Privacy and Data Collection in the Transportation Industry

May 1, 2014

nextcity
Introduction

The transportation industry has faced challenges regarding privacy and data collection. Privacy advocates, privacy-conscious individuals and others have challenged the need and use of collected information. The complaints range from the risk of identity theft to location tracking and the data being stored too long.

But this is just the beginning. As trends such as account-based payment, acceptance of bank-issued credit and debit cards and interoperable systems that cross multiple agencies across states or even regions grow, privacy considerations will multiply.

Cubic is very committed to respecting customer privacy, protecting private information and achieving compliance with regulations, industry standards and best practices. With its extensive support for payment processing, customer service operations, financial systems and intelligent travel technology within the transportation industry, Cubic has many responsibilities for the protection of personally identifiable information (PII). This privacy and identity-focused discussion will review people’s concerns, how Cubic safeguards the information in its systems and operations, the benefits to transit riders of providing information and how customers always have a choice in what they provide. Our goals are to both inform and help dispel worries for our clients and their customers.

To make the brief more understandable for the reader, our discussion will use transit industry examples throughout as a convention; however, the brief applies equally to all of Cubic’s many activities in the transportation and city services industry. As Cubic moves forward with its NextCity vision, many other services will be incorporated into revenue management and customer service systems including tolling, parking, car or bike rentals and others. In addition, part of the NextCity vision is to provide analytics services to help cities mine their “big data” information records to optimize the use of their resources and influence travelers’ choices. All of these applications will make use of the same privacy and information security considerations presented here.

Privacy Concerns and Complaints

In this section, we present the main concerns that some individuals and privacy advocates have expressed about data security and privacy as it relates to the transit and transportation sector. The list was developed through an analysis of reporting as well as statements from privacy advocates.

It is important to understand the doubts and questions individuals have in order to tackle these concerns and explain how those uncertainties are managed by Cubic’s uses of, and safeguards for, customer information.

Card-linking Concerns: Linking personal information to a transit card without the individual having a choice is a common concern. People, including privacy advocates, fear that by using a transit card, either the transit agency or the system provider automatically has access to a range of personal information. They worry that the information is susceptible to misuse such as identity theft or unauthorized access to personal information such as a home or work address.

Some are concerned that smartphones or applications can read the card without permission or that their data will be under surveillance due to provided information.

---

1 NextCity is Cubic’s vision of a fully integrated journey information and payments management system that enables us to optimize transportation through influence and prediction.
**Government and Privacy Concerns**: Advocates have spoken out about the government possibly monitoring people unnecessarily. There is also worry over a company supplying personal information to the government voluntarily without a warrant. Similarly, many are concerned that if the card can be subsidized through a work or school program, those institutions will be able to track or monitor their activities.

**Company Data Practices Concerns**: There is concern about whether data is weakly encrypted without following accepted standards or encrypted at all. Advocates have articulated complaints that the information is kept for too long and beyond what is necessary. Some have even expressed concern over database abuse, which could occur internally by employees or subcontractors. There is also potential for agencies or their systems providers to sell customer information to businesses for profit.

Cubic respects these concerns and wants to help people understand how the company and its employees address these issues and protect customer information and privacy in its systems and service operations.

**Tackling Concerns Regarding Information Use**
Cubic respects individuals’ privacy and data security and is well prepared to manage it with experience gleaned from collecting more than $18 billion in transit fare revenues each year in major cities around the world including San Francisco, Chicago, Washington, D.C., Los Angeles, London, Sydney and many more.

As the transit industry has evolved with the migration to smartcard technology, the importance of data security and protecting PII has increased. Many agencies provide the option for their riders to associate their account information with their registered card, which can also include payment sources. The increasing trends toward account-based systems and the advent of open payment using contactless bank-issued payment cards at gates and buses elevate the need for data security and privacy sensitivity.

Cubic’s transit agency clients provide the privacy and data security policies that must be followed because they own the client relationships and the information. Plus, they are government agencies that are publicly regulated and heavily scrutinized by the public and media.

To protect the privacy of individuals and PII such as credit card information, Cubic complies with well-defined international and local regulations and standards, as well as best practices, to ensure that the data is only used for specific purposes such as providing customer service and ensuring payment. The information assists the customer in managing their account and even provides benefits, which will be discussed later.

The information is not disclosed or reviewed unless it is disputed by an individual or if there is a warrant or legal authorization that requires disclosure. The scenario is similar to situations in which an individual uses a credit card to make a purchase at various locations; the location information exists. However, it would only be used in special circumstances.

It is also important to know that customers always have a choice with card registration programs. If they elect to participate, they must take action to opt-in and provide contact and payment information. If they decide not to, they do not provide personal or payment account information. Instead, they typically pay with anonymous fare cards, cash or prepaid accounts. This means neither Cubic nor its agency client would have access to the customer’s information.

Personal information is only gathered when an individual has chosen to opt-in. Some examples of the optionally shared information include:
Privacy and Data Collection in the Transportation Industry

- Registering information about who they are
- Linking payment accounts to fare media
- What details the company knows about them through mandatory and optional fields

When a person opts–in, the data is used intelligently, which includes giving customers easy access to information that can enhance their transit and account management experience. Card registration can ease travel and assist a person with customization options that are not available to unregistered riders, as well as discounted fares and other tailored benefits.

Some examples of available benefits for individuals who register their cards include:

- Identifying owners of lost cards
- Credit for balances on lost cards
- Receiving marketing notices and communications such as coupons and deals
- Viewing their account information and transaction history on the website
- Disputing any suspected errors in fares they are charged

The majority of individuals choose to tie their identity to their travel card because of benefits such as online checking of their statements or restoring values to lost cards.

**Advantages of Sharing Travel Information**

Many people consider the information about their public transportation trips as private.

While privacy-sensitive riders have the option to remain anonymous, there are three main ways travel information can be used to help individuals that may convince them to consent to share data about their trips:

- The agencies and operators can use the data to help plan, manage and optimize the services they provide on an overall basis
- For the individual, Cubic’s systems can offer them proactive, personalized and predictive information that helps make their journey, better, safer, quicker, easier and smoother
- If the individual so chooses, personalized offers that may be of interest can be provided based on preferences such as frequency and type

Another distinction is that Cubic has the ability to de-personalize information. When the information is de-personalized, a person is viewed as a “John Doe.” The information is present, but it is not tied to an individual.

This is the approach taken when analyzing large volumes of travel data, for example, to look at how many riders travel along certain paths, analyze peak periods or evaluate which stations are the busiest.

This is a win-win because the anonymized data lets transit authorities better manage the transit system while all individuals are completely disconnected from it. De-personalized data has no impact on the individual.

**Safeguarding Information**

Cubic uses information responsibly and wholly respects customer privacy concerns. Cubic also goes to great lengths to safeguard information about people, their payment accounts and their travel. The process is taken very seriously and the company does its best to ensure customers feel at ease sharing information and using the company’s systems.
Compliance with leading privacy and information security standards, following industry best practices and setting strong internal privacy policies all play an essential role in achieving these goals.

**PCI DSS Compliance**

As of 2013, Cubic has achieved Payment Card Industry Data Security Standard (PCI DSS) compliance for many North American programs and several others around the world. In addition, the company has achieved Payment Application Data Security Standard (PA DSS) certification for a number of products and systems, a list that continues to grow.

PCI DSS and PA DSS are administered by the PCI Security Standards Council, an open global forum for payment account security standards established by five founding global payment brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

The standards include mandatory security control requirements for payment information and systems. The requirements apply to all entities and systems that store, process and transmit cardholder data. They provide an actionable framework for developing a robust payment card data security process including prevention, detection and appropriate reaction to security incidents. Compliance with PCI DSS helps reduce risk and protect cardholder data. It also helps identify, assess and fix potential vulnerabilities.

Comprehensive technical and operational requirements are set as well. The security controls are designed to protect data everywhere it is processed, stored and transmitted. Policies governing security are also required. The variety of requirements are verified for compliance.

PCI DSS is part of Cubic’s privacy plan.

**Customer Service Operations**

In situations where Cubic employees have access to PII, the strictest security policies apply.

For example, customer service representatives are not allowed to bring any electronic devices into their work space. This prevents downloads of PII into devices or taking photos of the screen with their mobile device cameras. Employees are even restricted from bringing pen and paper to prevent information misuse.

Cubic uses PCI DSS to strengthen their customer service practices. However, the company goes above and beyond those standards. To ensure Cubic maintains best practices, Cubic’s customer-facing facilities are routinely evaluated by top-tier security services such as Pinkerton.

**Access Controls**

Access controls provide restrictions on the use of PII data. The controls limit what can be seen by employees allowing them to see only what is needed for their job. This prevents misuse of information. Access controls define who can access the information and when that information is accessed. The customer service areas operate on these terms. Additionally, the areas of customer service are restricted by key card access. These employees are also taken through background checks and proper training on how to use data.

Employees access the systems containing personal information through role-based access, which requires strong passwords and the individual user’s ID. Cubic not only trains their employees but publishes these policies

---

as well. These policies provide employees with a reference to know what to do with the data and what not to do, including password strength and how sensitive data is. The system is designed to protect customer information as well as respect customer privacy.

In addition Cubic follows industry best practices in its customer service centers worldwide to protect information from internal fraud in the same ways that banks and healthcare companies do.

**ISO 27001**

Cubic’s IT security management framework is based on ISO 27001, a globally recognized and comprehensive standard that defines the best practices in every dimension of secure product development and operations from programming practices to file management to handling keys.

ISO 27001 covers all types of organizations and specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system. It lists requirements of security controls with customization for specific organizations. Its purpose is to protect information assets and assist organizations in achieving that same goal. The privacy policies can implement even further control over users’ data. The privacy policies can address issues the standards might not cover and reduce risk as much as possible. Privacy policies can also vary by transit agency, and Cubic complies with those contractual security practices. The policies are part of an overall management program targeting security and privacy. The privacy policies also include a variety of access controls.

**Data Retention**

Cubic only uses the information for business purposes, which is why the company retains the information for the minimum time required before it is securely removed. Another part of protecting customer information is encryption of sensitive customer data, such as credit/debit card and bank account numbers. Sensitive data is encrypted using industry standard cryptographic algorithms and protocols when it is stored and when it is transmitted across a network.

**National, Regional, State and Local Laws**

The company must abide by transit agency-specific policies, plus follow laws and standards for privacy and security particular to that client’s national, regional, state and local laws.

One topic of great concern in North America is data breach notification laws. California and 45 other states now have a breach notification law. Generally, these laws require an organization to notify customers in a breach situation in which customer information is leaked, whether lost, stolen or unintentionally released to an untrusted or unknown environment or entity.

A second example is Australian law, which has specific requirements that Cubic is contractually obligated to abide by, such as the New South Wales Information Security Guidelines and Privacy Act. Another is British Columbia, which has specific laws and generally more strict controls regarding data privacy.

---

Internal Privacy Policies

Cubic strives to take processes such as PCI DSS and ISO 27001, laws and regulations, and go a step beyond that by forming sound internal privacy and security policies. The company considers all angles of concern that an individual might have.

Despite regional differences, Cubic strives to follow the same set of standards for all programs anywhere in the world. The company’s internal policies and practices draw from the best and strictest requirements from all regions and combine them, giving Cubic and its clients one of the most effective privacy and security environments available worldwide in a payment processing and customer information system.

Conclusion

Thank you for reading.

The purpose of this brief was to give you an overview of how Cubic addresses people’s concerns about the privacy and the security of their identity, travel and payment information in the many transportation industries Cubic serves.

With its global experience, Cubic draws from the best security practices and strictest requirements from all regions and combines them, giving its clients and their customers a highly secure environment.

Compliance with leading privacy and information security standards like PCI DSS, PA DSS and ISO 27001 are at the core of the company’s security framework. These standards span system development, operations and customer service.

Cubic extends these with best practices for access control and physical security measures, paying particular attention to its customer service centers where its representatives handle PII. The same procedures and policies used in the financial services and healthcare industries are employed in Cubic’s own customer-facing operations.

Transportation customers always have a choice in what information they provide, and can elect to pay cash and travel anonymously if they prefer.

Most customers do elect to share information, however, to gain the many benefits available to them when they register their transit cards or link them to payment sources. Our goals are to both inform and help build the confidence of our clients and their customers who do trust Cubic with their personal and private information.

We hope these ideas can help you start planning new possibilities for protecting and managing your own use of customer information. Where do you go from here? To start, we hope you share this brief with your colleagues. Work with your management to make sure they understand the importance of privacy and information security in the changing world of transportation revenue management and customer service systems.

When the time is right, consider contacting us. Cubic Transportation Systems has created a broad portfolio of capabilities in its NextCity platform, all of which protect client information using the techniques presented here.

We would be delighted to make specific recommendations for your situation and provide you with more detailed information about what we have to offer and how we work. Do not hesitate to contact us in whichever way suits you best. Contact information for our offices worldwide can be found at www.cts.cubic.com.