Privacy Impact Assessment
for

CPNI Reporting

December 17, 2008

Contact Point
Nancy Clark
Criminal Investigative Division
Information Technology Section
US Secret Service
202-406-9333

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The US Secret Service (USSS) and the Federal Bureau of Investigation (FBI) co-sponsor and manage the CPNI (Customer Proprietary Network Information) Reporting website. The website is a tool for telecommunications carriers to report a breach of its customer proprietary network information to law enforcement. The USSS and the FBI are conducting this Privacy Impact Assessment (PIA) because the CPNI Reporting website contains personally identifiable information (PII).

Overview

The CPNI Reporting website is a mechanism for telecommunications carriers to report to law enforcement a breach of its customer proprietary network information (CPNI). The Federal Communications Commission authorized the website pursuant to its mandate that telecommunication carriers report CPNI data breaches to the USSS and FBI through a "central reporting facility." For Notification of Customer Proprietary Network Information Security Breaches, please see Federal Communications Commission (FCC) Rule 07-22 (codified at 47 C.F.R. 64.2011).

CPNI is the data collected by telecommunications corporations about a consumer's telephone calls. It includes the time, date, duration, and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill. For the statutory definition of CPNI, please see the Telecommunications Act of 1996, 47 U.S.C. § 222 (h)(1)[1]. If a carrier submits a report of CPNI breach to the CPNI Reporting website, the carrier is requested to provide the name, telephone number, and email address of a contact person for that carrier. The website does not ask for or require a personal (non-business) telephone number or email address. In addition, the website specifically advises individuals against including any CPNI data in their reports.

The information collected from the carrier is simultaneuously sent to the appropriate division of the USSS and the FBI. Once an investigation is started by either agency, each agency may share resulting information with the other.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

[1] (1) Customer proprietary network information
The term "customer proprietary network information" means—
(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
except that such term does not include subscriber list information.

1.1 What information is collected, used, disseminated, or maintained in the system?

The information collected consists of the name of the contact person submitting the CPNI report for the telecommunications carrier, job title, work telephone number, work email address, business address, branch address, and incident location. CPNI specifically does not include subscriber information, i.e., it does not include subscriber name, social security number, address, etc.

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

Information is collected directly from individual employees of the carrier submitting the CPNI Report.

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

The information is collected from the telecommunications carrier in order for the USSS and/or FBI to respond as quickly as possible to the CPNI breach report. The USSS and the FBI use the data submitted to this website to help determine whether investigative action will be taken.

1.4 How is the information collected?

Information is collected electronically from data submitted to the CPNI Reporting website.

1.5 How will the information be checked for accuracy?

Information is collected directly from the individual employees of the carrier reporting the CPNI breach; the presumption exists that the information provided is accurate so as to facilitate a speedy response to breach reports.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The collection of the information is authorized by FCC Rule 07-22 (codified at 47 C.F.R. 64.2011) and Section 222 of the Communications Act of 1934, as amended. 47 U.S.C. § 222.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Contact information is limited to the information necessary to perform the information distribution functions of the program or project. All information is collected with the consent of the

individual providing it. Accordingly, the privacy risk from the amount and type of data collected appears to be minimal.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The USSS and FBI use the information submitted to determine whether to initiate an investigation. They use personally identifiable information (PII) to contact individuals in reference to a CPNI breach.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Information is stored but is not manipulated in any way other than to populate address fields for a mass email or paper mailing. Data may be inputted into databases or electronic spreadsheets and accessed via the various data elements. For example, a query may be conducted to locate all contacts in a certain state.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Neither contact information nor CPNI investigative data is created, populated, or verified with data collected from commercial or publicly available sources.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk presented by the use of contact information is the potential that the information could be used in ways outside the scope intended by the initial collection. The System of Records Notice USSS.003 (Criminal Investigation Information System, 73 FR 77729) and the FBI's Central Records System (63 FR 8671) as well as the Privacy Act Statements given prior to collection limit the use of information collected to contacting individuals who have reported a possible CPNI breach. Additionally, all USSS employees and contractors are trained on the appropriate use of PII.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The USSS retains the information no longer than is useful or appropriate for carrying out the information dissemination, collaboration, or investigation purposes for which it was originally collected. Contact list information will be retained for no more than six years after the last use. Information which is collected that becomes part of an investigative case file will be retained for a period which corresponds to the specific case type developed (e.g., judicial, non-judicial, non-criminal, etc.). These retention periods, established and/or approved by the National Archives and Records Administration, may cover periods as short as two years, or as long as 30 years, depending on the type or disposition of the case. Information which is collected that does not become part of an investigative case file will be destroyed/deleted after one year, or when no longer needed for agency business, whichever is sooner.

Any derivative documents created by FBI personnel or contractors using information reported via the portal will take on the disposition schedule of the FBI file classification into which the document is filed, regardless of whether or not the information becomes part of an investigative case. The disposition varies by FBI file classification. When the FBI decides to use the information or conduct an investigation, that information will be recorded in the FBI's records system and will follow the FBI's records retention schedule.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Consistent with requirements contained within 36 CFR 1234 and the E-Government Act of 2002, efforts to schedule the electronic system which collects the information have already begun (including communication and coordination with NARA), with final approval anticipated within 12 months.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Pending final approval from NARA, contact list information will be retained for no more than six years after the last use. This minimizes retention and security costs associated with maintaining contact lists. Additionally, any individual may opt out of any distribution list at any time in order to have their information expunged from the list, thereby eliminating any privacy risks posed by retention of their contact information.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

As a general rule, contact information will not be shared with internal DHS components because there is no need to know.

4.2 How is the information transmitted or disclosed?

As a general rule, contact information will not be shared with internal DHS components because there is no need to know.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

As a general rule, contact information will not be shared with internal DHS components because there is no need to know.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Contact information will be shared with the FBI as a collaborating partner in the CPNI Reporting website. The FBI will share the information pursuant to its own authorities and processes.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. The sharing of contact information between USSS and the FBI is consistent with the routine uses contained in the USSS's System of Records Notice USSS.003 (Criminal Investigation Information System, 73 FR 77729) and the FBI's Central Records System (63 FR 8671).

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information is shared in a collaborative workspace between the USSS and FBI, which is authorized by FCC directive, with USSS bearing responsibility for the security of the portal and transmission of the data to the FBI. Any information shared with organizations outside USSS is required to be appropriately secured per Office of Management and Budget Memorandums 06-15, Safeguarding Personally Identifiable Information, and 06-16, Protection of Sensitive Agency Information.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

A risk is presented whenever the USSS shares information it has initially collected from agencies or individuals outside of DHS. If external sharing of information would exceed the narrow purpose for which the contact information was collected, then the information is not permitted to be shared. The System of Records Notice USSS.003 (Criminal Investigation Information System, 73 FR 77729) and the FBI's Central Records System (63 FR 8671) limits the instances where contact information may be shared with outside entities. Further, all USSS employees and contractors are trained on the appropriate use and sharing of information.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. This privacy impact assessment and the System of Records Notice USSS.003 (Criminal Investigation Information System, 73 FR 77729) and the FBI's Central Records System (63 FR 8671)

provide notice regarding the collection of contact information. The collection of contact information is immediately preceded by notice regarding the scope and purpose of the contact information at the time of collection. The Privacy Act Statement, required under 5 U.S.C. § 552a(e)(3),(see appendix A), provides individuals notice at the moment of collection.

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

Yes. Individuals are not required to provide personal (non-business) telephone numbers or email addresses. However, if some form of contact information is not provided individuals will not be able to receive information in response to CPNI breach report.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Consent to use the information is implicit in its provision. USSS will only use the information for the limited purpose for which it was collected, i.e., contacting individuals. Should an individual suspect information is being used beyond the given scope of the collection, they are encouraged to write to the system managers.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The privacy risk associated with notice in the collection of contact information is that the individual is not aware of the purpose for which the information submitted may be used. Notice is always provided prior to the collection of information. This risk is primarily mitigated by limiting the use of contact information to what is necessary for the purposes of contacting the person according to his or her voluntary subscription or request. Additionally, the System of Records Notice USSS.003 (Criminal Investigation Information System, 73 FR 77729) and the FBI's Central Records System (63 FR 8671) provides notice of the purpose of the collection, redress procedures, and the routine uses associated with the collection of contact information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Access requests should be directed to United States Secret Service, FOIA/PA Officer, Suite 3000, 950 H Street, NW, Washington, DC 20223.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The procedures are the same as those outlined in Question 7.1.

Additionally, the System of Records Notice USSS.003 (Criminal Investigation Information System, 66 FR 45362) and the FBI's Central Records System (73 FR 77729) details access provisions along with the names of officials designated to field such requests.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified at collection that they may correct their information at any time by the procedures outlined above. Procedures for correcting information maintained within the system is also outlined in the Criminal Investigation Information System SORN (USSS.003, 73 FR 77729).

7.4 If no formal redress is provided, what alternatives are available to the individual?

Appropriate redress is provided.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals may correct their information at any time during which the USSS possesses and/or uses their contact information. Any risks associated with correction of information are thoroughly mitigated by the individual's ability to opt out of the contact list or correct their information via the same process by which they submitted information.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

DHS physical and information security policies dictate who may access USSS computers and filing systems. Specifically, DHS Management Directive 4300A outlines information technology procedures for granting access to USSS computers, which is where the majority of contact information is stored. Access to contact information is strictly limited by access controls to those who require it for completion of their official duties.

8.2 Will Department contractors have access to the system?

Yes, depending on the project or program. Many times contractors are tasked with information distribution and other outreach tasks. Contractors are required to have the same level of security clearance in order to access USSS computers as all other DHS employees.

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

All USSS employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of personally identifiable information such as what is contained in contact lists. Also, DHS recently published the "Handbook for Safeguarding Sensitive PII," providing employees and contractors additional guidance.

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

Most simple contact lists are stored on spreadsheets or similar formats that do not qualify as an information technology system requiring a Certification and Accreditation (C&A) pursuant to the review processes established by the Chief Information Security Officer; however, these documents are stored on secure Department networks which have completed C&As. Other contact lists which are part of more robust functionalities reside on information technology systems that are required to receive a C&A.

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

All Department information systems are audited regularly to ensure appropriate use and access to information. Specifically related to contact information, such lists residing on a local area network's shared drive are restricted by access controls to those who require it for completion of their official duties. Folders within shared drives are privilege-protected.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk of unauthorized access exists with any information technology system or document. The Department conducts thorough background checks on every employee and contractor. Access to the systems and networks which store the contact information are protected pursuant to established Departmental procedures (see 8.4).

All Department employees and contractors are trained on security procedures, specifically as they

relate to personally identifiable information.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The CPNI Reporting website is an information-collection tool.

9.2 What stage of development is the system in and what project development lifecycle was used?

The CPNI Reporting website detailed here is not necessarily involved in a specific lifecycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

If a particular technology used in the collection or handling of information in connection with the types of contact lists addressed in this PIA raises specific and/or heightened privacy concerns, the implementation of the technology will require a separate PIA.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Appendix A

PRIVACY ACT STATEMENT

The USSS and the FBI are authorized to solicit this information from you pursuant to section 64.2011 of the rules of the Federal Communications Commission (FCC) and section 222 of the Communications Act of 1934. Your disclosure of this information is mandatory. Failure to provide this information may result in an investigation and possible imposition of penalties by the FCC pursuant to the Communications Act of 1934.

This information is being collected in order that the relevant investigating agency may contact you in the event that your organization experiences a breach of customers' CPNI.

This information will be maintained by the USSS in its Criminal Investigation Information System, USSS.003 73 FR 777729 (December 19, 2008)[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=01-21653-filed.pdf], and by the FBI in its Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998) [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1998_register&docid=98-4206-filed.pdf], as amended by, 66 Fed. Reg. 8425 (Jan. 31, 2001) [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=01-2397-filed.pdf], 66 Fed. Reg. 17,200 (Mar. 29, 2001) [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=01-7676-filed.pdf], and 72 Fed. Reg. 3410 (Jan. 25, 2007) [http://edocket.access.gpo.gov/2007/pdf/E7-1176.pdf].

Information regarding the disclosure of this information that may be made pursuant to routine uses published in the above-referenced systems of records may be viewed by clicking on the links above.