Missing Persons Community of Interest (MPCI)

Using Fair Information Practices to Develop Privacy Best Practices For Missing Persons Organizations

Editor: Bob Gellman (bob@bobgellman.com)
Contributors: Tim Schwartz (tim@timschwartz.org)
Vicki Welsh

Revision: 1.5
Date: October 26, 2013

Table of Contents

Purpose

The purpose of this document is to help members of the Missing Persons Community of Interest (MPCI) to develop functional privacy practices for the processing of personal information about missing persons following natural disasters. The MPCI is an independent, informally organized group of humanitarian organizations, companies, and volunteers. This document may be useful to those developing, managing, and using information systems containing personal information.

Definitions

Missing Person

An individual who is not in contact with his or her family or friends due to a natural disaster. Each missing persons organization may use its own definition of *missing person*, as well as its own definition of what constitutes a natural disaster.

Personal Information or Personally Identifiable Information (PII)

Information relating to an identified or identifiable natural person ("individual").

Processing

The collection, maintenance, use, or disclosure of personal information.

Data Subject

A natural person whose personal information is being processed.

Data Controller or Record Keeper

The individual or organization responsible for the processing of personal information and for compliance with any applicable data protection or privacy rules.

Fair Information Practices (FIPs)

Practices for addressing the privacy of information about individuals. Different versions of FIPs exist. The version used here derives from the Organisation for Economic Cooperation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[1]

1 The OECD's version of FIPs is most influential statement in general use. See http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. For a short and general history of FIPs, see Robert Gellman, *FAIR INFORMATION PRACTICES: A Basic History* (2012) (Version 1.91), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

Fair Information Practices

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

A data controller should be accountable for complying with measures, which give effect to the principles stated above.

Introduction

Fair Information Practices (FIPs) are a set of internationally recognized practices for addressing the privacy of information about data subjects. The elements of FIPs provide a menu of major privacy principles that are helpful in the development of best practices for – or operating – any personal information system. FIPs can be implemented in many different ways so the ideas presented here include only some of the available options. The FIPs principles can and should always be adapted to the technologies in use, applicable laws, and local institution's needs.

Defining the scope of any missing persons database system is a prerequisite to applying privacy principles. A missing persons organization will likely have data about different categories of individuals, including missing persons, third parties, service providers, volunteers, staff, and system users. Personal information for each of these categories may not be maintained in the same information system, the same privacy policies may not apply to each category, and the priority for developing privacy policies may not be the same. The focus here is on information systems that collect personal information about missing persons.

Some of the particular challenges of missing persons activities include: 1) unpredictable timing for the start and location of processing activities; 2) telecommunications challenges; 3) impracticality of obtaining consent or providing actual notice; 4) emergency conditions where basic human needs may trump privacy concerns; 5) some systems may be entirely open to public access; and 6) data processing in more than one national jurisdiction.

The best practices outlined here will not focus on compliance with the privacy obligations of specific countries where missing persons organizations operate. Countries with modern data protection laws generally require data controllers to comply with most elements of Fair Information Practices already. Some of the best practices listed here may exceed legal requirements. However, in the United States and some other countries, there may be no applicable privacy law.

Openness Principle

> There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

The openness principle requires that any data subject be able to learn of the existence of a processing operation, who is the data controller, and what personal data is being processed. Where the data subjects are missing persons, normal methods for notifying individuals about record keeping activities may not work well. In many circumstances providing a notice to missing persons is likely impossible. Internet notices of privacy practices (in multiple languages when possible) that describe personal data activities may be the best way to provide general notice to individuals and to the world. A notice of privacy practices might include additional information about activities specific to each natural disaster. For each disaster operation, a notice of privacy practices might require translation into an additional language. Local information particular to each disaster might be added to the notice of privacy practices when possible to allow affected individuals to learn more about the data systems and about their rights.

Best Practices

1. **Maintain an internet notice of privacy practices in multiple languages depending on the population being served.**
2. **Include in the notice of privacy practices an appropriate level of detail about the manner in which data is recorded, deleted, displayed, accessed, and shared.**
3. **Provide a notice of privacy practices accessible to users. If users of a website must register, provide the notice of privacy practices at that time.**
4. **Prepare a supplemental notice of privacy practices for each disaster.**
5. **Communicate with other missing persons groups and with relevant organizations and government agencies in advance of a natural disaster in order to a) understand their operations and requirements; b) develop cooperative methods; c) establish data and other standards when possible; and d) develop relationships.**
6. **Remember that a notice of privacy practices is useful in informing and training staff and volunteers about policies that should govern their activities.**
7. **Make the notice of privacy practices publicly available at all times.**

Collection Limitation Principle

> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Some elements of the collection limitation principle will be difficult to satisfy in a disaster. Providing notice of privacy practices to or obtaining the consent of a data subject may not be possible in most circumstances, and it may not be essential because notice or consent are not *appropriate* for some humanitarian activities following disasters.

Limiting the collection of personal information should remain a goal. Many data elements can and will be identified and defined in advance, but local circumstances may call for the use of unplanned elements. For example, some health information or location information may be needed to describe an individual. However, the collection of complete medical histories will likely be inappropriate in most cases.

A best practice allows the routine collection of standard data elements (e.g., name, age, nationality, location, etc.) but requires additional approval or specific findings or particular circumstances for the collection of non-standard data elements or sensitive data elements (e.g., political opinions). Personal information not necessary for the purpose of the data controller should not be collected.

Best Practices

1. **Define in advance which data elements will be collected.**
2. **Do not collect unnecessary personal information. Be cautious when collecting identification numbers.**
3. **Only collect non-standard data elements when justified by specific needs and only following specific approval by an appropriate administrator.**

Data Quality Principle

> Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

The accuracy, completeness, and timeliness standard of the data quality principle is qualified by the phrase *to the extent necessary*. Under emergency circumstances, the need for flexibility in meeting accuracy, completeness, and currency standards is understandable. When the purpose for which missing persons data was collected is over, the principle does not require the application of resources to keep the data current. A best practice is to include a policy that determines how long data for any given disaster will be maintained, when (possibly in stages) any unnecessary personal data will be destroyed, and when data will be de-identified (along with other appropriate safeguards) if there is value in keeping data for research or other secondary purposes.

Best Practices

1. **Establish and implement a clear policy for data deletion and data retention.**
2. **Establish a policy for ending public disclosure of personal information when the need diminishes. A policy could a) rely on a fixed time frame following a disaster; b) monitor usage and end disclosure when usage drops; or c) use a phased process that first closes off acceptance of reports about missing persons, then closes off public search, and finally allows only administrative or research use of PII.**
3. **Create safeguards (possibly including de-identification or encryption) for longer term storage of personal data.**
4. **When transferring data to other users, specify policies about data deletion or deidentification.**

Purpose Specification Principle

> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

> Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

The purpose specification principle works together with the use limitation principle, and both are considered together. Specification of purposes for any personal data processing implements the general policy that data collected for one purpose should not be used for another purpose. This privacy policy is widely admired, but it is not always possible to define purposes in advance with precision. Governments and other who maintain routine administrative records sometimes find that a lack of foresight creates problems following a disaster. Temporary privacy codes or other accommodations may be needed to allow those records to be used for disaster-related activities.

The purposes of a missing persons information system should be defined, including specifications about the possible use of the data for other emergency-related activities, such as public health and law enforcement; sharing with other missing persons and disaster relief organizations; and use for secondary activities, such as research. Defining purposes clearly and in advance will help those making decisions immediately following a disaster to know when particular disclosures are allowable. A broad definition of purpose may be needed but should remain mindful that purposes should be *explicit and legitimate*.[2]

The purpose specification principle recognizes the tension between the need for specificity and the difficulty of foreseeing all possible uses and disclosures. It allows for other purposes that are *not incompatible* with the stated purposes. For example, the EU Directive expressly states that secondary activities for historical, statistical, or scientific purposes are not considered as incompatible with the purpose of any system.[3] Missing persons organizations may choose to apply that policy, recognizing the privacy risks of longer term data retention.

Implementing the purpose limitation and use limitation principles consistently and fairly can be difficult in ordinary circumstances and may be particularly challenging in disasters. The principles recognize that it may not be possible or practical to specify in detail and in advance each purpose for which personal data is intended to be used.

---

2 See Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Recital 28, 1995 O.J. (L 281) 31, 39, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

3 *EU Data Protection Directive*, at Art. 6(1)(b).

There are ways to address the uncertainties inherent in an incompatibility standard. Internal controls may help, such as requiring appropriate supervisory approval to prevent individual staff members from making ad hoc determinations. Discretion may be greater if disclosures involve one or two records than if disclosures involve larger numbers or an entire database.

These principles allow uses with the consent of the data subject. However, consent will generally not be possible in emergency circumstances.

Best Practices

1. **Define a broad statement of purposes for each record keeper and tailored for each distinct database. Purposes must be explicit and legitimate.**
2. **Establish administrative controls on ad-hoc determinations of new purposes.**
3. **Establish stricter controls for disclosure of larger numbers of records or an entire database.**
4. **Be aware of any legal restrictions on the export of personal information to other countries.**
5. **Review operations following a disaster in order to improve compliance with privacy standards.**

Security Safeguards Principle

> Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

The security safeguards principle is a high level statement that personal data should be protected by reasonable security safeguards. The principle specifies the need for protections against loss, unauthorized access, destruction, use, modification, or disclosure. Security obligations must keep pace with technology. A risk assessment for any missing persons system is a best practice. Part of that assessment should consider whether the missing persons organization has any legal or other obligation to provide a notice to data subjects in the event of a security breach. Providing a breach notice to data subjects is impractical during an emergency, but it would be worthwhile for any organization to consider in advance the possibilities and, if relevant, the methodology. The maintenance of personal data beyond emergency circumstances following a disaster may give rise to breach notice obligations that cannot be dismissed as impractical. The maintenance of sensitive information may be a factor as well. Even data made publicly available needs some level of security to prevent unauthorized changes or downloading of an entire database.

Best Practices

1. **Conduct a risk analysis for each ongoing missing persons activity in advance of any disaster response.**
2. **Evaluate any obligations that a data controller has to provide notice of a security breach to data subjects.**
3. **Safeguard data systems that are publicly accessible against unauthorized changes and against unauthorized copying of the entire database.**

Individual Participation Principle

> An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

This principle covers access and correction rights. Each individual should have the right to know whether a data controller has data pertaining to the individual; the right to see and/or copy their data; the right to be given a reason if a request for access is denied and to challenge the denial; and a method to challenge data that is not accurate or complete.

Implementing standard access and correction rights in emergency circumstances may not be a priority or even a possibility. However, individuals in a missing persons database may have vital reasons that they want to see their data, correct it, or even make some of their data unavailable to some or all possible users. Notwithstanding emergency circumstances, a missing persons organization has an interest in maintaining accurate data. Data subjects will be one source of accurate information. The extent to which formal rights can be accommodated in an emergency will vary, but a best practice includes the awareness of the issues involved and at least an informal way of responding to individual requests that require attention during an emergency. Individual use of access and correction rights is likely to be rare in many circumstances, but it is also likely to be important when individuals seek to use their rights.

Best Practices

1. **Addressing individual rights of access and correction can be challenging during emergency circumstances. Provide at a minimum an informal means of responding to individual requests may be appropriate, especially when an individual's interest is significant.**
2. **For databases maintained for longer periods or beyond the immediate needs of disaster response, maintain a more formal process that allows individuals to exercise rights.**

Accountability Principle

> A data controller should be accountable for complying with measures, which give effect to the principles stated above.

There are many ways to provide accountability measures for FIPs. For example, the accountability principle for compliance with FIPs can be met with administrative enforcement, arbitration, internal or external audits, complaint processing, staff training, a privacy office or officer, and more. Some of these accountability measures will be practical for a missing persons organization, but perhaps not during an emergency. An after-disaster review of activities with an eye toward privacy issues may be a useful way of finding issues, adjusting standards, and educating staff about issues. Some organizations have a Chief Privacy Officer (CPO) who can be useful in many different ways to provide accountability during and after operations. A CPO need not be a full-time job, but centralizing privacy responsibilities in one place can be useful.

Best Practices

1. **Centralize privacy responsibilities in a Chief Privacy Officer.**
2. **Conduct after-disaster review for privacy.**
3. **Conduct regular internal review of privacy activities and update privacy policy when required.**
4. **Use internal audits to make sure that records are deleted according to schedule.**
5. **Provide an effective response to complaints.**
6. **Maintain audit trails for disclosures (at least for bulk disclosures)**

Ideas for Future Revisions

- A best practice for collecting photographs under the collection limitation principle.

Document history

Version 1.0 – First draft (RG)
Version 1.1 – Incorporates TS edits and RG responses (RG)
Version 1.2 – Incorporates edits and ideas from VW and MPCI call 5-3-13 (RG)
Version 1.3 – Following 6/20/13 call (TS, VW, RG)
Version 1.4 – Further minor edits by RG & TS
Version 1.5 – Design revisions and minor spelling edits (TS)