DEPARTMENT OF TRANSPORTATION

Office of the Secretary (OST)

PRIVACY IMPACT ASSESSMENT

Consumer Complaint Application Online System (CCA)

August 31, 2004

Table of Contents

Overview of OST (OST) privacy management process for CCA

The Office of the Secretary (OST), within the Department of Transportation (DOT), has been given the responsibility of formulating national transportation policy and promoting intermodal transportation. Other responsibilities include negotiation and implementation of international transportation agreements, assuring the fitness of US airlines, enforcing airline consumer protection regulations, issuing regulations to prevent alcohol and illegal drug misuse in transportation systems, improving the security of the national transportation system, and preparing transportation legislation. [1]

As part of its support function for DOT, OST (and specifically, the Office of Aviation Enforcement and Proceedings Aviation Consumer Protection Division (ACPD)), is responsible for investigating and tracking complaints against airlines. As part of this public service, ACPD assists airlines in identifying and remedying consumer concerns. Also, ACPD reports aggregate complaint statistics to Congress, the media, and the general public. To help fulfill this need, OST uses a Web-enabled system, Consumer Complaint Application Online System (CCA). CCA records, tracks, and provides reporting on consumer complaints, inquiries, opinions, and compliments against airlines.

Privacy management is an integral part of the CCA project. DOT/OST has retained the services of privacy experts to help assess its privacy management program, utilizing proven technology, methodologies, and sound policies and procedures.

The privacy management process is built upon a methodology that has been developed and implemented in leading companies around the country and globally. The methodology is designed to help ensure that DOT and OST will have the information, tools, and technology necessary to manage privacy effectively and employ the highest level of fair information practices while allowing OST to achieve its mission of protecting and enhancing all U.S. civil transportation systems. The methodology is based upon the following:

- *Establish priority, authority, and responsibility***.** Appoint a cross-functional privacy management team to ensure input from systems architecture, technology, security, legal, and other disciplines necessary to ensure that an effective privacy management program is developed.
- *Assess the current privacy environment*. This involved interviews with key individuals involved in the CCA system to ensure that all uses of Personally Identifiable Information (PII), along with the risks involved with such use, are identified and documented.
- *Organize the resources necessary for the project s goals*. Internal DOT/OST resources, along with outside experts, are involved in reviewing the technology, data uses and associated risks. They are also involved in developing the necessary redress systems and training programs.
- *Develop the policies, practices, and procedures*. The resources identified in the paragraph immediately above work to develop an effective policy or policies, practices, and procedures to ensure that fair information practices are complied with. The policies effectively protect privacy while allowing DOT/OST to achieve its mission.
- *Implement the policies, practices, and procedures*. Once the policies, practices, and procedures are developed, they must be implemented. This involves training of all individuals who will have access to and/or process personally identifiable information. It also entails working with vendors to ensure that they maintain the highest standard for privacy while providing services to the OST project.
- *Maintain policies, practices, and procedures*. Due to changes in technology, personnel, and other aspects of any program, effective privacy management requires that technology and information be available to the privacy management team to ensure that privacy policies, practices and procedures continue to reflect actual practices. Regular monitoring of compliance with privacy policies, practices, and procedures is required.
- *Manage exceptions and/or problems with the policies, practices, and procedures*. This step involves the development and implementation of an effective redress and audit system to ensure that any complaints are effectively addressed and corrections made if necessary.

Personally-Identifiable Information and CCA

The CCA system uses both Personally Identifiable Information (PII) and non-personally identifiable data to record, track, and manage complaints, information requests, compliments, and opinions pertaining to airlines. In this process, members of the public may call, write, or email ACPD with information about an airline-related service issue. Using pre-defined criteria, ACPD reviews comment information and identifies whether that comment is classified as a complaint, information request, compliment, or opinion. Then, ACPD records the information as appropriate in its database and takes action as needed. ACPD fulfills requests for information by mailing information brochures to the requestor, providing the URL for its website, or it may record and pass on to an airline information that is being requested.

Though members of the public may make anonymous opinions and compliments, all complaints must be able to be tied to an individual in order to help prevent trivial, false, or malicious complaints. For

complaints that meet these criteria, ACPD records the complaint, passes on the information to the airline in question, and it may follow up with an investigation. Also, on a monthly basis, ACPD publishes aggregate airline complaint statistics.

PII in CCA may include name, postal address, phone number, fax number, and email address. An individual may provide personal information during a phone call with the ACPD staff, or in the body of an email or letter. When ACPD investigates a complaint, it enters additional information obtained through the investigation process into the CCA system.

In addition, CCA uses logon names and passwords to control access. Therefore, CCA also contains the name and password of each ACPD user and associates the data with that individual.

An individual□s PII enters the CCA system when that person voluntarily sends that information along with a complaint, information request, opinion, or compliment to ACPD pertaining to an airline. Though an individual is not required to provide PII, ACPD only records comments as complaints in its database if it includes this information.

Alternately, an individual may send complaint and personal information to ACPD on behalf of another individual. For example, an individual may send in a complaint on behalf of his or her mother, along with his or her mother□s PII.

Why CCA collects information

CCA information is collected to assist ACPD record, track, and take appropriate action on complaints, opinions, information requests, and compliments pertaining to airlines. The CCA system includes PII to help assist in the follow-up and resolution of airline service issues.□ It is the means by which the ACPD and airlines can verify the identity of the commenter and the accuracy of the information being submitted for consideration.

How CCA uses information

Information in CCA is used by ACPD to investigate airline complaints and fulfill requests for information. During this process, ACPD may contact individuals involved in this process. ACPD refers information in CCA to the airline to which it pertains in order to help facilitate airline redress of any issues. In addition, ACPD creates and publishes monthly reports to inform the public about airline customer service issues. No PII is included in these public reports.

How CCA shares information

ACPD analysts enter, access, and use PII in CCA to categorize and record airline service issues, follow-up on appropriate actions, and report aggregate statistics. In addition, ACPD refers to airlines PII and non-PII in the CCA system as they pertain to each airline. Each month, ACPD aggregates complaint results and publishes reports that do not contain any PII. In addition, from time to time, media or advocacy organizations may request aggregate data, or in some cases, access to CCA. ACPD may allow a requestor to research CCA data after that requestor has signed a non-disclosure agreement that prevents that individual from recording or using CCA PII. Also, an individual not associated with an airline may request CCA PII to follow-up with one or more people making a comment about an airline service issue. In these few instances, ACPD will contact the commenter, ask for permission to share PII, and follow his or her direction.

CCA is also a Privacy Act system of records and complies with the information sharing practices described in the Routine Uses section of its Privacy Act system of records (SOR) notice.

How CCA provides notice and consent

Individuals submit comments about airlines voluntarily. There is also no requirement to submit PII along with comments, though anonymous comments are not categorized as complaints. Complaint forms that can be downloaded from the Web include a link to a privacy policy that describes privacy practices. In addition, OST is currently completing the process of obtaining signed affirmations that all individuals accessing CCA have read and understand a Rules of Behavior document that describes privacy expectations. Also, as a SOR, CAA provides a SOR notice in the Federal Register. DOT does not use CCA PII for any other purpose, except as allowable by law.

How CCA ensures data accuracy

CCA PII is received directly from the individual in question, or on behalf of that individual through another's assistance. Designated ACPD staff members enter data into CCA and are responsible for accurate data entry. If an ACPD staff member finds a data inaccuracy, he or she makes corrections to the data.

ACPD strives to have accurate PII in the CCA. At any time, an individual may request to verify his or her PII in the CCA system, and ACPD will make changes to correct inaccurate information. In order to avoid malicious, false, or frivolous complaints in the CCA, PII remains in the CCA system as a means for ACPD and airlines to contact the individual and determine, if necessary, the validity of the both the commenter's PII and the comment.

How CCA provides redress

At any time, an individual may contact the CCA System Owner, as designated in the SOR notice, for redress of privacy issues. In addition, the complaint forms that can be downloaded from the Web provide a link to a privacy policy. This privacy policy provides contact information for the OST Privacy Officer, who will address any privacy concerns.

How CCA secures information

The CCA system is housed in Washington, DC. Personnel with physical access have all undergone and successfully completed DOT background checks. In addition, OST is currently completing the process of obtaining signed affirmations that all individuals accessing CCA have read and understand a terms and conditions statement that describes privacy expectations.

In addition to physical access, electronic access to PII in CCA is limited according to a matrix of job function and accounting activities. Different users are provided different levels of access.

OST controls access privileges through the following roles:

- Disability Hotline contractor
- Analyst Level
- Manager Level

◦ Guest Level

The following matrix describes the privileges and safeguards around each of these roles as they pertain to PII.

ROLE	ACCESS	SAFEGUARDS
Disability Hotline Contractor	Initiate record for analyst review and □read record	The following safeguards apply: • Passwords expire after a set period. • Accounts are locked after a set period of inactivity. • Minimum length of passwords is eight characters. • Accounts are locked after a set number of incorrect attempts. (not currently enabled, due in the next system release 1st QTR, FY05)
Analyst Level	Initiate record, assign categories, follow up on investigation, add and change additional notes and data.	The following safeguards apply: • Passwords expire after a set period. • Accounts are locked after a set period of inactivity. • Minimum length of passwords is eight characters. • Accounts are locked after a set number of incorrect attempts. (not currently enabled, due in the next system release 1st QTR, FY05)
Manager Level	Read, update, and delete data. Also, assign roles and privileges in system.	The following safeguards apply: • Passwords expire after a set period.

		• Accounts are locked after a set period of inactivity. • Minimum length of passwords is eight characters. • Accounts are locked after a set number of incorrect attempts. (not currently enabled, due in the next system release 1st QTR, FY05)
Guest Level	Limited, read-only access to record.	Guest must be signed on to CCA by Analyst or Manager

Access for all CCA users must be granted by a Manager, who also sets privileges.

System of records

CCA is a Privacy Act system of records (SOR), because it can be searched by an individual□s name. DOT is currently working to meet Privacy Act requirements, including posting a SOR notice. OST has interim certification and accreditation for CCA; it is working to fully certify and accredit the system in accordance with DOT requirements.□

---

[1] http://www.dot.gov/ost/