Federal Trade Commission
Privacy Impact Assessment for the
Correspondence Management System (CMS)

January 2009

1. System Overview

The mission of the Federal Trade Commission (FTC or Commission) is to enforce the Federal Trade Commission Act by preventing the use of unfair methods of competition and unfair or deceptive acts or practices; to enforce many other consumer protection and antitrust statutes; and to enhance informed consumer choice and public understanding of the competitive process. The FTC seeks to accomplish this mission without unduly burdening legitimate business activity. In support of these activities, FTC staff engage in extensive communications with federal, state, and local government agencies, as well as with consumers and industry groups.

As required by section 208 of the E-Government Act, the FTC has prepared this Privacy Impact Assessment (PIA) for its Correspondence Management System (CMS) to explain what personally identifiable information the system maintains and how the FTC uses and safeguards that information. CMS serves as the Commission's central system for tracking Congressional and White House correspondence received by the Commission, including in particular by the Office of the Chairman, the Office of the Secretary, the Bureau of Consumer Protection, the Bureau of Competition, the Office of Congressional Relations, and the Office of the General Counsel. The system tracks all Congressional correspondence sent to the Commission, including letters received directly from Members of Congress – in which they express their own views and/or forward correspondence from their constituents – and Congressional letters sent to other federal agencies which those agencies in turn forward to the Commission for response. The system also tracks all letters from the White House to the Commission forwarding constituent correspondence.

The Office of the Secretary uses CMS to help carry out its responsibility for receiving and processing all correspondence from the White House and Members of Congress, approximately 2,500 to 3,000 letters each year. The information about members of the public collected in CMS is derived from the written correspondence received by the Commission. For each letter received by the FTC, CMS tracks: the type of inquiry; the Commission employee who is responsible for responding to the inquiry; the intended recipient of the response; and the status of the response. The FTC forwards a response to each inquiry, either to the appropriate Congressional office or – with respect to inquiries on behalf of constituents and when requested by the Member of Congress – to the constituent himself or herself. When the White House forwards constituent correspondence, the FTC responds directly to the constituent.

Until 2008, CMS was a subsystem of a larger FTC system called the Consumer Information System (CIS), which stores complaints from consumers who are victims of fraud or identity theft. CMS has been modified to operate as an independent application with no relationship to CIS. CMS was designed to collect the least amount of information necessary to fulfill its intended function. CMS utilizes a database and a set of tools provided by Oracle Corporation to manage the data, security, and business rules of the application. Using Oracle maximizes data quality, data security, and system performance. Users access CMS using a software program that runs on a user's desktop developed in Oracle Forms. Users have the ability to read or modify data only if they have been specifically granted such rights for business

purposes. Access to data in CMS is limited to authorized users who have a need for access to the data in order to carry out official business functions.[1]

The Program Manager of CMS is:

Susan Taylor
Manager of Congressional Correspondence
Office of the Secretary
United States Federal Trade Commission
(202)326-2671
staylor@ftc.gov

2 Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

CMS stores three types of information:

(1) Information provided by consumers in correspondence submitted to the White House or to a Congressional office. This includes the nature of the complaint and some or all of the following information about a consumer:

a. First Name
b. Last Name
c. Street Address
d. City
e. State
f. Zip Code
g. Country
h. Home Phone
i. Work Number
j. Fax Number
k. Email address

(2) Information about the Member of Congress or White House official who forwarded the correspondence, including the following data elements:

a. First Name
b. Last Name

[1] As discussed in Section 2.1(4) below, each incoming letter from the White House or a Member of Congress – and each outgoing response from the Commission – also is scanned into the Commission's non-public document management system.

c. Position Title
d. Office Address
e. Congressional Committee Names and Addresses

(3) In limited circumstances, some additional personally identifiable information (PII) may be stored in CMS if that information is required to draft an appropriate response to the inquiry at issue.

Each incoming letter from the White House or a Member of Congress – and each outgoing response from the Commission – also is scanned into the Commission's internal document management system. As a consequence, other PII – such as Social Security numbers, birth dates and bank account numbers – may be maintained by the Commission if that data is included in the correspondence received by the Commission.[2] However, such information is not separately entered into or stored in CMS.

2.2 What are the sources of the information in the system?

The information stored in CMS is collected from correspondence received from the White House or Congressional Offices. The information in a given letter may derive either from the consumer on whose behalf the letter is written or from the Congressional Office involved.

2.3 Why is the information being collected, used, disseminated, or maintained?

As noted above, Congress has empowered and directed the Commission to prohibit the use of deceptive acts or practices; unfair acts or practices; and unfair methods of competition, in or affecting commerce – pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41-58, *as amended* – and to prevent mergers, acquisitions, price discrimination, and certain other practices that may "substantially lessen competition" or "tend to create a monopoly," in violation of the Clayton Act, 15 U.S.C. §§ 12-27, *as amended.* Congress has also empowered and directed the Commission to enforce or assist with implementing a large number of other statutes. The Commission relies on a variety of different types of assistance in carrying out its responsibilities under all the foregoing statutes, and letters from Members of Congress and the White House provide valuable information which is frequently used to develop or support Commission law enforcement and other initiatives.

---

[2] Social Security numbers that appear in a given letter from the White House or a Member of Congress are now redacted before the document is stored electronically in the non-public document management system. Although Social Security numbers have for several years been redacted from the versions of White House and Congressional correspondence that are scanned into the non-public document management system, earlier correspondence stored in that system still contains such numbers. These and other privacy issues arising from the non-public document management system are being addressed through the preparation of a separate PIA for that system, and therefore are not discussed in detail in this PIA.

As a part of this process, the information in CMS is collected in order to facilitate the efficient, accurate, and timely handling of incoming correspondence from Congress and the White House. For a given letter, the Commission uses CMS to track both the incoming letter and the status of the FTC's response. For each letter, the FTC identifies the nature of the issue or issues involved; determines whether any such issues can be resolved by the Commission or the Commission staff, and if so conducts whatever investigation may be appropriate; and develops an appropriate response to the issue. The foregoing research is not conducted through CMS; CMS only is used to track the status of the research required and the status of the response needed. Certain information from a given letter which is stored in CMS – such as names, contact information, or other PII – may be used to draft the requisite response to the Member of Congress or to the constituent.

2.4 How is the information collected?

The Commission receives correspondence via letter carrier mail; a personal delivery service; email; or facsimile. Members of the Commission staff then manually enter into CMS the information identified in Section 2.1 above, and each letter is thereafter scanned into the internal document management system.

2.5 How will the information be checked for accuracy and timeliness (currency)?

The organization responsible for drafting a response to a given incoming letter may contact the constituent involved – or the Congressional Office involved, in consultation with the Office of Congressional Relations – to secure additional information or to verify the accuracy of the information in the incoming letter, including information entered from the incoming letter into CMS. As discussed above, for a given incoming letter, the data maintained within CMS primarily consists of contact information which is used for directing the response to that letter to the appropriate Congressional Office or constituent. Members of the Office of the Secretary staff update that information as warranted.

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

The system uses technologies only in ways which the Commission has previously employed. CMS utilizes a database and a set of tools provided by Oracle Corporation to manage the data, security, and business rules of the application. Using Oracle maximizes data quality, data security, and system performance. Users access CMS using a software program that runs on a user's desktop developed in Oracle Forms.

2.7 What law or regulation permits the collection of this information?

The collection of documents and information within CMS is governed by the Federal Trade Commission Act, 15 U.S.C. 41 et seq. and the Privacy Act of 1974, as amended (5 U.S.C.

552a).

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The system is used only for internal purposes (subject to the information in Section 3.3 below), and the FTC maintains safeguards to protect this information as described in this document. For these reasons, the privacy risks are low. Risks to privacy arise primarily from internal threats to the information contained within the CMS database, which include the unauthorized or inadvertent release of PII, and unauthorized browsing for information.

Several safeguards have been implemented to mitigate these risks, and to prevent the unauthorized disclosure of PII from CMS. First, the system uses access controls so that only certain Commission personnel can access CMS and add, change, or delete information. Moreover, other Commission personnel who wish to view information in the CMS database may do so only through the use of a separate user-identification and password. These restrictions help to protect the information in CMS from internal threats.

Second, the computer on which the database is stored is protected by a firewall and is not accessible from outside the Commission. As required by OMB Memorandum 03-22 – and consistent with Commission obligations under the Federal Information Security Management Act – the Commission affirms that it follows IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured in the relevant system; that it has identified appropriate security controls to protect against that risk; that it has implemented those controls; and that appropriate monitoring, testing and evaluation are conducted on a regular basis by the Commission (or by a contractor or subcontractor, where applicable) to ensure that the requisite controls continue to work properly, thereby safeguarding the information.

3 Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

The information from a particular consumer is used to resolve his or her inquiry, and to communicate the requisite information back to the consumer, either directly or, much more commonly, through the appropriate Congressional Office. The information is also used to provide tracking reports, which help to ensure that the Commission answers each letter received in a timely manner.

3.2 Which internal entities will have access to the information?

The information is primarily used by members of the staff in the Office of the Secretary, who are authorized to enter data into and to edit data in CMS. Moreover, members of the staffs of the Office of General Counsel and the Office of Congressional Relations may use this information (on a read-only basis) in the course of their work. Furthermore, when the Office of

the Secretary forwards a given incoming letter to one of the Bureaus or Offices for the preparation of a draft response, the Office also forwards a printed referral form containing some of the data entered into CMS. To the extent that contractors may also have access to CMS – primarily for the purpose of maintaining or repairing the system – they are bound by non-disclosure agreements prohibiting the unauthorized disclosure of information collected by the Commission.

The FTC often seeks public comments on Commission rulemakings or other public proceedings. These comments are posted on the Commission's public website. When Members of Congress submit – on their own behalf or on behalf of one or more of their constituents – letters that constitute public comments, such documents must be posted on the Commission website. In that circumstance, some of the information in CMS is shared with the Records and Filings Office, for the purpose of ensuring that the incoming letter is properly processed as a public comment.

3.3 Which external entities will have access to the information?

Once the issues raised by a particular incoming letter have been researched and addressed, the Commission sends a response to the appropriate Congressional Office or constituent. The response letters may contain some of the information collected by the Commission (as described in Section 2 of this document), such as the name of the constituent involved, and the city in which he or she resides. However, the response letters do not contain sensitive personally identifiable information.

The Commission may be required or authorized by law to share certain data collected in CMS in other circumstances, including in response to Freedom of Information Act requests from private individuals or organizations. In these situations, the Commission redacts sensitive personally identifiable information and sensitive health information – as required by Commission policy and any applicable rules or court orders – from the material provided in response to any such requests. The Commission may also be required or authorized by law to share certain data collected in CMS with state or other federal government entities.

4 Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

Notice is provided in the Systems of Records Notice, Section 4.2, Miscellaneous Office Correspondence Tracking System, as well as in this Privacy Impact Assessment. It is not practicable to provide any other type of notice, because the FTC does not solicit the information at issue from individuals. Any PII that the Office of the Secretary places in CMS instead derives from correspondence which individuals voluntarily submit – either to the White House or to a Member of Congress – and which the White House or the Member of Congress then forwards to the Commission in order to help resolve the problems at issue. Moreover, constituents contacting Congressional offices frequently sign a "privacy release statement," which

Congressional offices sometimes forward in turn to the Commission in conjunction with the constituent letters.

4.2 Do individuals have the opportunity and/or right to decline to provide information?

For the reasons stated in Section 4.1, individuals may not necessarily have notice of or an opportunity to consent to Commission collection or use of the information they provide, other than by refraining from including the information in their correspondence to the White House or to Members of Congress. As noted above, the provision of any such information is completely voluntary; members of the general public are not obligated in any way to submit information, whether in the form of correspondence or otherwise, to the White House or to Members of Congress.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Individuals do not have the right to consent to particular uses of the information at issue, because once a letter is sent to the Commission by the White House or a Member of Congress, it is not practicable to give the constituent involved the opportunity to opt out of providing PII or other information the letter may contain, or to consent to any particular use of that information. As noted above, while CMS is not designed to collect sensitive personally identifiable information or sensitive health information, each letter received from the White House or a Member of Congress is scanned into the internal document management system – after any Social Security numbers it contains have been redacted – and the remaining information in the letter is therefore stored in the document management system. Whether stored in CMS or the document management system, the information in the letter is used to assist the constituent involved in resolving his or her specific problem. As noted in Section 3.3 above, the Commission may also be required or authorized by law to share certain data collected in CMS with state or other federal government entities.

4.4 What are the procedures that allow individuals to gain access to their own information?

Consumers may request a copy of information in the system covered by the Privacy Act, by following the Commission's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. 4.13. For more information on accessing information, please visit the Commission's Freedom of Information Act Office Web Page, located at http://www.ftc.gov/foia/contact.shtm.

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

The privacy risks which may arise from providing an individual with access to his or her

own records are low, because individuals may only access their records as described in Section 4.4. The Commission's Privacy Act procedures permit the FTC to verify a requesting individual's identity before granting him or her access to the records at issue.

5 Web Site Privacy Issues

No components of CMS are accessed via a web site. Therefore, this section is not applicable.

6 Security of Information in the System

6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure that information in CMS is appropriately secured. CMS is a Minor Application that rides on the Infrastructure General Support System (GSS) which is categorized as a moderate using Federal Information Processing Standard (FIPS) 199.

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

CMS is considered to fall within a larger system know as General Support Systems, and does not require a separate Certification & Accreditation. A Certification & Accreditation was completed for the General Support Systems on September 11, 2007.

6.3 Has a risk assessment been conducted on the system?

CMS is considered to fall within a larger system known as General Support Systems, and does not require a separate risk assessment.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

The system uses proven, secure technologies for internal use only and therefore does not raise privacy concerns.

6.5 What procedures are in place to determine which users may access the system and are they documented?

Only authorized FTC employees and contract staff may obtain access to the system. An individual may secure access to the system – with the approval of his or her supervisor – by submitting the appropriate forms to the Commission's information technology office. The application administrator then reviews the application and if permissible grants the appropriate level of access permissions to the individual.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC personnel, including those who work on CMS, are subject to FTC agency-wide procedures for safeguarding sensitive personally identifiable information and sensitive health information. All FTC personnel also receive annual computer-based training and other guidance explaining how to safeguard this information.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

The FTC both employs the limits on access to the CMS system described above and exercises management oversight of users accessing the system, in order to prevent misuse of the data the system contains.

6.8 Who is the point of contact for any additional questions from individuals?

The point of contact for any additional questions from individuals is the Commission's Chief Information Security Officer.

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

Data in CMS is to be maintained for six years after the Commission's reply. See also Section 7.2.

7.2 What are the plans for destruction or disposal of the information?

Commission records are to be retained and destroyed in accordance with schedules and procedures issued or approved by the National Archives and Records Administration (NARA). CMS data is scheduled under SF-115 "Request for Records Disposition Authority" number N1-122-96-2/A, which provides for deletion of the data in CMS relating to a particular letter six years after the response has been sent.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

See Section 2.8. In addition, the data in CMS will be disposed of in such a way as to make it impossible to recover.

8 Privacy Act

8.1 Will the data in the system be retrieved by a personal identifier?

The data in the system may be retrieved by a personal identifier, such as name and address.

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

The information concerning individuals to be collected in CMS is covered by an existing Privacy Act System of Records notice, which describes, in particular, System FTC-IV-2: Miscellaneous Office Correspondence Tracking System Records - FTC. For the Privacy Act System of Records notice, see **http://www.ftc.gov/foia/lisofpaysystems.shtm.**

Prepared for the Business Owners of the System by:

_____
Susan Taylor
Manager of Congressional Correspondence
Office of the Secretary

Review:

_____
Alexander C. Tang, Attorney
Office of the General Counsel

_____

Marc Groman
Chief Privacy Officer

_____
Margaret Mech
Chief Information Security Officer

Approved:

_____
Stan Lowe
Chief Information Officer
Federal Trade Commission

Date:_____