



Joseph P. Bort MetroCenter
 101 Eighth Street
 Oakland, CA 94607-4700
 TEL 510.817.5700
 TDD/TTY 510.817.5769
 FAX 510.817.7848
 E-MAIL info@mtc.ca.gov
 WEB www.mtc.ca.gov

Memorandum

TO: BATA Oversight Committee

DATE: December 1, 2010

FR: Executive Director

W. I. 1256

RE: FasTrak[®] Privacy Policy (BATA Resolution No. 96)

Assembly Bill 1175, which was approved in the 2009 legislative session, directed BATA to contract with a nationally recognized firm with expertise in privacy issues to conduct a review and analysis of the privacy issues associated with BATA's FasTrak[®] electronic toll collection system. The bill stipulates that BATA will provide a report on the assessment to the Legislature by January 31, 2011.

In February 2010, BATA contracted with PriceWaterhouseCoopers, LLP (PwC) to conduct the required analysis. The analysis considered the customer data collected as part of the FasTrak[®] program and how data is processed, stored, and secured at the FasTrak[®] Regional Customer Service Center (RCSC) and internally at BATA. Based on the analysis, PwC found that:

1. The FasTrak[®] RCSC has many expected administrative and IT systems architecture controls in place to protect customer data. PwC noted that the FasTrak[®] RCSC was deemed compliant in all areas of the Payment Card Industry (PCI) standards by a Qualified Security Assessor (QSA).
2. BATA's internal policies and procedures in regards to privacy and security of customer data for the FasTrak[®] program should be strengthened.

In response to the findings and recommendations of the analysis, staff is proposing updates to the FasTrak[®] Program Privacy Policy Customer Notice (BATA Resolution No. 96, superseding BATA Resolution No. 45) to better explain to customers how their personal data is used, stored and protected. The updates include more detail to customers on how their personal data is used and shared with third parties, how long data is retained, the measures BATA uses to protect data, and how they can update their personal information. The Privacy Policy is provided to customers on the FasTrak[®] web site and will be distributed to customers when they sign-up for the FasTrak[®] program.

Staff is also developing and documenting internal policies and procedures, pursuant to an Executive Director's Management Memorandum, to provide direction to agency staff regarding protecting customer data. The internal policies establish a governance structure to coordinate privacy related activities throughout the agency, procedures for staff's handling and retention of customer data, and guidance for the development of third party contracts to ensure that

contractors who have access to customer data protect the data from unauthorized use and disclosure. These internal policies and procedures will direct the protection of customer data for all of the operational programs (e.g. FasTrak[®], Clipper and 511) administered by BATA, MTC, and MTC SAFE.

It should be noted that at no time has BATA sold or shared customer data with any third party for the purposes of marketing or advertising services. BATA has only used or shared customer data with third party contractors or other toll agencies for the operation of the FasTrak[®] program or as required to comply with legal processes (such as a subpoena) served on BATA.

Table 1 includes a summary of the major findings of the analysis conducted by PwC and the policies and procedures that have been developed to address the findings. Attachment 1 includes a draft of the report to be submitted to the Legislature. Staff will provide an overview of this material at the Committee's December 8, 2010 meeting.

Recommendation

Staff recommends that the Committee refer BATA Resolution No. 96, - FasTrak[®] Privacy Policy, to the Authority for approval.



Steve Heminger

Table 1
FasTrak® Program Privacy Analysis - Major Findings and Responses

Analysis Finding	Response
1. There is no formal governance structure to address and enforce privacy issues within BATA.	Internal procedures are being updated to establish a structure to oversee privacy issues within the organization, including establishing a Privacy Officer within the Office of General Counsel.
2. BATA does not provide a formal training program for staff in regards to privacy issues.	BATA has begun the process of training sessions for internal staff regarding the roles, responsibilities, and guidelines detailed in the privacy and security policies.
3. Current privacy policies do not address record retention for FasTrak® customer data.	The FasTrak® Program Privacy Policy Customer Notice and internal procedures are proposed to be revised to reflect data retention requirements that meet the requirements in Senate Bill 1268, which becomes law January 1, 2011. The bill stipulates that customer information be purged within four years and six months after the date a FasTrak account is closed or terminated.
4. The process of providing FasTrak customers access to their personal information is currently unclear.	The FasTrak® Program Privacy Policy Customer Notice is proposed to be revised to clearly inform customers how to update their personal information maintained by the FasTrak® program and how to contact the BATA Privacy Officer if questions arise.
5. BATA contracts contain general confidentiality clauses stating that customer data should only be used for the stated purposes and that the contracted entities abide by all laws and regulations.	Specific language to be incorporated into third party contracts in regards to privacy is being developed and the internal procedures will instruct staff to include these provisions in contracts that may have access to customer data.
6. The FasTrak website stores cookies, but the customer privacy notice does not address the use of cookies. Also, the privacy notice does not indicate that a third party contractor operates the FasTrak® RCSC.	The FasTrak® Program Privacy Policy Customer Notice is proposed to be revised to provide details about web cookies collected on the FasTrak® website and instruct customers on how to prohibit cookies from being written to their computers. The notice is proposed to also be revised to indicate that a third party operates the RCSC under contract to BATA.
7. The agency's IT security policies are not fully defined or implemented.	IT security policies and practices are currently being updated to define security roles and responsibilities and implement improvements to secure data.