelated aggregated data. For example, a data base of library records should not be linked with the MBTA's database. The combined database would be a larger target, and require only one security breach where before two were needed. Also, with a larger amount of information available there, and unfriendly agent could create more damage with malicious actions.

Section 8.2.2.4 Evolving with Technology

2.2.4 Keep up to date security and have regularly scheduled system security checks and updates.

Because new hacking and virus technologies are constantly being produced, and any system can be hacked given enough time, it will be necessary to periodically update the security software of the architecture to maintain a secure system. We recommend that the MBTA include somewhere in its internal policies a schedule for mandatory evaluation and updates of the current system.

Section 9 - Suggestions Not Included

There are many recommendations commonly included in other reports which we have decided to leave out. We left these out because they did not pertain to the situation of the MBTA and other transit systems, or because they did not make sense given our other recommendations. The recommendations what we did not include involve data quality, specifying a particular architecture, including additional information in the privacy policy, and printing notices where ever RFID is in use. These recommendations are not necessarily bad; we did not feel that they were required.

Section 9.1 Data Quality

Many recommendations for commercial RFID use emphasize the importance of data quality and correction methods[61]. While data quality in credit card information will be necessary for billing, it is not vital to system function that other personal data and travel data be of high quality. Low quality can be tolerated because of the minimal use of this data.

It will be expensive, time costly, and difficult to verify travel data to assure quality. At best, the MBTA could design a web page that allowed travelers to look at their recent travel logs and report errors. However, any architecture that makes it easy for multiple users to access their data and propose modifications would also make it easier to hack into. If data access and modification requires going to a physical location, T riders would be much less inclined to. So, we do not recommend concern about maintaining high quality data. Instead, we recommend that the MBTA restricts data use to tasks that are not critically dependent on data quality.

Section 9.2 - Specifying Where Data is Stored and How in the Privacy Policy

We did not recommend that the MBTA explain in its privacy policy where data is stored and in what fashion. The security risks of this action outweigh the potential benefits. The storage architecture matters little to users of the system, since the data can be taken from one architecture and moved to another without

[61] "EPIC" - http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf lists some documents in which these recommendations were made

modifying the data contents. Additionally, the data storage doesn't effect what processing can happen on the data. What data is contained and for how long are far more valuable pieces of information, which can be announced to the world with less security risk.

Section 9.3 - Recommending a Particular Storage Architecture

While Appendix B contains a particular architecture, it is meant as an example rather than a recommendation. In this situation, there are many architectures which would meet our recommendations. There is no need to constrain so severely the flexibility of the system.

Section 9.4 - Including Why Data Use is Acceptable in the Privacy Policy

While including the reasons behind data usage in a privacy policy could be helpful in building trust, we do not explicitly recommend for two reasons. Firstly, the acceptable uses of data should be fairly self explanatory. If a user does not agree with certain data uses, they can elect the opt-out option. Secondly, the more words that the privacy policy contains, the less likely users are to actually read it. If no one reads the privacy policy, it does nothing to inform the public and build general trust and understanding about the system.

In cases where use of personal information does not directly benefit the customers, data users should explain why their use of data is acceptable. For instance, if a company uses personal information to determine the cost of a product or ensure that the correct amount was paid, the company should explicitly state why use of personal data is acceptable.

Also, data users should explicitly state why data use is acceptable in cases where providing personal information is mandatory. In the case of the MBTA, we've recommended that the MBTA offer an opt-out policy. However, a government agency should explain why data use is fair in cases when providing personal data is mandatory.

Section 9.5 - Printing "RFID Inside" Whenever RFID Technology is Used

In the case of a transit system, anyone with prior knowledge of smart cards and RFID would know that the contactless cards contain RFID chips. Users who do

not know what RFID chips are would also benefit little from the announcement, except being given the incentive to research what the technology is. Other methods of communicating the existence of RFID technologies are available, and perhaps superior, such as newspaper articles announcing the change to smart cards. Within these other sources, some information could be given on what RFID is.

There are other applications where RFID is not readily apparent, such as inside the paper of dog food bags, where we agree that some warning should be printed. However, contactless smartcards are not stealthy methods of RFID use, and the warning label would be unnecessary.

Appendix A - Technical Information

A.1 - Overview of RFID System

A.1.1 What is RFID?

RFID is a term used for a system that uses radio waves as the carrier of a unique identifier or other data that typically, but not always, correlates the "host-object" to a listing in a central database. RFID technology has been around since the 1940s - the first real application being WWII airplane identification[62]. Due to the cost of manufacturing small, rugged and power efficient microchip technology, it hasn't taken widespread root until recently.

Figure 1
http://www.fouga.net/ - WWII Transponder Box

The system typically implemented for RFID consists of three main components: tags, readers, and middleware (i.e. Servers and software)[63]. Tags can be powered by a battery or can receive their energy from the reader. They can also be really small or quite big. Readers come in many different flavors as well. Most readers are connected to a main database which contains further information about the item associated with the tag. Together, these components create a robust and quite remarkable system which is only now starting to be realized in its finest potential.

A.1.2 What the DOD and Wal-Mart see in RFID

By January 2005, the United States Department of Defense and super-retailer Wal-Mart would like their suppliers to embed RFID technology into all products

[62] ZDNet UK – RFID Special Report- http://insight.zdnet.co.uk/specials/rfid/0,39026568,39153971,00.htm
[63] Definition of an RFID System: http://www.webopedia.com/TERM/R/RFID.html

shipped to them[64]. Many sources claim that it is unlikely RFID technology will actually make it into every item on the shelves of Wal-Mart by the January date, however, the request by these big two product-movers sets a tone for widespread implementation of this technology.

2 - http://www.cydome.de/ - RFID Tag on a Consumer item

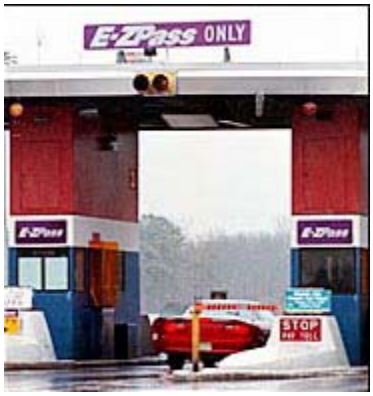
Wal-Mart's website claims that RFID technology will predominantly be used at the case and palate level, thus, most items in the store will not be tagged, but rather will have the time-tested one-dimensional barcode. Items that will have active RFID technology attached will be labeled as such for consumer awareness[65]. Technology such as RFID is being implemented to improve supply-chain management. Items such as a box of razors will surely have anti-theft devices enclosed, although RFID technology is probably considered too expensive for the individual item level. The price of tags is the predominant hindrance to near-ubiquitous implementation. Currently around $0.30 a piece for the passive tags that Wal-Mart would like to implement, the price would need to drop to around $0.05 a piece and gain a few percentage points in reliability before it would be profitable to use them in a more widespread fashion[66].

The DoD has been using RFID to cut back inventory processing headaches. RFID "allows the improvement of data quality, items management, asset visibility, and maintenance of materiel," says a briefing on the DoD decision. Furthermore, "RFID will allow the Defense Department to improve business functions and facilitate all aspects of its supply chain," the brief continues.[67] By 1/2005, the military would like passive RFID tags on most item-level tracked supplies. Once again, the government and commercial push to RFID will likely speed up widespread adoption, however, chip prices are still too high for ubiquitous implementation.

[64] Wired News - http://www.wired.com/news/business/0,1367,61059,00.html
[65] Wal-Mart website - Home Page>Supplier Information > Radio Frequency Identification Usage
[66] Wired News - http://www.wired.com/news/business/0,1367,61059,00.html
[67] DoD implements RFID - http://dc.internet.com/news/article.php/3098561

A.1.3 Active or Passive

A form of RFID which has been around for some time now is the SmartPass or EZ-Pass toll paying device. For those unfamiliar with this device, it is a small battery powered box which sits in the rear window of a vehicle. When that vehicle drives through a toll equipped with the proper hardware, the toll and the box communicate and deduct the proper toll amount from the proper user's account.[68]



3 - http://www.notbored.org - EZ Pass lane on a freeway

The form of RFID being used in this case is far different than the RFID being used in Wal-Mart or on mass transit systems. The differences mostly stem from how the device is powered: battery vs. harvesting its energy from the reader.

Battery powered RFID devices transmit farther, typically can do more calculations, might have sensors embedded on board and are bigger.[69] Most battery powered devices are called "active" RFID devices because they have power regardless of the presence of a reader. Active devices are used in large cargo tracking, most EZ-Pass systems, Exxon Speed pass systems etc. These devices are typically larger – they have a battery on board – and they are usually built in a boxy form factor. They can transmit further since they have their own power source and don't simply reflect back waves, but generate them. A typical RFID transponder used in automotive applications can transmit to about 25 feet.[70]

4 - http://www.port2port.co.il - Container tracking uses Active RFID

The other major category of RFID devices are called "passive." These devices do not have a battery but rather harvest their energy from the reader in some fashion. The best way to think

[68] EZ Pass Website- http://www.ezpass.com/static/info/index.shtml
[69] "RFID Basics" http://www.savi.com/rfid.shtml
[70] http://www.awid.com/new/Sub-Page/DougCram-Active-vs-passive.pdf

about passive RFID tags is that they reflect back the energy coming from the reader with some changes that carry the sent data[71]. One of the most common form factors of passive devices is the smart card. Because these devices must get their energy from another device, they lack the power to do computationally intensive tasks and thus typically have weak encryption, since good crypto typically requires memory and power.

A.1.4 What's so remarkable about this stuff?

RFID is seeing a lot of attention recently because it has the potential to revolutionize logistics. People who specialize in moving things around the globe would probably benefit greatly from better tracking of assets. UPS has made an entire market niche by knowing where things are and how to move them quickest. If industry and government didn't have to worry so much about making sure "stuff" got somewhere, business would occur much quicker and with less loss. Commerce could change forever. Imagine that a manufacturer, say Kellogg's, makes Honey Crisps, the hottest cereal around. They make them in big tubs and each tub is a homogenous mix of that type of cereal. Boxes are filled by tub and each box contains a small chip and an antenna – an RFID tag, essentially. As the boxes are filled, a scanner logs the box and associates it with the huge batch and the location it was made etc. The boxes are sent to the packing room where they are bundled into crates and onto palates. They are loaded with what appears to be carelessness onto trucks, but a sensor on the shipping door queries each and every box on each and every palate and asks it for its serial number. The database then associates a box with a palate with a truck. The trucks are driven to their destinations and the requisite number of crates is removed casually and delivered to the customer, namely a supermarket. An RFID sensor on the back of the truck interrogates the crates as it is pushed off and sends the data with a GPS tag to the main database which associates the boxes with crates with a truck with a drop-off location. The supermarket, assuming they are in the 21st century, also has an RFID sensor connected to this database grid. This logs the entry of the boxes into the store and verifies that they all made it to their destination.

A few days later, most of the cereal has been bought. Consumers, as they grab a box, go to the check-out line, an RFID sensor checks the box and now associates their credit card number with their purchase and can be associated back to the batch and the crate and the van and the warehouses and now, to the buyer. People go home, chow down on their food and some, unfortunately, experience food poisoning. People get wise to the cereal causing the problem and call

[71] http://www.awid.com/new/Sub-Page/DougCram-Active-vs-passive.pdf

Kellogg's. Kellogg's gets the number off the box and immediately does a query on the entire batch and correlates food poisoning reports. The database analysts realize that the common thread is the truck the cereal was shipped on. They immediately check where all the product went and recall those exact boxes – nothing more, nothing less. They make a profit, the consumer is safer, their product is tracked and they lose less money to theft and the like.

One might look at this example and note that the RF portion of the RFID system had a lot less to do with making this work than the database part. This is absolutely true, however, the architecture lowers the threshold of "willing to input data into DB" to near zero, as data is automatically entered passively (to the user) by invisible radio waves and "smart" chips.

One might also look at this example and be scared for the dickens because credit cards can be easily linked to products and companies can track how much a consumer uses the bathroom by correlating amount of Charmin with the user and dividing by the household size (also in a public database somewhere). Well… unfortunately, that is something RFID doesn't really improve upon – it's a philosophical question of whether that data should ever be linked or even exist – some say no, others yes. That discussion will take place in our recommendations section. The important thing to note, however, is that technology alone is not bad or good, scary or exciting – it's the implementation and the administrators who can make or break a system.

A.2.0 Plunging one level deeper (technically)

A.2.1 Active vs. Passive revisited

Active and passive cards are the two main types. Big devices (EZ Pass, Container tracking etc) mostly use active tags. Small devices (consumer goods, smart cards, etc) mostly use passive tags. Active tags literally contain a battery, passive tags get their energy from the reader. Good – that's the basics (and close to all we really need to know for this discussion); however, for the purpose of contemplating the deep philosophical meaning of "how far can my card be read," one might find the intricacies of these implementations quite interesting.

A.2.2 Passive Cards – Inductive vs. RF coupled

Passive cards are powered by the reader. This means that if someone stood on a subway and had a reader, that person could read a Charlie card – provided they could get close enough to give it the juice it needs to send back a response.

There are two main types of passive cards, Inductively coupled and RF coupled. Inductively coupled cards get their energy through the near field radiation from the reader. This means, essentially that there is a coil of wire in the reader which has a high frequency current flowing through it. Your card also has a coil of wire. When two coils of wire (one with a time-varying current flowing through it) get close to each other (horizontally – i.e. in a flat fashion) they can transmit power to each other. When the coil in the card is connected or "loaded" power is drawn from the magnetic field created by the reader in the near field (less than a wavelength away). If the coil is not connected then much less power is drawn from the field. This difference can be seen by the reader as a voltage drop (or lack thereof) across *its* coil. Data can be sent by connecting and disconnecting the coil in the card using a transistor. A disconnected coil might indicate a '1' and a connected coil might indicate a '0,' perhaps.[72]

5 - http://www.giveaway.com.cn – Inductor powered toothbrush

Implementations of inductive coupling are used quite commonly in electric toothbrushes. Since people wouldn't want the toothbrush to short out or zap the user, the entire device is covered with plastic – so how does the electricity get in there to move the bristles? Well, the base has a coil with current flowing through it and the brush has a coil with a storage element attached to it. Together, they transfer power as discussed above.[73]

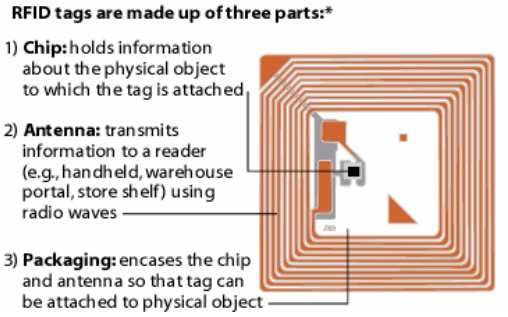
The only problem with this technique is that the two objects must be close to each other (like ¼ the wavelength of the oscillating current in the coil) to actually work efficiently. For all intents and purposes, that means the Charlie Card must be within a few inches of the reader for it to transfer enough power to get the card to respond properly. (Assuming the Charlie Card is inductively powered, which it is.)

[72] http://www.rfid-handbook.de/rfid/types_of_rfid.html
[73] http://www2.abc.net.au/science/k2/stn/posts/topic179735.shtm

The other main type of powering mechanism is RF or Backscatter coupling.[74] Cards get their energy from the far field of the reader in RF coupling. Essentially, the reader sends out an RF wave which propagates out in a sort-of baloonish fashion from the reader. The farther away from the reader, the less power is transferred. The max read distance is determined by how much power is emitted from the reader. Some reports say RF coupled devices can be read at 17 feet[75]. This means that the Charlie Could be kept in someone's pocket and read from a distance without detection. Small movements in user position wouldn't affect trying to read the card at this distance for an extended period of time – as one might do if trying to break an encryption mechanism. Fortunately for the MBTA and consumers, the MIFARE standard (what the Charlie Card uses) is inductively coupled and isn't as susceptible to this sort of attack.[76]

An interesting thing to note is that a simple piece of Aluminum foil folded into an envelope (with the card inside) can prevent all RFID from leaking out and into the hands of an evil-doer. If users are afraid their cards will be read surreptitiously, they might consider this cheep "Faraday Cage" solution to the problem and rest assured that their waves are safe in the foil – just make sure the card is not visible at all and that all edges are folded over for this to work.[77]

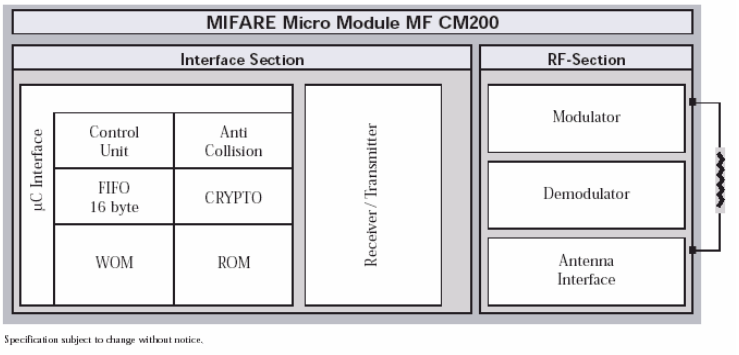
A.2. How cards are fabricated



RFID tags are made of three components – an IC, an antenna and packaging. An IC is an integrated circuit – a chip – which has etched onto it a set of "instructions" which command it to interact with the reader and do something useful. This chip might contain memory, crypto tools, modulation & demodulation components, control units, anti-collision and other tools which allow it to do more advanced functions. The IC is the brain of the RFID tag – without it, we'd simply have a theft prevention coil which resonates but does nothing.

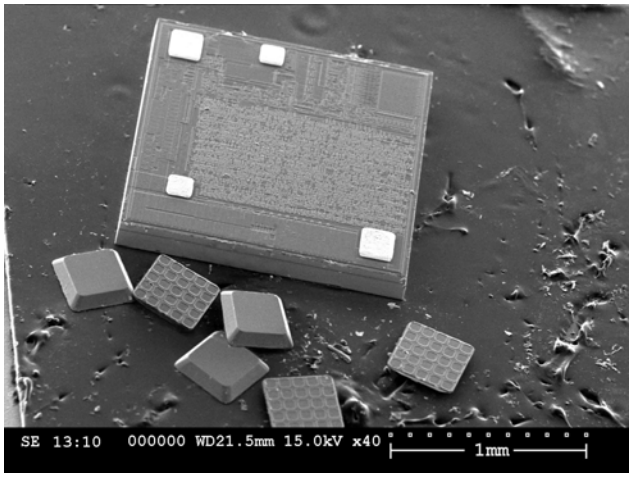
[74] http://www.connect802.com/rfid_facts.htm
[75] http://www.rfidjournal.com/article/articleview/1078/1/1/
[76] http://www.semiconductors.philips.com/markets/identification/products/mifare/
[77] http://en.wikipedia.org/wiki/Faraday_cage

The Antenna is also key to the RFID tag. The antenna is essentially a coil of wire which resonates with a certain frequency of radio waves – namely those coming out of the reader. The antenna can be a coiled piece of wire which was at one point spooled or it could be printed metallic ink which happens to be printed such that it makes an antenna the correct size.



6 - Philips' Schematic for a MiFare card

Most modern, cheep RFID tags use printed or stamped antennas. Some new techniques are actually "growing" antennas using chemical deposition techniques which could also solve the age-old problem of strapping an antenna onto a chip.[78]



7 - Microchip under a Microscope - Deloitte

The last component of the RFID tag is the packaging. The packaging can be a sliver of plastic – i.e. a card, or it can be a sticky tag which adheres to a retail product. Packaging can also be a proper housing, or… whatever. The packaging is fairly insignificant aside from holding the tag together. Packaging should not be metallic or adhered to a metallic object, as metal will block the RF radiation and prevent proper functioning of the tag.

[78] http://www.rfidjournal.com/article/articleview/975/1/1/

A.3 Pushing the technical limits

RFID cards can do a lot, for sure, but despite manufacturer claims of reading distances and encryption techniques, there are fundamental laws of electromagnetics which must be obeyed. Read distance, for example, arises because of two things: the data signal and noise. The data signal needs to be "louder" than the noise or else it becomes as useful as a quiet poetry reading in a rock concert. Typically, the best way of reducing noise and boosting signal is to stand closer – hence, the read distance concerns with RF coupling. There are other techniques, however, which can enhance read distance.

8 - http://www.paicast-5.rl.ac.uk - a bigger sized aperture for RF radiation (used for satellite communications)

An aperture is essentially a "hole" through with signals enter a system. A lens and a satellite dish are both apertures. As demonstrated with the Hubble space telescope, a bigger lens means you can see further.[79] The same goes for RF – a bigger aperture (not a bigger antenna, per se) allows one to read RFID cards from farther away. The implementations of possible "snooper" apertures are far beyond this paper, but it is physically possible to build systems which can read some cards at much greater distances. The important message here is that one shouldn't rely on physical "limitations" or manufactures' specs to provide a cloak of privacy, but rather implement security mechanisms despite the physics. Every day, we make advances in science and technology, there is nothing stopping someone from making a device which can read an RFID card from a few hundred feet away as if the two were only a few inches apart.

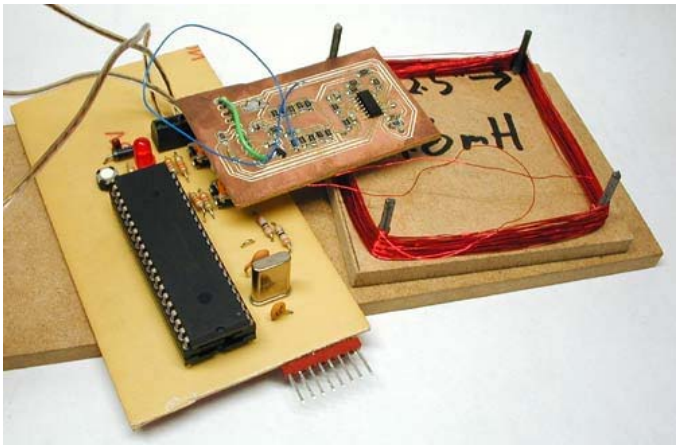
A.4 ###%20# hWo eNeds nEcryption? ####^%687#

In the beginning, there were cards and there were readers. Cards emitted a signal and always emitted that signal when readers asked for it. All were happy until people started poking around. When the technology to read cards became less secretive and more widespread among the cracker population, the security of this access mechanism was lost. Crackers could interrogate a card and replicate its output. They could fool a reader into thinking their emulator was a

[79] http://www.astro-tom.com/telescopes/beginner's_advice.htm

real card and thus, they could masquerade as someone they were not – without the person being any wiser.

There's a nifty article about cloning a prox card at <http://cryolite.ath.cx/perl/skin/prox> which details a curious engineer's endeavors to hack a prox card system. Basically, the author figured out how the cards transmitted a signal by looking at the output of a card when blasted with a single frequency of RF energy. He managed, through some complicated procedures, to replicate that signal on request. By recognizing the method by which the bits were encoded onto the waveform, he figured out how to turn a randomly read card with the same specs into a cloned card.



9 - http://cryolite.ath.cx/perl/skin/prox - The setup used

The author essentially defeated a trusted prox card system. He could, for instance, have been a terrorist wanting to gain access to a building protected by prox card access. If he knew where workers got lunch, he could stand next to one of them at the check out counter and silently copy someone's card while it remained in that person's wallet. He could then transfer those bits to his clone card and replicate the signal, thus gaining entry into the "secure" building.

By using some signal processing tricks, he could read the card's data significantly farther away because the cards simply repeated the same bits over and over until removed from the field surrounding a reader. It wouldn't be difficult, he reasoned, to attach a malicious reader device on the opposite side of a wall from a bank of "nice" readers and simply gather data from cards by listening carefully and using some signals tricks.[80]

Lukas Grunwald, a consultant in the security and e-commerce field, developed a program called RFDump which allows users to edit an RFID tag's contents.[81] The program could be added to a handheld computer and be used by people who want to alter or correct information on RFID cards in their possession. Unfortunately, programs like this could also be used to steal expensive items in a

[80] http://cryolite.ath.cx/perl/skin/prox
[81] http://www.rfidgazette.org/2004/07/lukas_grunwalds.html

store by relabeling them as other, less expensive, items. Attention paid to programs like RFDump and people like the RFID hacker above has foisted encryption in RFID systems to the spotlight.[82] If RFID tags are not secure when used for secure exchanges, they pose a major threat.

A.4.1 128 bit vs. 3DES vs. scrambling letters

Not all forms of encryption are created equal. If I wanted to send you an "encrypted message," I would have a wide selection of options available to me. I could convert the text into binary and add some predetermined number to each digit, I could add different numbers to each digit, I could reverse the order of the numbers than multiply each by 13786 and then subtract two… you get the idea. It should be obvious that if I simply add one to each number, it would be trivial to crack my cyphertext (encrypted message) – especially if the code cracker has a computer which can perform over one million operations per second. It would be much more difficult to crack my cypertext if I were to take a phrase, passage or encyclopedia, convert it to one's and zeros than add it to my message and truncate what doesn't overlap. We would simply need to exchange what passage or set of numbers I used to encrypt the message so you could decrypt it.

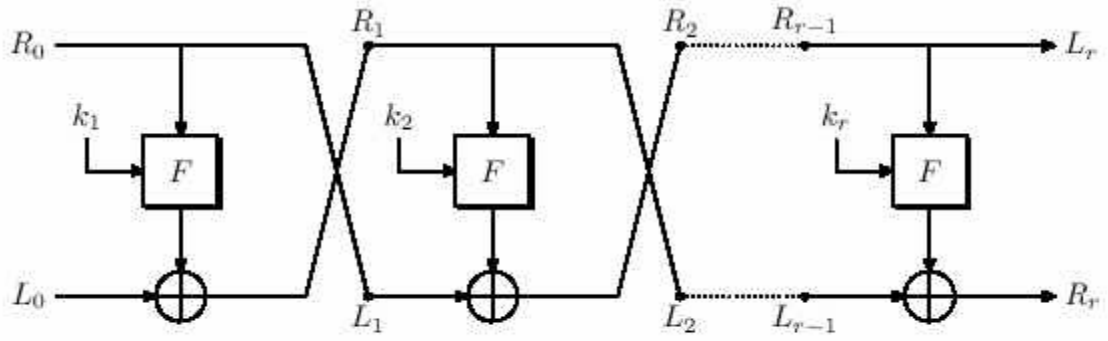


Figure 2.1: *Feistel Cipher.*

10 - http://kingkong.me.berkeley.edu - The DES algorithm

The important point here is that some encryption is "better" than others. Some encryption takes a few *minutes* to crack, other forms take *centuries* (using the current computers we have and operate). Typically older algorithms are less secure and newer algorithms with larger key sizes are more secure, as they implement new discoveries of applications in mathematics. At the end of the day, however, some weak encryption is arguably a tad better than no encryption at all.

[82] http://blog.informationweek.com/001260.html

A.4.2 What manufactures want you to believe

In the past, there was no encryption. Cards would send bits, readers would read bits. Currently, however, there is a push to get more encryption on RFID cards. Microsoft, in a document about RFID privacy, stated encryption as key to prevent security liabilities.[83] MIFARE, the standard which the MBTA will implement on its RFID Charlie Cards utilizes 3DES.[84] "Triple DES" is an algorithm which uses an NSA encryption technique called "Data Encryption Standard" three times on the same data to arrive at a "secure" cyphertext.[85]

DES, the father of 3DES was not secure. In 1998, the Electronic Frontier Foundation cracked DES in 56 hours using a supercomputer. Now, DES could be cracked in less than an hour.[86]

3DES isn't currently considered easily crackable. Reports say it would take centuries to crack.[87] Seeing that T users don't stand in the same place for more than 15 minutes, some say encryption is fine as it is.

A.4.3 What Encryption experts want you to know

Since the dawn of time, there have been secrets and there have been people wanting to know those secrets. Encryption techniques like the Caesar shift (shifting a letter or two up or down) were secure until people learned to crack them.[88] The Enigma, the German WWII encryption device, was considered uncrackable – now there are websites with applets that let you write and crack your own Enigma codes.[89] Encryption experts caution society not to settle, because given a few years, almost all codes are broken.[90]

Another consideration in the encryption debate is *when* the encryption takes place. If Eve is a spy trying to gain entry into a secret cult and she knows there is a password, she might try listening to what people speak when they approach the sentry. If the organization implements a form of encryption on their password and then tells their members the encrypted password, Eve will still be able to gain entrée.

---

[83] http://www.eicar.org/rfid/infomaterial/RFID_privacy1_1.pdf
[84] http://www.siki.com/ips/english/product/MIFARE%20Catalog%2030010.pdf
[85] http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html
[86] http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html
[87] http://www.processor.com/articles/P2608/24p08/24p08chart.pdf?guid=
[88] http://www.simonsingh.net/The_Black_Chamber/caesar.html
[89] http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/
[90] http://www.networkcomputing.com/1006/1006colmoskowitz.html

An illustration of this issue would probably clear some confusion. Imagine Eve listening in on the conversations at the door. The members of the organization say their name followed by "Dogfood" when they approach and are allowed in. To stop Eve from understanding this mechanism, the members speak their name backwards and say an "encrypted" version of "Dogfood." This, the organization believes, will thwart potential spies.

Eve stands at the door, listening intently. She hears "nairb…Foobarg," the next person approaches and she hears "ekim… Foobarg." She might have no idea what the members are saying nor understand that "ekim" is Mike backwards, but she can easily approach the door and say "Ekim…Foobarg" and (albeit with blonde hair and a feminine shape) appear to be a valid member, as she has stated a members name backwards and said the encrypted password.

RFID experts at the MIT AutoID center (an organization which studies and sets standards for RFID technologies) have expressed concerns about the crypto capabilities on board RFID smart cards[91]. While industry claims to have on-board crypto and PKI (public key infrastructure)[92], it seems unlikely that a small, low-power, inexpensive chipset can perform all these functions.

Steve Weiss, a grad student at the RFID center, writes about the issue far more elegantly in his Masters' thesis than I shall, but I'll attempt to express the main idea of his arguments. His paper can be found on the Auto ID center website and on crypto.csail.mit.edu. Essentially, Steve states that chipsets on RFID cards contain about 2000 gates (devices able to perform a binary computation) which are dedicated to security. Hardware implementations of DES, Steve writes, take upwards of 10 – 15 times as many gates. If the chips lack the computational power and storage space, there is no way the cards can perform active, worthwhile encryption.[93]

Philips, the maker of the ISO14443 standard MIFARE card, which the MBTA will use for its Charlie Card, claims to have implemented many of these security features.[94] They claim that MIFARE contains 1KB of EEPROM (memory) and performs active crypto on its fixed 32 bit unique serial number or transmitted data. It is still unfathomable for some to imagine that such complex calculations can be performed on a passive card, but regardless, companies are aware of issues in cryptography and are almost surely working to make their technology secure.

[91] E-mail interaction with Auto ID ctr grad student Joe Foley
[92] http://www.rfida.com/weblog/2004/06/rfid-smart-cards-oberthur-wins-first.htm
[93] http://crypto.csail.mit.edu/~sweis/masters.pdf
[94] http://www.siki.com/ips/english/product/MIFARE%20Catalog%2030010.pdf

A.4.4 What should we demand in the future (technically)

Consumers and businesses deserver protection from intruders. An RFID infrastructure which provides ample security will have an encryption system that does more than send the same encrypted data every time it is read. There is a case for active cards, in that they typically can perform many more calculations than passive cards since they have more power available to them, however, it is impractical to think that the MBTA will pay several dollars for each card when passive cards are less than a buck and consumers are generally naïve to the differences.

Consumers and businesses need a system where cards cannot be cloned. A "very improbable" chance of cloning is not acceptable. Unless there is a zero percent chance than someone will succeed at cloning another users' card, there will be hackers (MIT students, perhaps) who might accept the challenge and succeed. While MIT students would be trustworthy with this technology, if it were to fall into the wrong hands, the MBTA and consumers could be out quite a bit of money. If a company claims that their smart cards do 3DES encryption, consumers have a right to have proof which makes sense to them.

We have spoken a bit about encryption for cards, but the databases must also have encrypted connections. It is dumb if a criminal can install a tap on the line running from the card reader to the server and get all the data he wants, despite the actual comms line between the card and reader being encrypted.

Cards also should not emit an identifiable signal when interrogated by a non-MBTA reader. This requires authentication, which is best accomplished in a PKI infrastructure, but Philips claims it is being implemented. We'll see.

Appendix B - A Possible Design

This appendix describes a possible data storage design to meet the following goals:

- using the benefits of RFID to shorten lines and reduce cost
- storing aggregated travel data for statistical studies
- storing personal travel data for a limited time
- allowing users to replace lost cards
- enabling the MBTA to charge fares based on distance traveled
- logging access to MBTA databases

The following design covers the data storage aspect of the MBTAs information archetecture. We assume functionality of RFID cards, readers, and networks needed to transfer needed information to the servers. We also assume that RFID cards simply store a unique identifying number which correlates to an entry in an MBTA database.

This design involves two databases. The first database contains personal information and a recent travel log. The second database contains long term travel logs, but no personal information.

Section B.1 General Design

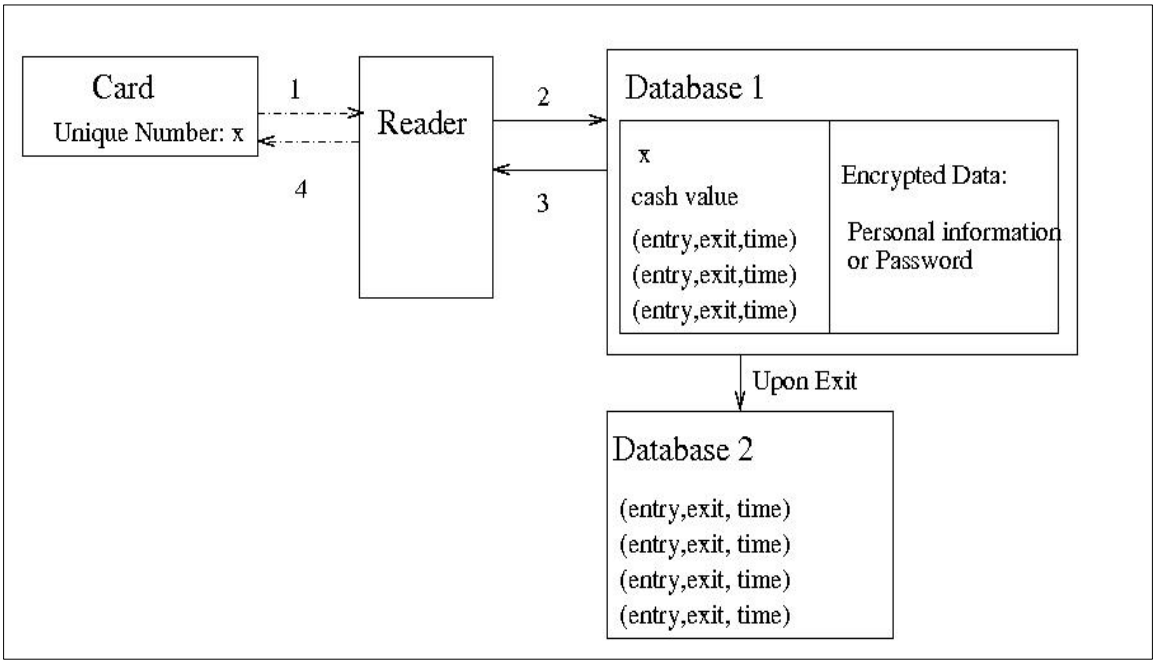


Figure B.1
Schematic of Suggested Database Design

The first database contains the following information:

- Unique ID of each issued Charlie Card
- Account balance
- Personal information or a shared secret (traveler's password)
- A travel log containing entries for each trip with
    - Boarding location and time
    - Disembarking location and time
- A boolean flag field that is turned switched when a card is reported as stolen

The second database contains the following data:

- A user's travel history spanning a set period of time. As above, these would contain:
    - Boarding location and time
    - Disembarking location and time

Note that the second database stores no personal information nor correlates with any personal information that could be used to link the travel data in the second database to personal identifying information in the first. Furthermore, users have the option of storing personal information or storing a password (unique, yet enables one-way verification). The advantages and disadvantages of these two options are explained in sections 3 and 4, variations on the general design.

Section B.1.1 Operation of the Databases

Daily T use data is automatically entered into the first database. When a customer enters a station and swipes his or her card, a record is created with this person's unique ID. The reader logs this ID number in the first database, along with time and location of entry. Using the first database, the system verifies the validity of this card and ensures proper fare balance. The result of verification (accept or reject) is sent to the turnstile (an accept may have the result of opening a gate, or allowing the turnstile to rotate). Upon successful entry, the location and time is correlated with the user ID and logged in the first database.

When the customer leaves from the concluding station, the RFID card is used to swipe out. The card reader sends the unique ID to the first database, along with a time and location of exit. The first database records this data in the travel log. The fare that the customer owes is calculated and subtracted from the amount of money in their account. (If the fare is based on distance traveled, the cost would be variable. If the account does not have adequate funds, the gate can display a

message suggesting the user add funding to his or her card at a kiosk located in the station or take any other action deemed appropriate.)

After a specified time period, perhaps one or two weeks, travel data will be copied to the second database without the corresponding personally identifying fields. This would ensure that the second database contains adequate aggregate travel information yet is stripped of all personal information. All personal data older than this time period will be deleted, ensuring that personal data is not linked to travel data yet statistics about travel are still maintained.

Section B.1.2 Meeting the Specifications

This database meets the requirements specified above:

- using the benefits of RFID to shorten lines and reduce cost
- storing aggregated travel data for statistical studies
- storing personal travel data for a limited time
- allowing users to replace lost cards
- enabling the MBTA to charge fares based on distance traveled
- logging access to MBTA databases

RFID can be used to meet the six requirements above without compromising the promise of the new technology.

An advantage to this proposed architecture is that people who need statistical information on travel can be given access to the second database without incurring the risk of compromising any sensitive information (i.e. the personal information or passwords in the first database). Because older travel information is removed from the personal data and stored without any information to connect it to personal data, this architecture meets the goal of storing personal travel data for a limited period of time.

To replace lost cards, a customer would provide his or her personal information or password and card ID (depending on the variant of the system). The user would be reissued a card with a new ID number, which has the same account balance and travel data as the old card. The first database would be updated so that a new entry is created for the new ID number, with the old travel data, account balance and password or personal data. The first database would also be updated so that the old ID number (associated with the stolen card) would have a zero balance or some flag which would make it useless to the thief.

As described above, fare can be calculated based on entry and exit locations, should the system require it.

This design does not prohibit the server from recording whenever an employee logs on and what data he or she accessed. We did not explicitly include these design elements in the proposal above because they would needlessly complicate the discussion. The interface which allows employees to access data could be a query which would verify the employee permissions, and record the time, data access, and purpose.

Section B.2 Variation 1: Shared Secret (Password)

In this variation, the first database stores only a shared secret like a password and user ID related to the customer. The database contains no personal information. This variation has the advantage that all cards are anonymous. Because the system stores no personal data, there is no risk of abuse of personal information.

We still recommend that travel data be periodically transferred from the first database to the second, because an individual could still be tracked if their ID number was known. However, this risk is greatly reduced.

The disadvantage of this variation is that users must remember a password and identification number in order for lost cards to be reissued. This variation also lacks some of the advantages of the one presented below.

Section B.3 Variation 2: Personal Information

In the second variation, the first database stores some personal information about the user, such as name, contact information, credit card number, credit card company, and credit card verification information. (If the customer is paying via cash or check rather than credit card, the credit card related data would be left blank).

As in the recommendations given above, this information should be kept reasonably minimal. No piece of information in the database should be stored unless is directly leads to additional functionality for the customer. For instance, the customer's religion, sexual orientation, and favorite color are not directly needed for any declared functionality. However, name, contact information, and

credit card information can be used in the reissuing of lost cards, and automatic reloading.

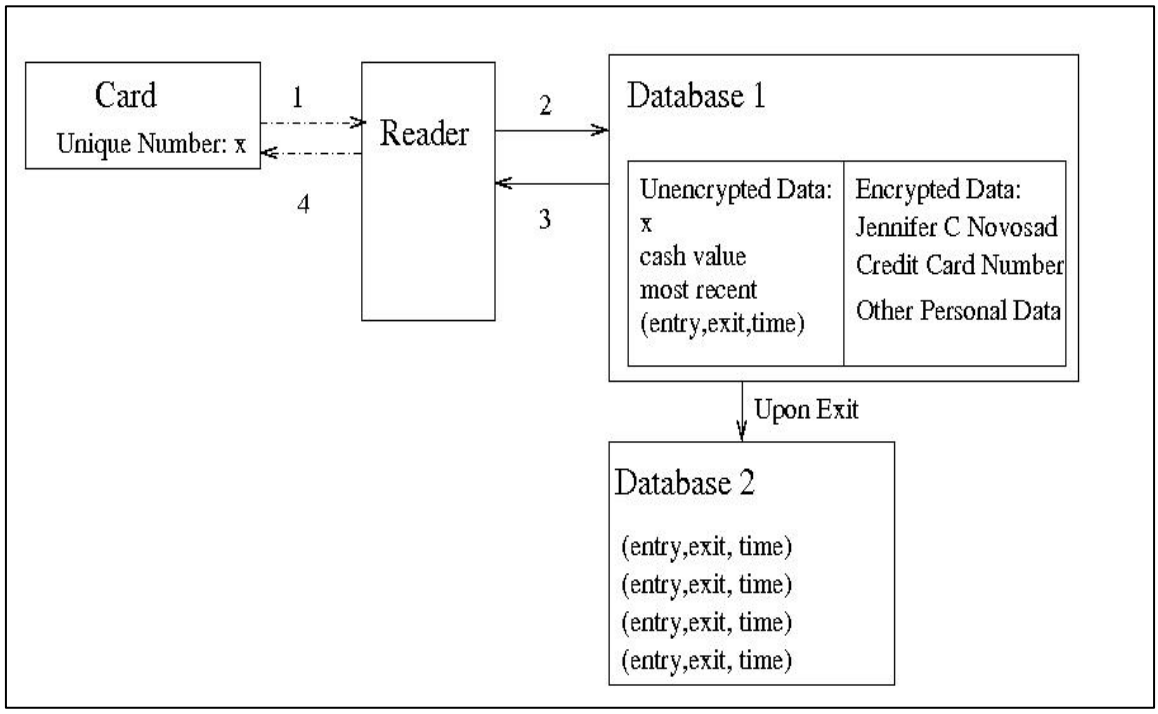


Figure B.2
Schematic for Variation 2 of the Design

Additionally, the RFID card should still only store a single number. If the card is read illegally by an unauthorized card reader, the information of a card ID number would be less useful than any personal information.

The advantages of this system are that it

- allows for an opt-in automatic reloading program
- allows for card reissuing without forcing the customers to memorize passwords (the customer would provide his/her name, and a photo ID, for instance)

However, it has the disadvantages that

- If the card has automatic reloading and is lost/stolen, the customer must report it quickly, or risk paying for someone else's T fare for an arbitrary amount of trips
- There is personal data in the system which could be subject to internal or external abuse

To help make the personal data less at risk for internal abuse, personal data could remain encrypted on the system until needed (to reissue a lost card or perform automatic reloading).

Section B.4 A Combination

To combine the useful customer service benefits of storing personal data with the privacy provided by not storing personal data, a combination of these two variations would be ideal. Users could provide as much personal information as they desired, and leave the other data fields blank.

In this method, each user has control over the balance they choose between privacy and functionality. For instance, if the credit card information is not provided, the customer would give up the ability to use automatic reloading. If no personal information is given, the customer would give up the ability to get a lost card reissued. However, in giving up these benefits, the customer would gain the level of privacy protection that he/she felt necessary.

For the system to handle this variation, a special symbol (false, for example) could be used to represent blank fields. In order for automatic reloading to occur, there could not be a blank for any certain fields. Whenever automatic reloading might be used, the system would first check the validity of all the necessary fields.

The disadvantage of this design is in explaining to customers what information they must provide in order to get certain benefits. Customers are at risk of becoming confused if instructions are not clear. However, this system has a big advantage of combining the benefits of the other two variations with customer choice.

Appendix C - Modifying a Current System to Incorporate our Recommendations

In this section, we detail how a current implementation can be extended to incorporate our recommendations. We proceed by explaining how to configure the database to separate travel information and personal information at regular intervals.

We treat the current database as a black box. The database needs three requirements: data must be able to enter, data must be able to leave, travel data must have a time stamp, and data must be able to be deleted.

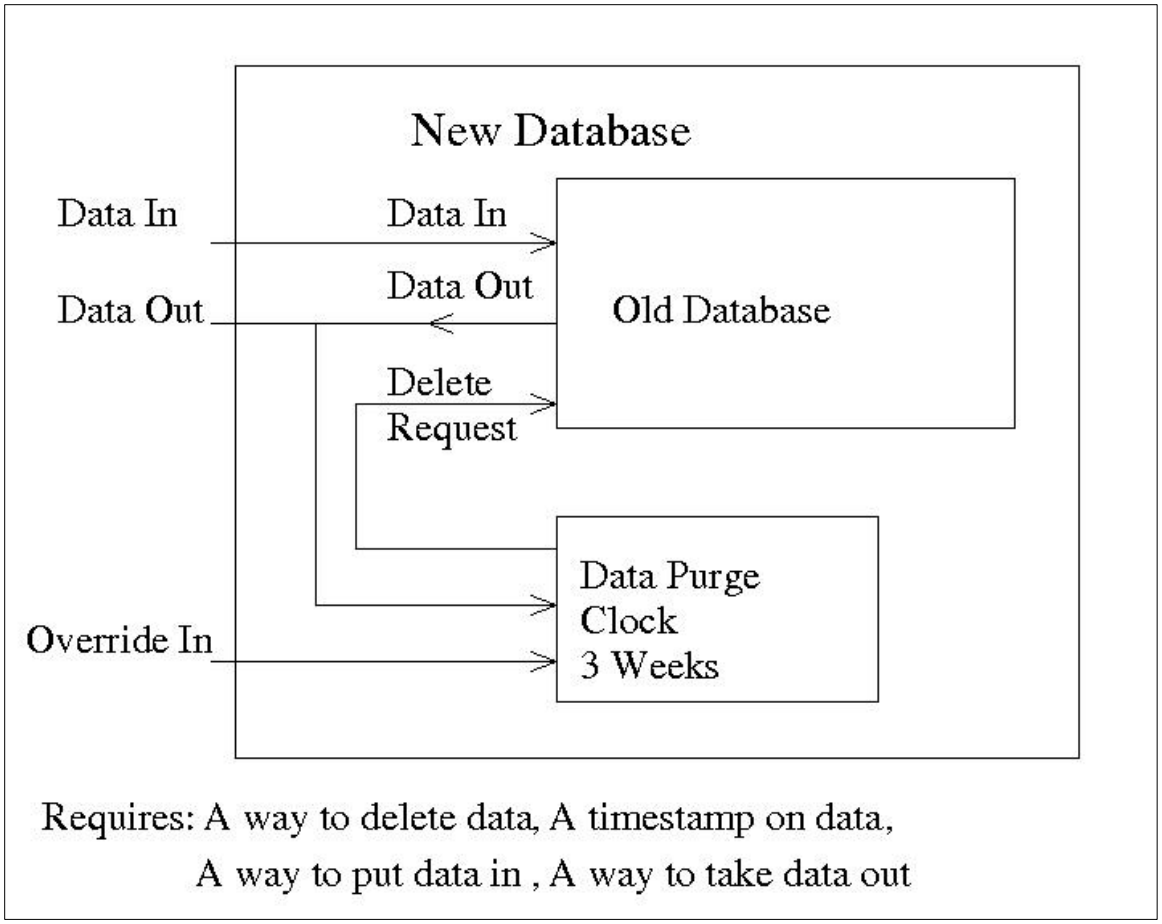


Figure B.3
A schematic of how an envelope design can be used to extend a current implementation to separate travel data from user data at regular intervals.

As in figure B.3, the new design would have three connections to the outside. The first would be a method of putting data into the system in the same manner as the original database. The second would be a method of extracting data from

the system. This method would also be exactly the same as the old method. Preserving these interfaces would help ease integration of this new database to the rest of the system by following the same design specifications for input/output as the old system.

The new system would have an internal clock programmed to separate personal information from travel data after some amount of time (say, two weeks). We will refer to this component as a Data Purge Clock. Every two weeks, the Data Purge Clock receives all of the information from the database. It scans the information for places where personal information is connected to old travel information. In these cases, it copies the old travel information into one entry of the old database (an aggregated entry of some kind). It then deletes the travel data from the entry with the personal information.

The Data Purge Clock should have an override in the event that special circumstances arise in which the separation of travel data from personal data should not occur for a particular customer. E.g. if this customer is currently on trial, and the information in the database is considered evidence, the users name should be entered into the override.

The Data Purge Clock will be computationally expensive. To minimize the effects of this cost, the Data Purge Clock might be designed to check a portion of the alphabet each night, or only run at a set time in evening when the T system is not running. By operating on smaller chunks of the information more often, and operating when little other activity is going on, the computational expense will not be a drain on other components of the system.

Appendix D - RFID and Transit Smartcard Glossary[95]

Active Tag – Any RFID tag which contains a power source, namely a battery.

Antenna – A conductive object that is designed to receive electromagnetic waves and carry them into a circuit.

Capacity - The amount of information (bits) that can be stored in a tag. Bits might be user accessible or designed to help establish and maintain a communications link between the reader and tag.

Capture Window – Balloon shaped volume in front of reader where the tag will function, given it is designed to work with said reader.

Electromagnetic Coupling – The act of using electromagnetic waves / radiation to power or communicate with another device.

Electrostatic Coupling – The act of inducing a voltage on a plate or strip of conductor to power a device.

Encryption – Obfuscating a set of data using a reversible algorithm.

Error – An operation or set of data which occurs due failure in a part of the system.

Error Rate - # errors / # transactions.

Factory Programmed Tag – A tag that has data imprinted onto it as part of the manufacturing process and cannot, typically, be rewritten.

Field Programming – The act of programming a tag after the manufacturing process -typically performed by an end user for the purpose of encoding relevant data onto the tag. Tags usually have factory programmed data, like a serial number, written onto them, but can also have user-written data which can be rewritten.

Frequency – The rate at which a signal follows the smallest segment of the signal which, when repeated indefinitely, is exactly the same as the original signal.

[95] Portions of Glossary adapted from <http://www.aimglobal.org/technologies/rfid/resources/papers/rfid_glossary_of_terms.htm>.

Inductive Coupling – The process of using a current induced in a coil to power a device.

Interrogator - See Reader

Misread- The condition where data read differs from data on the tag.

Modulation – The act of "wrapping" a signal onto a frequency using various techniques such that many signals can be sent without interfering with one another by using different frequencies.

Registered Card – An RFID smartcard that is registered with a transit authority. The transit authority can associate the card with the individual who registers it.

Opt-Out – A provision that gives smartcard users the opportunity to choose between an unregistered and registered card. A good opt-out provision does not force an individual to use a lower-quality product, such as a Magnetic Stripe Card as opposed to an RFID Smartcard.

Passive Tags – An RFID tag which does not contain a power source but rather obtains its power from the reader.

RFID – Radio Frequency Identification. The collection of tags, readers and middleware which together comprise a wireless system that uses stored, semi-unique data to accomplish tasks such as performing rapid inventory, automating fare collection on transit systems and speeding retail purchases.

Range - The distance at which successful reading / writing can happen.

Read – The interception, decoding, extraction, and interpretation of data sent from one device to another.

Read Only - See Factory Programmed Tag

Reader – A device which is connected to a central database and communicates with an RFID tag.

Separation - Operational distance between two tags.

Smartcard – A card that contains an embedded RFID chip and can be used for practical purposes, such as redeeming a transit fare.

Tag – The device which stores data and communicates with readers. Typically, a tag is in the form of a credit card shaped device, a small box, or a flat label. Transponder is the most accurate term for a tag, however 'tag' is used more prevalently and refers almost specifically to an RFID tag when speaking about electronics.

Unregistered Card – A card that is not registered with a transit authority. It cannot be associated with a particular person.

Reference List

Interviews

Barrios, Jared. Interview with Brian Myhre, Jennifer Novosad, and Chris Suarez. 5 Oct. 2004. The Massachusetts State Capital.

Berrang, Steven and Josh Martiesian. Interview with Brian Myhre and Chris Suarez, 15 Nov. 2004. Massachusetts Bay Transit Authority.

Caplan, Leslie. Interview with Chris Suarez. 8 Dec. 2004. Chicago Transit Authority.

Jimenez, Dalie. Interview with Brian Myhre and Chris Suarez, 6 Dec. 2004. The Office of Massachusetts State Senator Jared Barrios.

Jimenez, Dalie. Interview with Ian Brelinsky, Anita Chan, Brian Myhre, Jennifer Novosad, and Chris Suarez, 22 Sep. 2004. The Office of Massachusetts State Senator Jared Barrios.

Komola, Thomas. Interview with Brian Myhre, 25 Oct. 2004. MIT Police Department.

Michaud, Dan. Interview with Jennifer Novosad. 27 Oct. 2004. MIT Card Office.

Saccoia, Pat. Interview with Chris Suarez. 18 Oct. 2004. Washington Metropolitan Area Transit Authority.

Simonowicz, Mary. Interview with Chris Suarez. 7 Dec. 2004. CTA Transit Store.

Sledge, Marvin. Interview with Chris Suarez. 6 Dec. 2004. CTA Customer Service.

Print and Electronic Resources

"1998 Data Protection Act." United Kingdom. <http://www.hmso.gov.uk/acts/acts1998/19980029.htm>.

"Activists sue to stop random MBTA bag searches." Associated Press. 27 July 2004. 11 Nov. 2004. <http://www.boston.com/news/politics/conventions/articles/2004/07/27/activists_sue_to_stop_random_mbta_bag_searches/>.

"AVI – Passive vs. Active Tags." <http://www.awid.com/new/Sub-Page/DougCram-Active-vs-passive.pdf>.

Bean, Brandon, Robert Dudley, and Hideaki Tomikawa. "Business Case Study: Auto-ID Fare Collection at the MBTA." 1 Feb. 2003. MIT Auto-ID Center. 10 Dec. 2004. < http://www.autoidcenter.cn/solution/download/Auto-ID%20Fare%20Collection%20at%20the%20MBTA.pdf>.

Brenner, Kimberley. "Atlanta's Transit Authority, MARTA, is taking the Georgia City Contactless." *RFIDNews*. February 1, 2003.

"Brief of Amicus Curiae from The Center for Constitutional Rights and Privacy Activism in Support of Appellant, John Gilmore." *Gilmore v. Ashcroft*. Filed August 19, 2004. <http://209.123.170.170/gilmore/_dl/CCR&PA%20Amicus%20Brief.pdf>.

"Central Puget Sound Fare Coordination Project." <http://transit.metrokc.gov/prog/smartcard/smartcard.html>.

"Chapter 66A Section 1, Definitions." Massachusetts State Code. <http://www.mass.gov/legis/laws/mgl/66a-1.htm>.

"Chapter 66A Section 2, *Fair Information Practices*." Massachusetts State Code. <http://www.mass.gov/legis/laws/mgl/66a-2.htm>.

"Chicago Card FAQs Page." <http://chicago-card.com/ccplus/faq.aspx>.

"Chicago Card Privacy Statement." <https://www.chicago-card.com/cc/privacy.aspx>.

"Chicago Transit Authority Privacy Policy Statement." Online posting. 15 Dec. 2004. Chicago Transit Authority. 11 Nov. 2004. <http://www.transitchicago.com/help/privacy.html>.

"Customer Bill of Rights." Massachusetts Bay Transit Authority. <http://www.mbta.com/contact_us/customerbill.asp >.

Davis, Jonathan. "Balancing Debt & Pay-As-You-Go Financing." 10 Oct. 2002. MBTA. 10 Dec. 2004. <http://gulliver.trb.org/conferences/Fin3/Track2_Davis_10-28-02.pdf>

Davis, Jonathan R. MBTA Privacy Action Plan to Senator Barrios, October 13, 2004.

"Definition of an RFID System."
<http://www.webopedia.com/TERM/R/RFID.html>.

"DoD implements RFID." http://dc.internet.com/news/article.php/3098561

"Electric toothbrush charger." Self-Service Science Forum.
<http://www2.abc.net.au/science/k2/stn/posts/topic179735.shtm>.

"English Guide to Oyster."
<http://www.oystercard.com/files/lan/English.pdf>.

"EPIC" - http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf

"EZ Pass Website." http://www.ezpass.com/static/info/index.shtml

"Fair Information Practices, Chapter 66A, Section 2." Massachusetts State Law.
<http://www.dmr.state.ma.us/Chapter_66a_Section2.html>.

"Faraday cage." Wikipedia. <http://en.wikipedia.org/wiki/Faraday_cage>.

Farber, David. "[IP] [E-PRV] [RFID] Dave Emory examines EZ Pass transponders." 9 Jul. 2004. eList eXpress LLC. 11 Nov. 2004.
<http://www.interesting-people.org/archives/interesting-people/200407/msg00086.html>.

Flint, Anthony and Mac Daniel. "'Charlie' to begin new ride with modern fare system." The Boston Globe. 9 Nov. 2004. 11 Nov. 2004
<http://www.boston.com/news/local/articles/2004/11/09/charlie_to_begin_new_ride_with_modern_fare_system?mode=PF>.

Gilles Deleuze, "Postscript on the Societies of Control", from _OCTOBER_ 59, Winter 1992, MIT Press, Cambridge, MA, pp. 3-7. Available HTTP:
<http://www.n5m.org/n5m2/media/texts/deleuze.htm>.

Heigham, James C. and Leonard H. Freiman. "Tapping Officials' Secrets: Massachusetts." 2001. The Reporters Committee for Freedom of the Press. 11 Nov. 2004. <http://www.rcfp.org/cgi-local/tapping/index.cgi?key=MA>.

Heigham, James C. and Leonard H. Freiman. "Tapping Officials' Secrets: New York." 2001. The Reporters Committee for Freedom of the Press. 11 Nov. 2004. <http://www.rcfp.org/cgi-local/tapping/index.cgi?key=NY>.

Joshua. "RFID Secutiry Woes." 30 Jul. 2004. Geek News. 11 Nov. 2004. <http://www.geek.com/news/geeknews/2004Jul/gee20040730026261.htm>.

Kanellos, Michael. "Under-the-skin ID chips move towards Hospitals." 27 Jul. 2004. 11 Nov. 2004. <http://news.com.com/Under-the-skin+ID+chips+move+toward+U.S.+hospitals/2100-7337_3-5285815.html?t4ag=st.rn>.

Kent, Stephen T. and Lynette I. Millett "IDs -- Not That Easy: Questions About Nationwide Identity Systems." Committee on Authentication Technologies and Their Privacy Implications, National Research Council. 11 Apr. 2002. 11 Nov. 2004. <http://www7.nationalacademies.org/cstb/pub_nationwideidentity.html>.

Laurant, Cedric and Kenneth Farrall. "RFID Workshop Comment P049106." Electronic Privacy Information Center. 21 June 2004. 11 Nov. 2004. <http://www.epic.org/privacy/rfid/ftc-comts-070904.pdf>.

Lemos, Robert. "RFID tags become hacker target." 20 Jul. 2004. CNET News. 11 Nov. 2004. <http://news.com.com/RFID+tags+become+hacker+target/2100-1029_3-5287912.html>.

"MBTA Police – Safety/Crime Prevention." Massachusetts Bay Transit Authority. 11 Nov. 2004. <http://www.mbtapolice.com/prevention/index.html>.

McBride, Gregory B. Letter to Letter to Michael Mulhern. 12 Aug. 2002. 11 Nov. 2004. <http://www.fta.dot.gov/library/legal/buyamer/inltrs/cubic81202.html>.

McIntyre v. Ohio Elections Commission. 514 U.S. 334.

"Metro Privacy and Data Use Policy, Washinton D.C." <http://www.wmata.com/about/datause.cfm>.

"Metro privacy and data use policy." Online posting. Washington Metropolitan Area Transit Authority. 11 Nov. 2004. <http://www.wmata.com/about/datause.cfm>.

"Metro Short-Range Transportation Plan."
<http://www.mta.net/projects_plans/shortrange/SRTP.htm>.

"MIFARE - contactless Smart Card Ics."
<http://www.semiconductors.philips.com/markets/identification/products/mifare/>.

"Minneapolis Metro Transit Ride to Rewards Program."
<http://www.metrotransit.org/riderPrograms/rideToRewards.asp>.

O'Connor, Mary Catherine. "Transit Moves Ahead with RFID." *RFID Journal*. Oct. 27, 2004.

"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." 2001. Organization for Economic Co-Operation and Development. 11 Nov. 2004. <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

"Organization for Economic Cooperation and Development Guidelines." Organization for Economic Cooperation and Development. 1980. <http://www.oecd.org/home/>.

"Oyster card wins public nominated award."
<http://www.oystercard.com/files/press/Oyster_wins_award_July_04_FINAL.doc>.

"Oystercard – Explanation of Pre Pay Tickets."
<http://www.oystercard.com/buy_1_4.php>.

"Passive Tags Track Cars."
<http://www.rfidjournal.com/article/articleview/1078/1/1/>.

"Personal Privacy in an Information Society." Electronic Privacy Information Center. 1977. <http://www.epic.org/privacy/ppsc1977report/>.

"Privacy and Secure Identification Systems White Paper." Feb. 2003. Smart Card Alliance. 11 Nov. 2004.
<http://www.smartcardalliance.org/alliance_activities/privacy_report.cfm>.

"Privacy Policy." MIT Card Office. 11 Nov. 2004.
<http://web.mit.edu/mitcard/privacy.html>.

"Radio Frequency Identification Usage." Wal-Mart. <http://www.walmartstores.com>.

"Radio Frequency Identification." <http://www.connect802.com/rfid_facts.htm>.

"RFID Basics" http://www.savi.com/rfid.shtml

"RFID Privacy Workshop @ MIT. 15 Nov. 2003. Massachusetts Institute of Technology. 11 Nov. 2004. <http://www.rfidprivacy.org/2003/agenda.php>.

"RFID Special Report." *ZDNet UK*. <http://insight.zdnet.co.uk/specials/rfid/0,39026568,39153971,00.htm>.

"Romney Sings the Praises of MBTA's New Automated Fare Collection System." MBTA News/Events. 8 Nov. 2004. 11 Nov. 2004. <http://www.mbta.com/insidethet/press_releases_details.asp?ID=1072>.

Scheidt & Bachmann GmbH. 11 Nov. 2004. <http://www.scheidt-bachmann.de/index-e.html>.

"Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii." Electronic Privacy Information Center. 1973. <http://www.epic.org/privacy/hew1973report/>.

"Shrouds of Time: The history of RFID." 1 Oct. 2001. The Association for Automatic Identification and Data Capture Technologies. 11 Nov. 2004. <http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf>.

"Smart Card Talk: Smart Cards and U.S. Transit Agencies." Sept. 2003. Smart Card Alliance. 11 Nov. 2004. <http://www.smartcardalliance.org/newsletter/september_04/feature_0904.html>.

"SmarTrip Overview." <http://www.wmata.com/riding/smartrip.cfm>.

Solove, Daniel J. "Digital Dossiers and the Dissipation of Fourth Amendment Privacy." Southern California Law Review, Vol. 75, July 2002. <http://ssrn.com/abstract=313301>.

Surden, Harry. "Unbundling the Privacy Debate: RFID, Privacy and Emerging Technologies." Stanford University. 11 Nov. 2004. <http://www.stanford.edu/~hsurden/RFID_Privacy_Law.htm>.

"The Chronicle of the Boston Transit System." 2003. Massachusetts Bay Transit Authority. 11 Nov. 2004. <http://www.mbta.com/insidethet/taag_history.asp>.

"Transport for London Privacy Policy." <http://www.londontransport.co.uk/tfl/privacy.shtml>.

"Transport for London Ticketing data Protection Statement." <http://www.londontransport.co.uk/tfl/nftt_dataprotection.shtml>.

"Types of RFID." RFID Handbook. <http://www.rfid-handbook.de/rfid/types_of_rfid.html>.

United States of America v. Gerald Frank Kroll. 481 F.2d 884;

"Wal-Mart, DoD Forcing RFID." Wired News. <http://www.wired.com/news/business/0,1367,61059,00.html>.

Weis, Stephen A. "Cryptography and Information Security Group." CASIL MIT. 11 Nov. 2004 <http://crypto.csail.mit.edu/~sweis/>.

"Workshop Proceedings." Online posting. RFID Privacy Workshop @ MIT. 15 Nov. 2003. 11 Nov. 2004. <http://www.rfidprivacy.org/2003/agenda.php