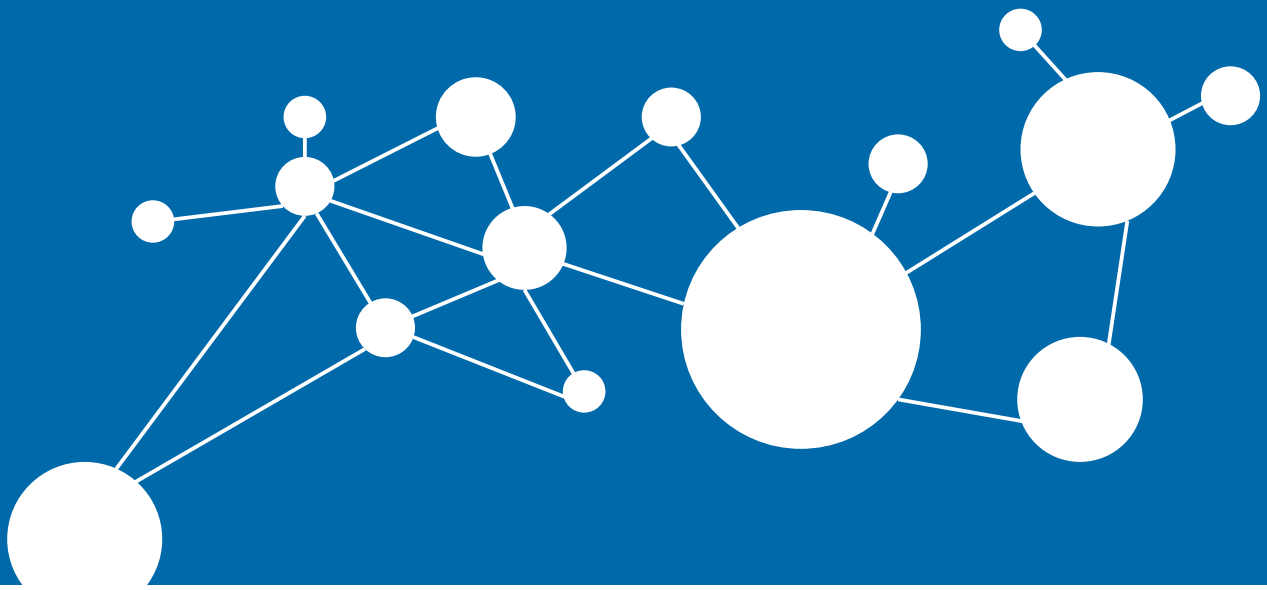
Policy Series vol 2

Privacy and Missing Persons after Natural Disasters

By Joel R. Reidenberg, Robert Gellman, Jamela Debelak, Adam Elewa, and Nancy Liu



CLIP Center on Law and Information Policy AT FORDHAM LAW SCHOOL

Wilson Center

COMMONS LAB

Privacy and Missing Persons after Natural Disasters

By Joel R. Reidenberg, Robert Gellman, Jamela Debelak, Adam Elewa, and Nancy Liu

PRIVACY AND MISSING PERSONS AFTER NATURAL DISASTERS

Center on Law and Information Policy
Fordham Law School
140 West 62nd Street
New York, NY 10023
(212) 930-8879

http://law.fordham.edu/clip

Commons Lab
Science and Technology Innovation Program
Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue, N.W.
Washington, DC 20004-3027

www.CommonsLab.wilsoncenter.org

Reidenberg, Joel R., Gellman, Robert, Debelak, Jamela, Elewa, Adam, and Liu, Nancy. *Privacy and Missing Persons After Natural Disasters.* Washington, DC and New York, NY: Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars (2013).

Copies are available for download free of charge at http://www.scribd.com/collections/3840667/Commons-Lab-Science-and-Technology-Innovation-Program-STIP or http://ssrn.com/abstract=2229610.

This report is a joint project between the Center on Law and Information Policy at Fordham Law School (Fordham CLIP) in New York, NY, and the Commons Lab of the Science and Technology Innovation Program (STIP) of the Woodrow Wilson International Center for Scholars, in Washington, DC.

are those of the authors and are not presented as those of any of the sponsoring organizations or financial supporters of those organizations. Any errors and omissions are the responsibility of the authors.

The Center on Law and Information Policy at Fordham Law School (Fordham CLIP) was founded to make significant contributions to the development of law and policy for the information economy and to teach the next generation of leaders. Fordham CLIP brings together scholars, the bar, the business community, technology experts, the policy community, students, and the public to address and assess policies and solutions for cutting-edge issues that affect the evolution of the information economy. Fordham CLIP's work is disseminated and used to help influence the guiding principles of the new knowledge-driven society and help find solutions to difficult legal issues posed by information technologies.

The Woodrow Wilson International Center for Scholars is the national, living US memorial honoring President Woodrow Wilson. In providing an essential link between the worlds of ideas and public policy, the Center addresses current and emerging challenges confronting the United States and the world. The Center promotes policy-relevant research and dialogue to increase the understanding and enhance the capabilities and knowledge of leaders, citizens, and institutions worldwide. Created by an act of Congress in 1968, the Center is a nonpartisan institution headquartered in Washington, DC; it is supported by both public and private funds.

Conclusions or opinions expressed in Center publications and programs are those of the authors and speakers. They do not necessarily reflect the views of the Center staff, fellows, trustees, advisory groups, or any individuals or organizations that provide financial support to the Center.

The Center is the publisher of *The Wilson Quarterly* and the home of both the Woodrow Wilson Center Press and the *dialogue* television and radio program. For more information about the Center's activities and publications, please visit them on the Web at http://www.wilsoncenter.org/.

The Science and Technology Innovation Program (STIP) analyzes the evolving implications of such emerging technologies as synthetic biology, nanotechnology, and geo-engineering.STIP's research goes beyond laboratory science to explore new information and communication technologies, sensor networks, prediction markets, and serious games. The program provides critical yet nonpartisan research for the policymaking community and guides officials in the design of new governance frameworks. It gauges crucial public support for science and weighs the overall risks and benefits of technology for society at large.

The Commons Lab of STIP seeks to advance research and independent policy analysis on emerging technologies that facilitate collaborative, science-based and citizen-driven decision-making, with an emphasis on their social, legal, and ethical implications. The initiative does not advocate for or against specific technological platforms. It works to ensure these technologies are developed and used to maximize benefits while reducing risks and unintended consequences. The Commons Lab focuses on novel governance options at the "edges" where the crowd and social media operate—between formal and informal organizations and proprietary and open-source models of data ownership and access.

Commons Lab Staff
David Rejeski, Director, Science and Technology Innovation Program
Lea Shanley, Director, Commons Lab
Zachary Bastian, Early-Career Scholar, Commons Lab
Ryan Burns, Research Assistant
Joe Filvarof, Program Assistant
Aaron Lovell, Writer/Editor

Blog: http://CommonsLab.WilsonCenter.org
Facebook: http://www.facebook.com/CommonsLab
Twitter: http://twitter.com/STIPCommonsLab
Scribd: http://bit.ly/CommonsLabReports
YouTube: http://biy.ly/CommonsLabVideo

The Commons Lab of the Science and Technology Innovation Program is supported by the Alfred P. Sloan Foundation.

About the Authors

Professor Joel R. Reidenberg led the Fordham CLIP team responsible for the research and writing of this report, with the assistance of members of the Missing Persons Community of Interest (MPCI). Robert Gellman, a privacy and information policy consultant, was the lead author. The team also included Jamela Debelak, Executive Director of Fordham CLIP, and two student researchers, Adam Elewa and Nancy Liu. Tim Schwartz, Chair of the Missing Persons Community of Interest, served as technical consultant to the Fordham CLIP team.

Joel R. Reidenberg holds the Stanley D. and Nikki Waxberg Chair in Law and is the Founding Academic Director of Fordham CLIP at Fordham Law School. Reidenberg's published books and articles explore both information privacy and information technology law and policy. He has served as an expert adviser to the US Congress, the Federal Trade Commission, and the European Commission on data privacy matters. Reidenberg received an A.B. degree from Dartmouth College, a J.D. from Columbia University, and both a D.E.A. droit international économique and a Ph.D in law from the Université de Paris-Sorbonne. He is admitted to the Bars of New York and the District of Columbia.

Robert Gellman is a privacy and information policy consultant in Washington, DC. A graduate of the Yale Law School, Gellman has worked on information policy issues for more than 35 years. He served for 17 years on the staff of a House of Representatives Subcommittee responsible for privacy, freedom of information, health confidentiality, and other information policy matters. He served as a member of the Department of Health and Human Service's National Committee on Vital and Health Statistics (1996-2000), an advisory committee with responsibilities for health information infrastructure matters. He is the author of numerous columns, papers, congressional reports, and scholarly articles on privacy and related issues.

Jamela Debelak is the Executive Director of Fordham CLIP. She also serves as Adjunct Faculty, teaching courses on Internet Law. Prior to joining Fordham CLIP, Jamela was an associate in the IP Transactional Group at Dechert LLP. She earned her B.A. degree *summa cum laude* from The Ohio State University and is a *magna cum laude* J.D. graduate of Temple Law School.

Adam Elewa is a law student at Fordham Law School. He is a *summa cum laude* graduate of Stevens Institute of Technology.

Nancy Liu is a law student at Fordham Law School. She is a *magna cum laude* graduate of Macaulay Honors College at Hunter College.

Acknowledgments

This report was reviewed in draft form by individuals chosen for their legal and technical expertise. They provided comments to help ensure that the published report meets the highest standards for objectivity and evidence. Fordham CLIP would like to thank the following individuals for their review of this report:

- **Colin J. Bennett**, Ph.D., Department of Political Science, University of Victoria
- **Mark Prutsalis**, President & CEO, Sahana Software Foundation
- **Daniel J. Solove**, J.D., John Marshall Harlan Professor of Law, George Washington University Law School
- **Charles D. Raab,** AcSS, FRSA, Professor of Government, School of Social and Political Science, University of Edinburgh
- **Edward S. Robson,** Esq., Robson & Robson LLC
- **Blair Stewart**, Assistant Privacy Commissioner (Auckland), Office of the Privacy Commissioner, New Zealand

These reviewers were not asked to endorse the conclusions or strategies in this report, nor did they review the final draft of the report before its release. Lea Shanley, Zachary Bastian, and Aaron Lovell of the Woodrow Wilson Center were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. The Wilson Center also supported and coordinated the final publication process.

Neither the reviewers nor the Woodrow Wilson Center are responsible for the content, views, or data contained in this publication. This report exclusively represents the views of the authors, who retain responsibility for the content, including all errors of fact and interpretation.

The authors are very grateful to Tim Schwartz for his assistance, advice, and counsel throughout the drafting process and for providing commentary on numerous drafts of this report and to Jordan Kovnot, Fordham CLIP Privacy Fellow for his editorial assistance. Fordham CLIP would also like to thank the following members of the Missing Persons Community of Interest who agreed to be interviewed for this project: Romain Bircher, International Committee of the Red Cross; Sharon Hawa, American Red Cross; Keith Robertory, American Red Cross; Ka-Ping Yee, Google, Inc.; Dorothy Chou, Google, Inc.; and Sarah Aizenman, Missing.net. Finally, the authors also thank Lea Shanley for her assistance throughout this project and the Woodrow Wilson Center, Edward Stroz and Stroz Friedberg for their generous support.

This publication was made possible by a grant from the Alfred P. Sloan Foundation to the Wilson Center and by Fordham University alumnus and trustee Edward M. Stroz and his digital risk management company, Stroz Friedberg LLC.

Edward M. Stroz is founder and Co-President of Stroz Friedberg, a leading global consulting firm for managing digital risk and uncovering digital evidence. In addition to overseeing the firm's growth, he assists clients in responding to Internet extortions, denial of service attacks, hacks, unauthorized accesses, theft of trade secrets, and advising on electronic discovery issues.

A former Special Agent for the Federal Bureau of Investigation, he created and supervised the FBI's Computer Crime Squad in New York City and worked on many high-profile cases. Mr. Stroz lectures widely on the threats of computer crime and abuse posed by insiders and is co-author of *Cyber Adversary Characterization: Auditing the Hacker Mind* published by Syngress Publishing. He has also presented expert testimony in many courts. A graduate of Fordham University, Mr. Stroz is a Certified Public Accountant, a Certified Information Technology Professional, and a Licensed Private Investigator.

Stroz Friedberg is a global digital risk management and investigations firm, specializing in digital forensics, data breach and cybercrime response, electronic discovery, security risk consulting, and business intelligence and investigations. Stroz Friedberg works at the crossroads of technology, law, and behavioral science to help clients manage the inherent risks and responsibilities of doing business in a digital era.

Contents

Foreword

Identifying individuals caught up in major natural disasters and reconnecting them to their families and communities is a challenging task. Earthquakes can destroy communications infrastructure. Floods can inundate storehouses of official records. Planners rarely know where and when a disaster will strike. After a disaster strikes, those who can do so flee. Those who cannot may be hidden in debris and seriously injured or worse. Access to the disaster zone may be difficult for days or weeks. The position may change from hour to hour. Many further challenges could be listed.

Individuals believed to be in a disaster zone may be listed as missing. People on the list may later be discovered alive or be positively identified as deceased. Some may never be found.

It may be an understatement to say the task of assembling and maintaining reliable information about missing people in the wake of a major disaster is difficult.

However, it is essential in the cause of common humanity. The first response to a major natural disaster must be to save life without regard to who the victims are. But any well-organized response must quickly take steps to seek to identify the missing.

The human emotions involved are intense. The stress of not knowing whether one's family member is alive or dead is agonizing. The agony may persist for a prolonged period. To digress from natural to man-made disasters, one may ponder the analogy of the mechanized destruction of the Western Front, where many bodies went unidentified. Communities made memorials to meet the human need for something tangible to remember the missing. One thinks also of the challenge to natural grieving when someone is advised that a solider is "missing in action." A denial of information about the fate of a family member may be a kind of torture. Think of the cruelty of regimes in the various "dirty wars," which informed families that their loved ones had "disappeared" rather than reveal the sordid truth.

In recent years, one innovation in the processing of information has been the growth of social media. This has manifested itself in many useful ways during natural disasters. Through the assistance of 'digital volunteers,' crowdsourced information has enabled real time mapping of the effects of a disaster zone where traditional means might have required days or weeks to compile something similar. Social media has been used to deploy volunteers productively in recovery efforts.

Social media has also been engaged to create crowdsourced missing persons registries. From a privacy perspective, this is a much more challenging proposition than mapping the physical infrastructure of a district or organising relief volunteers. Creating registries of missing persons raises a host of data protection and privacy issues. One central challenge is to ensure the reliability of information since inaccurate information about the fate of a person may be more distressing than saying nothing. Other challenging issues revolve around control and accountability.

We are fortunate that the authors of this report have reviewed the issues of privacy and missing persons registries, and other data protection aspects following from natural disasters. I congratulate the organizations supporting its publication and the authors for addressing such an important issue. The research and the legal and policy analysis will be an important contribution to understanding the subject and help prepare for future disasters in ways that are respectful of privacy.

Blair Stewart
Assistant Privacy Commissioner
Office of the Privacy Commissioner
Auckland, New Zealand
January 25, 2013

Executive Summary

When a natural disaster occurs, government agencies, humanitarian organizations, private companies, volunteers, and others collect information about missing persons to aid the search effort. Often this processing of information about missing persons exacerbates the complexities and uncertainties of privacy rules.

This report offers a roadmap to the legal and policy issues surrounding privacy and missing persons following natural disasters.

The report first identifies the privacy challenges in the disaster context and provides some recent examples that demonstrate how disaster relief information sharing raises unique privacy concerns and issues. It then outlines current missing persons information sharing activities in the context of disaster relief work and discusses how those information systems strike different balances between privacy and ease of use.

The report then proceeds to identify some key legal privacy issues and examines in detail how these legal requirements apply to missing persons organizations and what interpretative challenges privacy rules present. For the analysis, this report focuses on privacy law in the European Union and the United States because these jurisdictions serve as important examples of privacy regulation around the globe. The report offers a general analysis rather than a detailed assessment of any particular activity that would depend on the application of the law of a specific jurisdiction.

The report concludes with a set of options and strategies that organizations and policy makers involved in missing persons activities and in privacy could pursue to help address some of the privacy concerns:

- For the **Missing Persons Community of Interest**, an independent group of humanitarian organizations, companies and volunteers, options include assisting in the selection of privacy-friendly designs for missing persons databases, better coordination of privacy policies for its collaborators, and working with data protection authorities to address privacy issues.

- For **missing persons organizations**, options include assuring compliance with privacy rules, coordination of privacy policies, and sharing of relevant privacy resources. These organizations may have already addressed some of these challenges in their current activities.

- For **EU** d**ata protection authorities**, options include fulfilling the agenda set out in the 2011 resolution by the international data protection commissioners on data protection and major natural disasters, issuing clearer and more flexible data protection rules in response

to natural disasters, and providing interpretive guidance of the most important and uncertain existing rules to support missing persons activities.

- For the **European Union's Article 29 Working Party**, options are issuing interpretive guidance for disaster activities and reporting on progress in implementation of the 2011 resolution.

- For the **European Commission**, options are expressly addressing missing persons activities in the data protection regulation currently being drafted and providing more specific direction for the existing application of current rules to missing persons activities.

- For the **US government**, options include clarification of federal agency authority to share personal information for missing persons activities following disasters through executive or legislation actions.

- For other **national or sub-national governments**, options are adjusting or amending laws to allow for appropriate use of personal information for missing persons purposes following natural disasters.

I. Introduction

When a natural disaster occurs, information sharing among governments, relief organizations, and the public is critical to identify those affected and to provide necessary assistance and support. Information sharing about missing persons is one critical part of relief efforts that arise after every disaster. Missing persons information systems offer important tools for helping people reconnect during stressful circumstances by making critical information more easily accessible. The implications, though, for the processing of personal information are global. Victims, their relatives, and their friends all have a common need for information, but they may be located in different countries with different data protection regimes.

A number of organizations around the world—both for-profit and non-profit—work separately and collaboratively on ways to make information about missing persons in natural disasters available to appropriate individuals and institutions. Privacy is a concern for these organizations because they are often required to comply with privacy laws, yet these laws only occasionally include specific provisions accommodating information needs in emergency circumstances. In many countries, privacy rules protect fundamental rights and the right to privacy does not evaporate because of a natural disaster. As a result, in many disaster situations, privacy laws and policies intended to protect personal information have the potential to impede the useful sharing of critically needed information about missing persons. In effect, existing privacy laws and policies can create complex, international barriers to the way missing persons organizations collect, use and share information.

The report is designed to help the Missing Persons Community of Interest (MPCI), an independent, informally organized group of humanitarian organizations, companies, and volunteers, address privacy in their work to aid victims in coping with natural disasters. The report also seeks to assist privacy regulators and policy makers in understanding and addressing the special needs of the disaster relief context.[1]

Broadly speaking, the report seeks to examine the legal and policy issues surrounding the information sharing needs of missing persons activities and to identify and discuss the privacy issues implicated by those activities as they exist today and as they might change in the future. More specifically, the objectives are to:

- Describe generally privacy issues relevant to missing persons information activities;
- Provide more detailed descriptions and analysis of legal requirements for privacy as they relate to missing persons activities for selected but representative jurisdictions; and

[1] For information about the Missing Persons Community of interest, see http://wiki.crisiscommons.org/wiki/Missing_Persons, accessed Jan.10, 2013.

- Offer options and strategies to missing persons organizations and privacy policy makers for the design, organization, location, and other features of missing persons information activities and for laws and policies regulating the privacy of missing persons information.

The report reflects the perspective that anticipation, cooperation, and adjustment can balance all interests involved and can achieve a reasonable, proportional, and appropriate result that will support human needs in disasters while respecting privacy objectives to the extent practicable under the circumstances surrounding natural disasters. This approach recognizes that sharing information about missing persons is a legitimate objective in emergency situations, that data protection laws should accommodate this objective, and that the emergency circumstances require special exceptions to privacy rules that are proportional to the circumstances, including appropriate safeguards, and that remain in place only as long as the emergency circumstances necessitate.

This report provides a roadmap to the intersection of privacy issues and missing persons activities in the context of natural disasters. In Part II, the report sets out generally the privacy issues that arise from missing persons activities and provides some real world examples of how privacy laws can affect disaster relief efforts. Part III describes a recent effort of several organizations to improve information sharing for missing persons activities and highlights the additional privacy issues implicated by such activities. In Part IV, the report identifies some key privacy principles and provides an analysis of how those principles affect missing persons information system activities. Finally, Part V provides a set of options and strategies for stakeholders to address some of the issues identified throughout the report.

II. Privacy Challenges in the Disaster Context

This section sets out the basic privacy challenges for the disaster context. It first discusses two key definitions that are critical to frame the scope of the issues that will be addressed in this report. The section then articulates basic privacy issues and how they are raised in the disaster context. The section finishes by providing a series of recent real world examples that demonstrate how those issues have played out in actual disaster experiences.

A. Key Definitions

The definitions of “missing person” and “natural disaster” are important for understanding the scope of this report and the privacy interests implicated by missing persons activities. These definitions also provide the reference points for applying any special privacy rules or policies.

1. Missing Person

The term *missing person* can mean different things depending on the context. The status of individuals included in a missing persons database may range from unknown, found, missing to some, or simply out of communication. The organizations in the MPCI use several different formulations. One set of specifications, for example, uses a data model that accepts “missing

persons" entries for persons "sought or found."[2] Thus, a person's whereabouts need not be entirely unknown for him or her to be in a missing persons database. The Red Cross *Safe and Well* database allows people to register themselves in the database as "safe and well," enabling concerned family and friends to search for that person in the database.[3] Under this formulation, a missing person could simply be an individual out of communication.

Definitions from other sources help identify the critical elements frequently used to classify an individual as missing and to clarify which missing persons should fall within the scope of this report. The International Committee of the Red Cross (ICRC), for example, defines missing persons in the context of man-made disasters, such as armed conflict, as "those whose whereabouts are unknown to their families and/or who, on the basis of reliable information, have been reported missing in connection with an international or non-international armed conflict, a situation of internal violence or disturbances or any other situation that may require the intervention of a neutral and independent intermediary."[4]

Other definitions exist for individuals who may be missing for reasons entirely unrelated to disaster, including criminal activity and voluntary departure. For example, a New Mexico statute defines a missing person as "a person whose whereabouts are unknown to the person's custodian or immediate family member and the circumstances of whose absence indicate that (1) the person did not leave the care and control of the custodian or immediate family member voluntarily and the taking of the person was not authorized by law; or (2) the person voluntarily left the care and control of the custodian without the custodian's consent and without intent to return."[5] This class of missing person may include a woman absent from home who may have been kidnapped or a teenager who may have run away from home. These various definitions indicate that the critical element for purpose of this report is that an individual's whereabouts are unknown to those ordinarily close to the individual during a crisis period.

This report does not make a distinction between missing persons and "found" persons. A missing persons information system may have no way to know if a person is missing or has been found by any or all who have an interest in the missing person. It may not be practical or meaningful for a missing persons information system to mark individuals as found or to remove their information. Information about an individual may need to remain in the system until disaster-related activities end, even if the person has been "found" by friends and family.

Finally, while in the legal context, a *person* includes natural persons, corporations, agencies, and other types of associations, this report uses the term solely to refer to a natural person or individual because corporations, agencies, and other legal persons cannot be missing in the same

---

[2] "People Finder Interchange Format 1.4 Specification;" "full_name field," Ka-Ping Yee, last modified May 29, 2012, http://zesty.ca/pfif/1.4/.

[3] "American Red Cross Safe and Well," accessed Aug. 7, 2011, https://safeandwell.communityos.org/cms/index.php.

[4] Int'l Comm. of the Red Cross [ICRC], *Missing Persons and Their Families: Recommendations for Drafting National Legislation* 1 (Oct. 2003), http://www.icrc.org/eng/assets/files/other/missing_and_recommendations_missing.pdf.

[5] Missing Persons Information and Reporting Act, N.M. Stat. Ann. § 29-15-2 (2010), http://www.conwaygreene.com/nmsu/lpext.dll?f=FifLink&t=document-frame.htm&l=query&iid=6b5281ff.52f15c16.0.0&q=%5BGroup%20%2729-15-2%27%5D.

way that an individual might be. While a more precise term for this report would be *missing individual*, the phrase *missing persons* is too well-established to change.

For the general purposes of this report, therefore, a missing person is someone not in contact with his or her family and friends due to a natural disaster.

2. Disaster

Within the disaster relief community, no universal definition of disaster exists. The United Nations International Strategy for Disaster Reduction defines a disaster as a "serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources."[6] The International Federation of Red Cross and Red Crescent Societies have a similar definition, adding that a disaster may develop suddenly or because of long-term processes.[7]

The Stafford Act, the law governing most US Federal Emergency Management Agency (FEMA) programs, defines a major disaster as any natural catastrophe (e.g., hurricane, tornado, or storm), or any fire, flood, or explosion in the United States that the President determines to have caused damage of sufficient severity and magnitude to warrant major disaster assistance.[8] The President of the United States must declare a "major disaster" to activate federal disaster assistance from FEMA.

The International Federation of Red Cross and Red Crescent Societies identifies three classifications of disasters: natural disasters, natural hazards increased by humans, and disasters directly caused by humans. Natural disasters are tropical storms, floods, earthquakes, tsunamis, and the like. Natural hazards increased by humans are disasters arising from natural hazards that would not have occurred or would have been substantially mitigated if not for certain human actions. Some examples are deforestation that results in a landslide during heavy rainfall, and unnecessary tsunami and storm damage resulting from excessive building near beaches. Examples of disasters directly caused by humans are armed conflict and industrial events, such as explosions.[9]

While organizations involved in disaster response or missing persons activities typically have their own definitions of "disaster," the various definitions contain three core elements: (1) serious disruption of functioning of society. (2) threatened or actual significant harm, and (3) the

---

[6] United Nations Int'l Strategy for Disaster Reduction, Terminology on DRR (Disaster Risk Reduction), s.v. "Disaster," last modified Aug. 30, 2007, http://www.unisdr.org/we/inform/terminology#letter-d.

[7] Int'l Disaster Response Laws, Rules & Principles Programme [IDRL], Int'l Fed'n of Red Cross & Red Crescent Societies, *Introduction to the Guidelines for the Domestic Facilitation and Regulation of Int'l Disaster Relief and Initial Recovery Assistance* 14 (2011), *available at* http://www.ifrc.org/PageFiles/41203/1205600-IDRL%20Guidelines-EN-LR%20%282%29.pdf.

[8] 42 U.S.C. § 5122 (2006), *available at* http://www.law.cornell.edu/uscode/text/42/5122.

[9] Johns Hopkins Bloomberg Sch. of Pub. Health & Int'l Fed'n of Red Cross & Red Crescent Societies, *Johns Hopkins and Red Cross Red Crescent Public Health Guide in Emergencies* 26-27 (2d ed. 2008), *available at* http://www.jhsph.edu/refugee/publications_tools/publications/_CRDR_ICRC_Public_Health_Guide_Book/Chapter_1_Disaster_Definitions.pdf.

insufficiency of local capacity to respond, thereby requiring outside assistance. The missing persons activities within the scope of this report result from natural disasters that meet these three criteria.

B. Basic Privacy Risks and Issues for Missing Persons Activities

Privacy is not a new issue to many engaged in missing persons activities. For example, in the context of armed conflict or internal national violence, the ICRC conducted an electronic workshop on *The Legal Protection of Personal Data & Human Remains* in 2002.[10] The ICRC also has and is currently revising a set of *Guidelines on Protection in Violent Situations: Standards for Managing Sensitive Information*.[11] This effort seeks to "draft the basic principles to be followed in any situation and by all the entities concerned"[12] in armed conflict situations. Missing persons following natural disasters, however, raise context-specific issues and needs.

After a natural disaster, people can be identified as missing for a number of reasons. For example, disasters injure or kill some people, while others flee to neighboring countries. Similarly, evacuation procedures may separate families and tourists who arrive just before a disaster strikes causing them to be hard to trace. Often a natural disaster is accompanied by outages in communication technologies making it difficult for people located in a disaster area to find each other or to communicate with their relatives, friends, and acquaintances outside of the affected area.

As people are identified as missing, there is an urgent demand to find them that often leads to substantial information sharing. People affected by a disaster often attempt to contact and reconnect with friends and family and may share information about themselves through multiple sources located in different jurisdictions. Friends and family outside of the region may simultaneously search for information about their missing relatives by providing personal information about the missing persons to multiple organizations or online communities in order to inquire about their status. Similarly, humanitarian organizations aiding with disaster relief may supply personal information about the people they assist to members of the public in order to help reconnect victims with family and friends. It is a basic human response in an emergency to seek to communicate with loved ones, and unrestricted information sharing is often a natural way to address the information deficit that accompanies a missing status.

Much of this information sharing is valuable but it often raises new and complex privacy risks because a natural disaster creates unpredictable and unexpected information sharing. Privacy

---

[10] The final report of the workshop is available at http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf. Unlike the ICRC effort, this report does not address identification of human remains because that is not an activity of the Missing Persons Community of Interest. For other relevant ICRC documents, see Int'l Comm. of the Red Cross [ICRC], *The Missing and Their Families: Documents of Reference* (Feb. 2004), *available at* http://www.icrc.org/eng/assets/files/other/icrc_002_0857.pdf.

[11] http://www.icrc.org/eng/assets/files/other/icrc_002_0999.pdf.

[12] Int'l Comm .of the Red Cross [ICRC] Electronic Workshop on the Legal Protection of Personal Data & Human Remains, Apr. 2-May 6, 2002, *The Legal Protection of Personal Data & Human Remains: Final Report and Outcome* 6 (July 2002), *available at* http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf.

risks will often be specific to the circumstances of the disaster. Well-intentioned or innocuous sharing for one purpose related to a missing person may create risks or dangers in another context.

For example, a local resident concerned about the possibility of domestic violence may find that carefully guarded information about her location is no longer under her control because official and missing persons databases include her location information in public or unprotected systems. A foreign worker displaced by a disaster may fear that the sharing of information about his new circumstances may affect his right to work or reside. A refugee from a natural disaster may worry that her ability to remain in a new location may be affected if the local government becomes aware of her presence. A political dissident may be concerned that her location is now available to a government or an enemy. Health or financial information might simply be accessible more broadly than would otherwise be the case. An individual may find that his or her confidential health information is shared with family members as part of a missing person identification process. Genetic information used for identification could pass beyond the control of an individual and family. A hospitalized tourist may find his medical information shared in places that he never anticipated.

Other risks emerge from the retention of information by various third parties or from the incorporation of missing persons data in other unrelated databases through happenstance or aggressive data collection by commercial or government entities or through expansive processing by law enforcement. A government agency may decide that an individual's new circumstance adversely affects the individual's right, privileges, or benefits. A bank learning of the effect of a disaster on an individual may demand immediate payment of a loan. A business traveler may find that confidential travel arrangements are now public.

At the same time, legal restrictions similarly pose complex challenges. First, the privacy laws of affected countries may place restrictions on information processing, including data collection and data sharing, that are likely to be challenging following natural disasters. Privacy laws often regulate how organizations may collect, use and share information. For example, many laws require that the data collector gives notice of collection and obtains consent from the data subject before processing or sharing information. When communications systems are down and people are missing, notice and consent is often not practicable or not possible. Complying with a notice and consent requirement would effectively limit many missing persons activities. Similarly, many privacy laws limit the purposes for which information may be shared with third parties without consent of the data subject and often missing persons activities do not fit neatly into any of the permissible purposes. Again the default privacy rules may create a barrier to desirable missing persons information functions.

Second, information sharing may simultaneously implicate the laws of various countries making legal compliance a challenge. Disasters often affect multiple national jurisdictions and require the consideration of multiple legal regimes. For example, people may leave disaster areas, moving to jurisdictions not directly affected by the disaster and those with an interest in learning the status of missing persons may live anywhere in the world. Similarly, independent organizations and agencies involved in assisting or locating missing persons may be located in multiple countries and maintain missing persons information in separate information systems

meaning that records about missing persons may be held almost anywhere. Each entity involved may be subject to its own national privacy laws or, perhaps, to no law at all. Information shared among organizations will likely flow across international borders, raising complex questions about the rules governing data exports. Similarly, as people affected by a disaster attempt to contact and reconnect with friends and family, they may share information through multiple sources located in different jurisdictions. Disaster-related activities and the data flows that result cross many jurisdictional borders, often in unanticipated ways.

Finally, information processing following natural disasters is time-sensitive, upsetting established policies and practices. Missing persons data processing generates new types of data, new demands for data, and urgency not always present in routine processing. The unpredictability and immediacy of a natural disaster may make it impossible to rely on tools or procedures commonly used in the processing of personal information that balance privacy interests against competing concerns. For example, traditional notions of notice and consent for information sharing are unlikely to work. Urgency also may prevent the use of proper analysis of privacy implications through privacy impact assessments or other methods.

The privacy concerns implicated by missing persons activities are multifaceted. Information processors must consider the national laws of multiple jurisdictions as well as complicated issues of personal security and safety while acting under urgent time constraints.

C. Recent Real World Examples

Several recent natural disasters around the world illustrate the interplay between missing persons information processing and privacy laws. Australia, New Zealand, and the United States each encountered well-documented challenges under their privacy laws when responding to the needs of missing persons activities caused by a tsunami, earthquake, and hurricane respectively. In each case, privacy laws raised issues or created barriers with respect to efforts to share critical information in order to provide emergency services to those affected by the disaster. In each case, the government and humanitarian organizations involved in disaster relief believed that some modification of the law or clearer guidance was necessary to ensure that relief efforts could continue effectively. This Part reports on these experiences and the trade-offs adopted.

1. Australia

Australia may have been the first country to formally address privacy issues arising from natural disasters and emergencies. The 2002 Bali bombing and the 2004 Boxing Day tsunamis demonstrated the obstacles created by privacy laws and the need for remedial measures.

On October 12, 2002, terrorists bombed a nightclub area in the tourist island of Bali, killing approximately 202 people, mostly tourists. The victims hailed from 21 countries, with the greatest number from Australia.[13] Efforts by government agencies and humanitarian

[13] "Bali Death Toll Set at 202," *BBC News*, last modified Feb. 19, 2003, http://news.bbc.co.uk/2/hi/asia-pacific/2778923.stm.

organizations to share information about victims encountered obstacles under Australia's Privacy Act.

During a post-crisis review of the Australian Privacy Act, the Australian Red Cross (ARC) told the Senate Legal and Constitutional References Committee that the Act "imposed significant impediments" to its relief efforts, particularly in distributing assistance to the Australian victims. Notwithstanding the close liaison between ARC and Department of Foreign Affairs and Trade (DFAT), the Australian Privacy Act prevented ARC from accessing lists of deceased, injured, and missing people held by DFAT. Instead, the ARC had to develop its own list of deceased and injured by compiling data from a multitude of sources, including advertisements, media, web searches, word of mouth, and referrals.

Under Australian law, the ARC could not share its own lists of deceased and injured people with some state and territory governments that requested them. Some victims registered on ARC's computerized victim registration and inquiry system could not give permission for the sharing of their information due to the severity of their injuries. Other victims needed to consent to the sharing of basic information about assistance provided.[14] As Robert Tickner, Secretary General of the ARC, later told a Senate Committee, traumatized people with moderate to severe injuries had to tell their story again and again to different relief agencies, undoubtedly compounding their stress levels.[15]

Two years later on December 26, 2004, an undersea earthquake triggered multiple tsunamis along the coasts of countries bordering the Indian Ocean, killing over 225,000 people in 11 countries. Following the tsunamis, DFAT received over 87,000 phone calls from Australians concerned about the whereabouts of family members and friends. DFAT developed a list of 14,000 Australians who may have been in the area the tsunamis affected.

Privacy restrictions made it more complicated to track down these individuals to confirm their status. Specifically, the Australian Privacy Act limited information sharing between DFAT and private sector organizations. For example, because of the Act, airlines and travel agents were unable to disclose personal information to DFAT.[16] The Federal Privacy Commissioner acknowledged that the disclosures by airlines to families and friends reporting whether missing people boarded planes after the tsunamis hit "would normally appear to be a breach" of National Privacy Principle 2. Although National Privacy Principle 2 contains health and safety exceptions,

---

[14] Submission to Senate Legal and Constitutional References Committee, Parliament of Australia, Canberra, 2005, 2 (Australian Red Cross), http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/privacy/submissions/sub44.pdf.

[15] Cth, Parliamentary Debates, Senate, 22 Apr. 2005, 30-31 (Austl.), *available at* http://parlinfo.aph.gov.au/parlInfo/download/committees/commsen/8219/toc_pdf/3832-2.pdf.

[16] Submission to Senate Legal and Constitutional References Committee, Parliament of Australia, Canberra, 8 Mar. 2005, 6 (Department of Foreign Affairs and Trade), http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/privacy/submissions/sub39.pdf.

the Commissioner's interpretation suggests that the exceptions were not sufficient to permit information sharing following the natural disaster.[17]

For the most part, the Australian Privacy Act did not allow DFAT to automatically share information on victims in an overseas disaster with other government agencies helping the individuals.[18] DFAT noted in a submission to a Senate Committee that information sharing between government agencies was generally good, with the caveat that information sharing was not always as quick as would have been optimal due to the need to confirm that the Act authorized the information sharing in question.[19] For example, the Act impeded DFAT's ability to share personal information with government agencies such as Centrelink, which sought to avoid canceling regular social security payments to victims or pursuing victims for overdue payments.[20]

In 2005, a Committee of the Australian Senate conducted a broad inquiry into the effectiveness of Australia's Privacy Act in protecting privacy. The inquiry included a review of the Act's effect on responses to overseas emergencies. The Senate Committee acknowledged the concerns that ARC and DFAT had raised and urged the government to implement the Office of the Privacy Commissioner's recommendations.[21]

The following year, the Australian Parliament amended the Australian Privacy Act to address the practical issues that arise in disaster situations.[22] The amendment inserted Part VIA into the Act to make special provisions for the collection, use, and disclosure of personal information following an emergency or disaster.[23] Part VIA authorizes the government to make an emergency declaration that allows sharing of information otherwise restricted under the Act.[24] Events in Australia or overseas could trigger an emergency declaration, which takes effect immediately.[25] The declaration ceases to have effect at the earliest of three dates: (1) the end date

---

[17] Office of the Privacy Comm'r, Australia, Getting in On the Act: The Review of the Private Sector Provisions of the Privacy Act 1988, at 234 (2005).
[18] Submission to Senate Legal and Constitutional References Committee, Parliament of Australia, Canberra, 8 Mar. 2005, 6 (Department of Foreign Affairs and Trade), http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/privacy/submissions/sub39.pdf.
[19] Cth, Parliamentary Debates, Senate, 20 May 2005, 4 (Rod Smith, First Assistant Secretary, Public Diplomacy, Consular and Passports Div., Department of Foreign Affairs and Trade) (Austl.), *available at* http://parlinfo.aph.gov.au/parlInfo/download/committees/commsen/8383/toc_pdf/3913-2.pdf.
[20] Submission to Senate Legal and Constitutional References Committee, Parliament of Australia, Canberra, 8 Mar. 2005, 6 (Department of Foreign Affairs and Trade), http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/privacy/submissions/sub39.pdf.
[21] Senate Legal and Constitutional References Committee, Parliament of Australia, The Real Big Brother: Inquiry Into the Privacy Act 1988, at 160 (2005), *available at* http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/privacy/report/report.pdf.
[22] Revised Explanatory Memorandum, *H.R. Privacy Legis. Amendment (Emergencies and Disasters) Bill 2006* (Cth) 1 (Austl.), *available at* http://www.austlii.edu.au/au/legis/cth/bill_em/plaadb2006523/memo_0.html.
[23] *Privacy Act 1988* (Cth) s 80F (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.
[24] *Privacy Act 1988* (Cth) ss 80J, 80K (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.
[25] Prior to the amendment, the Privacy Act granted the Privacy Commissioner power to make an urgent temporary public interest determination (TPID) if the public interest in a disclosure breaching the Act clearly outweighs the

specified in the declaration, (2) the revocation of the declaration, or (3) twelve months after issuance of the declaration. While an emergency declaration is in effect, the collection, use, or disclosure of personal information authorized in Part VIA does not breach the Privacy Act's Information Privacy Principles, approved privacy codes, or National Privacy Principles.[26]

When an emergency declaration is in force subsequent to a disaster, an entity has the authority to collect, use or disclose personal information[27] relating to an individual if (1) the entity reasonably believes that the individual may be involved in the disaster; and (2) the collection, use or disclosure of personal information is for a *permitted purpose*[28] related to the disaster. The disclosure authority does not allow disclosures to media organizations. The authority to disclose is more permissive for government agencies than for other organizations or persons. If the entity making a disclosure is an agency, the disclosure must be to an agency, a State or Territory authority, an organization, an entity that is otherwise involved in managing or assisting in management of the disaster, or to a person responsible for the individual.[29] On the other hand, if the entity making a disclosure is an organization or another person, the disclosure must be to an agency, an entity *directly* involved in providing humanitarian disaster relief services to affected individuals, a person or entity prescribed by the regulations, or a person or entity specified by the Minister or a legislative instrument.[30]

2. New Zealand

On February 22, 2011, a 6.3 magnitude earthquake struck Christchurch, New Zealand's second largest city. [31] It caused an estimated $25 billion in widespread damage, killed 185 people, and injured thousands more.[32] The earthquake destroyed thousands of homes[33] and broke or damaged

---

public interest in adherence to the Act. An agency or organization must initiate a TPID, making it insufficient for handling a large-scale disaster that requires a quicker response.. (Cth) ss 80A, 80B (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.

[26] *Privacy Act 1988* (Cth) s 80P (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.

[27] For the purposes of Part VIA of the Privacy Act, personal information relates to both living and deceased individuals.

[28] A *permitted purpose* is a purpose directly relating to the government response to the disaster for which the emergency declaration is in force. Permitted purposes include, but are not limited to, the identification and assistance of individuals who may be affected, assisting law enforcement, coordinating, or managing the disaster, and ensuring people responsible for affected individuals are appropriately informed of matters relevant to: the individuals' involvement in the disaster or disaster response as to these individuals. *Privacy Act 1988* (Cth) s 80H (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.

[29] A person is responsible for an individual if they are a parent, a child or sibling at least 18 years old, a spouse or de facto partner, a relative at least 18 years old and a member of the individual's household, a guardian, a person with a power of attorney exercisable in relation to health decisions, a person who has an intimate personal relationship with the individual, or a person the individual nominated as an emergency contact. *Privacy Act 1988* (Cth) sch 3(2.5) (Austl.).

[30] *Privacy Act 1988* (Cth) s 80P (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414.

[31] "New Zealand Earthquake Report-Feb 22 2011 at 12:51 pm (NZDT)," Geonet, last modified Feb. 22, 2011, http://www.geonet.org.nz/earthquake/quakes/3468575g.html.

[32] "Christchurch earthquake-22 February 2011," Christchurch City Libraries, accessed June 12, 2012, http://christchurchcitylibraries.com/Kids/NZDisasters/Canterbury-Earthquakes/22-February-2011/.

[33] Nick Perry, The Associated Press, "Christchurch Earthquake 2011: New Zealanders Hold Memorial for 185 Killed in Devastating Temblor," *Huffington Post*, Feb. 21, 2012, http://www.huffingtonpost.com/2012/02/22/christchurch-earthquake-memorial_n_1292755.html.

water pipes, roads, bridges, power lines, cell phone towers, and landlines.[34] Phone lines and roads became jammed as confused and panicked people raced to contact their loved ones and return home.[35] The government immediately activated its National Crisis Management Centre and declared a national state of emergency the next day.[36]

New Zealand law provides comprehensive privacy protections that would have impeded necessary information sharing regarding missing persons during the disaster relief efforts. New Zealand's Privacy Act contains twelve Information Privacy Principles[37] governing the collection, use, storage, and disclosure of personal information by *agencies*[38] (public or private organizations and individuals). Generally, these principles require (1) that an agency collect personal information directly from the individual; (2) that personal information obtained for one purpose not be used for any other purpose; and (3) that personal information not be disclosed to a third party without consent or for one of the purposes for which the information was obtained.[39]

The Privacy Act did provide exceptions to these restrictions (a) when disclosure is necessary to prevent or mitigate a "serious and imminent threat" to public health or public safety, or the life or health of the individual concerned;[40] (b) when an organization has consent from the individual;[41] and (c) when the disclosure directly relates to one of the purposes for which the information was collected.[42] However, it was unclear whether these exceptions would apply to all necessary information sharing and therefore agencies were hesitant to rely upon them.

The New Zealand Privacy Commissioner, aware of the legal barriers that others had encountered in large-scale disasters such as the Boxing Day tsunamis, acted swiftly and within 24 hours of the emergency declaration issued a temporary information sharing code to assist in the relief effort.[43] The temporary code, issued under statutory interpretive powers granted to the Privacy Commissioner, provided greater certainty and gave broader discretion to emergency services and

---

[34] "Christchurch earthquake-22 February 2011," Christchurch City Libraries, accessed June 12, 2012, http://christchurchcitylibraries.com/Kids/NZDisasters/Canterbury-Earthquakes/22-February-2011/.
[35] "Christchurch earthquake-22 February 2011," Christchurch City Libraries, accessed June 12, 2012, http://christchurchcitylibraries.com/Kids/NZDisasters/Canterbury-Earthquakes/22-February-2011/.
[36] [2011] 670 NZPD 16948 (N.Z.), *available at* http://www.parliament.nz/en-NZ/PB/Debates/Debates/0/a/d/49HansD_20110223_00000064-Ministerial-Statements-Earthquake-Christchurch.htm. (John Carter, Minister of Civil Defence, *Ministerial Statement*, Feb. 23, 2011).
[37] Privacy Act 1993, § 6 Information Privacy Principles (N.Z.), *available at* http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html.
[38] Privacy Act 1993, §2(1) (N.Z.), *available at* http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296645.html.
[39] Privacy Act 1993, § 6 Information Privacy Principles (N.Z.), *available at* http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html.
[40] Privacy Act 1993, § 6: Information Privacy Principle 11(f) (N.Z.), *available at* http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM297038.html.
[41] Privacy Act 1993, § 6: Information Privacy Principle 11(c) (N.Z.), *available at* http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.
[42] Privacy Act 1993, § 6: Information Privacy Principle 11(a) (N.Z.), *available at* http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.
[43] New Zealand Privacy Comm'r, Proposed Civil Defence National Emergencies (Information Sharing) Code (information paper), *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Information-paper-National-Emergencies-Information-Sharing-Code-April-2012.doc.

government agencies responding to and managing the disaster.[44] Because of the cultural and privacy law similarities of Australia and New Zealand, the Commissioner modeled the Christchurch Code closely on the amendment the Australian Parliament made to the Australian Privacy Act after the Boxing Day tsunamis.[45]

The temporary code authorized agencies in certain circumstances to collect, use or disclose personal information for *permitted purposes*, purposes directly related to the government response to the Christchurch earthquake emergency.[46] The permitted purposes included identifying individuals injured, missing, or dead; assisting individuals to obtain repatriation services, medical treatment, financial and humanitarian aid, and other services; assisting law enforcement; coordinating and managing the emergency; and providing information to people responsible for affected individuals.[47] The code enumerated eight specific categories in which a person would be considered responsible for an individual.[48]

As initially promulgated, the temporary code expired on the earlier of two dates: May 24, which was three months after the temporary code's issuance, or on the date, which the national emergency declaration terminated.[49] The Privacy Commissioner made two separate amendments

[44] Letter from Marie Shroff, New Zealand Privacy Comm'r, to Hon Charles Chauvel, MP, Chair of the Regulations Review Committee, Mar. 2, 2011, http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Letter-to-Chair-of-Regulations-Review-Committee-2-03-11.doc.

[45] Letter from Marie Shroff, New Zealand Privacy Comm'r, to Hon Charles Chauvel, MP, Chair of the Regulations Review Committee, Mar. 2, 2011, http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Letter-to-Chair-of-Regulations-Review-Committee-2-03-11.doc.

[46] Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Feb. 24, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-incorporating-Amendments-No-1-and-No-2.doc. This authorization applied if the agency believed on reasonable grounds that (a) the individual concerned may be involved in the emergency; and (b) the collection, use, or disclosure is for a permitted purpose in relation to the emergency; and the disclosure is to a public sector agency; to an agency that is or is likely to be involved in managing or assisting in the management of the emergency; to an agency directly involved in providing repatriation services, treatment, health services or financial or other humanitarian assistance services to affected individuals; or to a person **responsible** for the individual. The temporary code provided that the broader disclosure authority for personal information did not cover disclosures to a news medium. *Id.*

[47] Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Feb. 24, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-incorporating-Amendments-No-1-and-No-2.doc.

[48] According to the Code, a person is responsible for an individual if the person is (a) a parent of the individual; (b) a child or sibling of the individual and at least 18 years old; (c) a spouse, civil union partner or de facto partner of the individual; (d) a relative of the individual, at least 18 years old and a member of the individual's household; (e) a guardian of the individual; (f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; (g) a person who has an intimate personal relationship with the individual; or (h) a person nominated by the individual to be contacted in case of emergency. Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Feb. 24, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-incorporating-Amendments-No-1-and-No-2.doc.

[49] Letter from Marie Shroff, New Zealand Privacy Comm'r, to Hon Charles Chauvel, MP, Chair of the Regulations Review Committee, Mar. 10, 2011, http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Letter-to-Chair-of-Regulations-Review-Committee-10-03-11.doc.

adjusting the expiration date.[50] The first delinked the expiration of the code from the emergency declaration termination date, fixing May 24, 2011 as the expiration date for the temporary code.[51] A later amendment extended the life of the code by five weeks.[52]

In issuing the first amendment to delink the expiration of the code with the emergency declaration, the Privacy Commissioner realized that if the code were to expire on the same day as the emergency declaration, the result could be unduly disruptive. Termination of the emergency could occur without much advance notice, possibly affecting ongoing information sharing arrangements.[53] Tying the expiration of the code to a fixed date provided greater certainty.

The second amendment allowed several agencies, particularly government departments, more flexibility to transition away from reliance upon the temporary code.[54] The end of the state of national emergency by no means signaled the end of intensive government efforts in its response to the earthquake and in missing persons activities.

Shortly before the temporary code expired, the Privacy Commissioner sponsored a research report on the code's practical usefulness. The report found that some government agencies relied upon the code as a lawful basis for collection, use, and disclosure of information, and that government agencies felt reassured by the code to share information as necessary in the circumstances.[55]

The code turned out to be useful in a diverse range of situations. It was particularly helpful to the Ministry of Social Development (MSD), the government agency in New Zealand that had the most current contact details for individuals.[56] Without the code, MSD may not have had a legal basis for sharing client information with other government agencies to meet the needs of the

---

[50] Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Feb. 24, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-incorporating-Amendments-No-1-and-No-2.doc.

[51] Amendment of the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Mar. 9, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Amendment-No-1-to-the-Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-with-explanatory-note2.doc.

[52] Extension of the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), May 13, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Amendment-No-2-to-Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-with-explanatory-notes.doc.

[53] Amendment of the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Mar. 9, 2011, explanatory note, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Amendment-No-1-to-the-Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-with-explanatory-note2.doc.

[54] Letter from Marie Shroff, New Zealand Privacy Comm'r, to Hon Charles Chauvel, MP, Chair of the Regulations Review Committee, May 17, 2011, http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Letter-to-Chair-Regulations-Review-Committee-17-05-11.doc.

[55] New Zealand Privacy Comm'r, Proposed Civil Defence National Emergencies (Information Sharing) Code (information paper), *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Information-paper-National-Emergencies-Information-Sharing-Code-April-2012.doc.

[56] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 5, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

clients for repatriation, as well as for health, financial, and other services.[57] For example, MSD disclosed information to Housing New Zealand to assist with prioritizing emergency housing in particularly vulnerable or damaged areas.[58] MSD also assisted a medical alarm service provider in contacting some of its elderly medical alarm users after the earthquake damaged and destroyed many residential care facilities.[59]

The temporary code also provided a legal basis for disclosing student information.[60] The Ministry of Education provided information to the Red Cross and to Civil Defence on student movements.[61] The code also allowed sharing of information with the Minister of Education and foreign embassies regarding international students enrolled in the language school in the Canterbury Television building.[62]

Some Christchurch state rental tenants also benefited from the temporary code. The Housing New Zealand Corporation agreed to suspend rent payments for its tenants for three weeks to help alleviate hardship in the aftermath of the earthquake. The code provided legal authority for the Housing New Zealand Corporation to give tenant names and addresses to Work and Income, in order to facilitate rent suspensions by Work and Income.[63]

The code also facilitated case management of high-risk community-based offenders on probation. The Christchurch Recovery Department of Corrections shared information with agencies to locate offenders who could not be found at their usual addresses. This information

---

[57] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 4, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

[58] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 3, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

[59] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 6, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

[60] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 4, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf. Without the emergency Code, the disclosures made by the Ministry of Education would have breached Privacy Principle 11.

[61] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 2, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

[62] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice-—Questionnaire Results: Public Version, 9 May 2011, at 2, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf. The collapse of the Canterbury Television building accounted for 115 of the 185 fatalities caused by the Christchurch earthquake. Kurt Bayer, APNZ Service, "CTV Building Collapse Like 'War Zone,'" *New Zealand Herald* (Jun. 26, 2012, 8:00 PM), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10815547.

[63] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 3, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

sharing helped the effort to manage the risk of the offenders committing new offenses, and to monitor offenders' compliance with conditions of release.[64]

The code was useful not only for government agencies but for private sector agencies as well. For example, it allowed an airline to disclose to police, family members and friends whether individuals had flown into or out of Christchurch.[65]

Largely due to the success of the Christchurch temporary code, the Privacy Commissioner of New Zealand proposed the Civil Defence National Emergencies (Information Sharing) Code, a regime of provisions that would come into effect automatically when a state of national emergency is declared, lasting until the end of the state of emergency. The objective of the proposed Code is identical to that of the temporary Christchurch Code, namely to provide agencies with broader discretion to collect, use and disclose personal information following a major natural disaster, so as to promote the vital interests of individuals during disaster relief efforts.[66] The proposed Code would benefit New Zealanders in two ways that the Christchurch code could not. It would come into effect immediately upon the declaration of a state of national emergency, and government agencies could rely on it when planning for emergencies.

3. United States

On August 23, 2005, Hurricane Katrina struck New Orleans, causing mass flooding as the levee system failed. Floodwaters submerged much of the city. The scale and extent the destruction from Hurricane Katrina was unprecedented, with a total estimated damage of over $81 billion, and a death toll of over 1,464 people.[67] The hurricane destroyed 275,000 homes as well as telephone landlines, cell phone towers, bridges, and highways.[68]

The hurricane disrupted communication and transportation infrastructures throughout southeast Louisiana.[69] The flooding incapacitated nine of eleven hospitals in New Orleans,[70] leaving

---

[64] New Zealand Privacy Comm'r, Christchurch Earthquake Code of Practice—Questionnaire Results: Public Version, 9 May 2011, at 3-4, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Questionnaire-Results-Public.pdf.

[65] Katherine Gibson, "Large scale emergencies and personal information—can the Privacy Act cope?" (LLM post-graduate paper, University of Auckland, 2011), 19, http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Katherine-Gibson-paper-on-Earthquake-code-10-05-11.pdf. Unless a police request related to the investigation of an offense, Information Practice 11 would bar disclosure.

[66] New Zealand Privacy Comm'r, Proposed Civil Defence National Emergencies (Information Sharing) Code (information paper), *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Information-paper-National-Emergencies-Information-Sharing-Code-April-2012.doc.

[67] The official death toll of Hurricane Katrina is highly disputed. Lise Olsen, "5 years After Katrina, Storm's Death Toll Remains a Mystery," *Houston Chronicle*, Aug..31, 2010, *available at* http://www.chron.com/news/nation-world/article/5-years-after-Katrina-storm-s-death-toll-remains-1589464.php.

[68] David L. Johnson, U.S. Dep't of Commerce, Nat'l Oceanic and Atmospheric Admin. [NOAA], Nat'l Weather Serv. [NWS], Service Assessment: Hurricane Katrina Aug. 23-31, 2005, at 1 (2006), *available at* http://www.nws.noaa.gov/om/assessments/pdfs/Katrina.pdf

[69] David L. Johnson, U.S. Dep't of Commerce, Nat'l Oceanic and Atmospheric Admin. [NOAA], Nat'l Weather Serv. [NWS], Service Assessment: Hurricane Katrina Aug. 23-31, 2005, at 1 (2006), *available at* http://www.nws.noaa.gov/om/assessments/pdfs/Katrina.pdf.

National Disaster Medical System (NDMS) medical response teams as the main source of medical care for tens of thousands of displaced patients. NDMS worked out of a temporary hospital set up at the New Orleans airport, administering first aid, triaging victims, and moving them to health care facilities outside the flood zone. At its peak, NDMS processed approximately 15,000 patients per day.[71] The coordination of medical treatment and reimbursement of medical expenses became especially difficult as thousands of Katrina victims left the area without their health records and moved to other health care facilities in a wide area of the South Central United States.[72]

Under these circumstances, strict compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule became impractical. To facilitate the provision of health care, the Secretary of Health and Human Services (HHS) declared a public health emergency[73] in nine states that hosted evacuees in need of health care.[74] When the Secretary of HHS declares a Public Health Emergency in conjunction with a Presidential National Disaster Declaration, the Secretary may issue a Section 1135 Waiver.[75] This waives sanctions and penalties arising from noncompliance with the following provisions of the HIPAA privacy regulations:

1. The requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care (as set forth in 45 C.F.R. § 164.510[b]);
2. The requirement to honor a patient's request to opt out of the facility directory (as set forth in 45 C.F.R. § 164.510);
3. The requirement to distribute a notice of privacy practices (as set forth in 45 C.F.R. § 164.520);
4. The patient's right to request privacy restrictions (as set forth in 45 CFR § 164.522[a]); or
5. The patient's right to request confidential communications (as set forth in 45 C.F.R. § 164.522[b]).[76]

---

[70] Crystal Franco et. al., "Systemic Collapse: Medical Care in the Aftermath of Hurricane Katrina," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 4, no. 2 (2006): 135-146, *available at* http://online.liebertpub.com/doi/pdfplus/10.1089/bsp.2006.4.135.

[71] Crystal Franco et. al., "Systemic Collapse: Medical Care in the Aftermath of Hurricane Katrina," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 4, no. 2 (2006): 135-146, *available at* http://online.liebertpub.com/doi/pdfplus/10.1089/bsp.2006.4.135.

[72] Sarah A. Lister, Cong. Research Serv., RL 33096, Hurricane Katrina: The Public Health and Medical Response 11 (2005), *available at* http://fpc.state.gov/documents/organization/54255.pdf.

[73] U.S. Dep't of Health and Human Servs, HHS Declares Public Health Emergency for Hurricane Katrina: Waiver Under Section 1135 of the Social Security Act (2005), *available at* http://www.hhs.gov/katrina/ssawaiver.html.

[74] Sarah A. Lister, Cong. Research Serv., RL 33096, Hurricane Katrina: The Public Health and Medical Response 11 (2005), *available at* http://fpc.state.gov/documents/organization/54255.pdf.

[75] The authority to waive some legal requirements comes from 42 U.S.C. § 1320b-5, and the Secretary responded to Katrina by waiving provisions of other laws in addition to HIPAA.

[76] "Is the HIPAA Privacy Rule Suspended During a National or Public Health Emergency?," U.S. Dep't of Health and Human Servs., accessed June 12, 2012, http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_in_emergency_situations/1068.html.

The waiver had limitations. It remained in effect "for a period of time not to exceed 72 hours from implementation of a hospital disaster protocol." It applied only in the geographic area covered by the President's declaration of national disaster. It was not effective "with respect to any action taken thereunder that discriminates among individuals on the basis of their source of payment or their ability to pay," and it did not cover actions of fraud or abuse. [77]

The HIPAA waiver for Hurricane Katrina is another example of an accommodation made in response to a natural disaster that affects implementation of an existing privacy law.

[77] "Is the HIPAA Privacy Rule Suspended During a National or Public Health Emergency?," US Dep't of Health and Human Servs., accessed June 12, 2012, http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_in_emergency_situations/1068.html.

Box 1. Proposed Canadian Amendment to PIPEDA

In Canada, the Privacy Act governs the collection, use, and disclosure of personal information for federal government institutions,[78] while the Personal Information Protection and Electronic Documents Act (PIPEDA) applies to private sector organizations.[79] Both laws are relevant to disaster-related information processing.

Following the 2004 Boxing Day tsunamis, Prime Minister Paul Martin and officials of the Department of Foreign Affairs and International Trade cited Canada's Privacy Act as the basis for refusing to release the names of 146 Canadians who were either missing or dead as a result of the tsunamis.[80] Jennifer Stoddard, Privacy Commissioner of Canada, clarified that such a disclosure would fall within the public interest exception contained in the Privacy Act.[81] According to the Act, a disclosure is allowed when the public interest in disclosure outweighs any resulting invasion of privacy, or when it would clearly benefit the individual whom the information concerns.[82]

The authority to disclose personal information is less broad for private sector organizations. For the most part, PIPEDA requires the knowledge and consent of the individual for collection, use, and disclosure of personal information.[83] Disclosure is permitted without consent under some circumstances, including where "made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure."[84] Whether this language is broad enough to address all emergency disclosures is uncertain.

An amendment proposed in 2011 would change the PIPEDA exception. Under the amendment, disclosure of personal information would be permitted for the "purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual"[85] or if "necessary to identify the individual who is injured, ill or deceased, the disclosure is made to a government institution, a part of a government institution or the individuals' next of kin or authorized representative."[86]

While still a proposal, the amendment illustrates that the need to reconsider elements of privacy restrictions to accommodate emergency circumstances continues to gain recognition around the world.

---

[78] Privacy Act, R.S.C. 1985, c. P-21, s 2 (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/P-21.pdf.
[79] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, s 4 (Can.), *available at* http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-2.html.
[80] David Fraser, "Commissioner Speaks Up on Interpretation of the Privacy Act and Naming Tsunami Victims," *Canadian Privacy Law Blog*, Jan. 6, 2005, http://blog.privacylawyer.ca/2005/01/commissioner-speaks-up-on.html.
[81] David Fraser, "Commissioner Speaks Up on Interpretation of the Privacy Act and Naming Tsunami Victims," *Canadian Privacy Law Blog*, Jan. 6, 2005, http://blog.privacylawyer.ca/2005/01/commissioner-speaks-up-on.html.
[82] Privacy Act, R.S.C. 1985, c. P-21, s 8(2)(m) (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/P-21.pdf.
[83] Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, sch1(4.3) (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf.
[84] Personal Information Protection and Electronic Documents Act S.C. 2000, c.5, s 7(3)(e) (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf.
[85] Bill C-12, 41st Parl. (1st Sess. 2011) s 7(6)(iv) (Can.), *available at* http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5144601.
[86] Bill C-12, 41st Parl. (1st Sess. 2011) s 7(9)(d.3) (Can.), *available at* http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5144601.

D. The International Response to the Privacy Problem

In November 2011, the 33rd International Conference of Data Protection and Privacy Commissioners met in Mexico City, Mexico. The Commissioners represented countries from around the world. At the meeting, the Commissioners specifically examined how privacy laws can affect the sharing of personal information after a natural disaster and they adopted a resolution on data protection and major natural disasters.[87] The Privacy Commissioner of New Zealand proposed the resolution with the co-sponsorship of several other privacy commissioners.

The resolution included a statement that data protection and privacy laws:

- Limit the permissible purposes for disclosure of personal information held by organizations; but
- Allow the disclosure of information in certain exceptional circumstances, although such exceptions are often narrowly drawn.

The resolution "encouraged" action by data protection authorities, government, and international organizations.[88] Specifically, the resolution called on data protection authorities to review whether their domestic data protection and privacy laws are suitably framed and flexible to best serve the vital interests of individuals in the event of a major natural disaster and, if warranted, to recommend reform.[89]

---

[87] International Conference of Data Protection and Privacy Commissioners, Mexico City, Mex., Nov. 2-3, 2011, *Resolution on Data Protection and Major Natural Disasters*, 2011/GA/RES/004 (Nov. 1, 2011), *available at* http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_004_Natural_Disasters_ENG.pdf.

[88] International Conference of Data Protection and Privacy Commissioners, Mexico City, Mex., Nov. 2-3, 2011, *Resolution on Data Protection and Major Natural Disasters*, 2011/GA/RES/004 (Nov. 1, 2011), *available at* http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_004_Natural_Disasters_ENG.pdf.

[89] International Conference of Data Protection and Privacy Commissioners, Mexico City, Mex., Nov. 2-3, 2011, *Resolution on Data Protection and Major Natural Disasters*, 2011/GA/RES/004 (Nov. 1, 2011), *available at* http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_004_Natural_Disasters_ENG.pdf.

The resolution also called on data protection authorities to periodically check their own preparations and consider whether they need take further administrative steps to be best able to serve their communities in advance of, or following, a major natural disaster; and, to provide advance guidance to their communities about the operation of data privacy law in natural disasters, including, in particular, aspects that will assist in ensuring effective public responses.

The Commissioners further called on governments to consider the data protection and personal information handling issues in their civil defense planning, including taking steps to ensure that public bodies are aware of provisions of data privacy laws that facilitate prompt and secure sharing of personal information essential to disaster response; to have effective information protection and recovery plans for public services that will be vital in the first responses to a disaster; to meet the needs of families to learn the fate of missing relatives; to ensure that any special measures that may limit the normal operation of data protection law are appropriately justified, proportional to the emergency, contain appropriate safeguards and endure only for so long as warranted by the disaster; and to continue to respect the privacy and dignity of disaster victims, survivors, and their families. The Commissioners asked that international organizations consider the issues arising from major natural disasters in their reviews of the international instruments on privacy and data protection.

The resolution of the Data Protection Commissioners illustrates that the international community is beginning to recognize that privacy laws can affect the use and sharing of personal information following natural disasters, that natural disasters create new demands for the processing of personal information and that data protection laws must be "flexible to best serve the vital interests of individuals following a natural disaster."[90]

III. Existing Programs to Promote Information Sharing

In the wake of natural disasters, organizations and volunteers process missing persons information, often using varying information sharing protocols. At the same time, there is great diversity among the organizations and companies involved in missing persons activities following natural disasters. The entities involved are geographically dispersed and range from humanitarian nongovernmental organizations (NGOs) to for-profit technology companies. While most of these groups began their efforts independently of one another, they recognized after the 2010 Haiti earthquake the critical importance of data sharing for missing persons activities. During that disaster, the posting of information about missing persons in so many different places online presented a significant obstacle to connecting people.[91] In response to that experience, an independent community of humanitarian organizations, companies, and volunteers came together to form the MPCI.

This section describes the MPCI, its current activities and then maps out the members' existing programs, and discusses how the design of these new information sharing systems raises additional privacy considerations.

A. The MPCI and Its Members' Roles

The MCPI formed to coordinate information sharing and cooperation among organizations and volunteers in order to improve information systems that assist in reuniting family and friends. The MPCI functions as an open forum to foster dialogue, education, and relationship building for the development of community technical standards. Participating organizations currently include:

- American Red Cross
- Casques Rouges
- Crisis Commons
- Facebook, Inc.
- Google, Inc.

[90] International Conference of Data Protection and Privacy Commissioners, Mexico City, Mex., Nov. 2-3, 2011, *Resolution on Data Protection and Major Natural Disasters*, 2011/GA/RES/004 (Nov. 1, 2011), *available at* http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_004_Natural_Disasters_ENG.pdf.

[91] Christopher P. Csikszentmihalyi, "Information on Haiti Is Getting Siloed," *Pogue's Posts* (blog), *New York Times*, Jan. 17, 2010, http://pogue.blogs.nytimes.com/2010/01/17/information-on-haiti-is-getting-siloed/.

- ICRC
- Sahana Software Foundation
- US National Library of Medicine

The MPCI focuses primarily on online systems for people missing because of natural disasters.[92] Participants in the MPCI include both those who develop design specifications for online information collection systems and those who develop and operate directly database systems.

Design specifications are prescriptive and tell database administrators how to construct a missing persons information sharing system, what data fields should be included, the contents of those fields, and other technical specifications. MPCI participants who develop design specifications include the Organization for the Advancement of Structured Information Standards (OASIS), the Sahana Software Foundation, and Ka-Ping Yee, editor of a key protocol who is currently an engineer with Google.[93]

Database systems and software, on the other hand, are instances of missing persons information sharing systems maintained or developed by particular individuals or institutions. Any specific database system may or may not adhere to a known design specification. MPCI participants who develop or operate data systems include Google, the American Red Cross, the ICRC, the US National Library of Medicine, the Sahana Software Foundation and the Red Helmets Foundation (in partnership with Bearstech and European Consulting Services).

1. Design Specifications

A major part of the MPCI's efforts center on determining the main components for technical specifications that would enable all member organizations to participate in some level of information sharing. Two leading standards are currently in use and efforts are underway to negotiate a possible integration of the two standards to improve interoperability.[94] Each standard is designed to be a universal format for missing persons databases that would simplify the automated processing of missing persons information and enable MPCI member systems to share missing person records. The utility of data standardization is analogous to the utility of language standardization. When a community speaks the same language, it reduces transaction costs associated with sharing and communicating.

---

[92] The MPCI has not addressed other missing person situations, such as those missing due to armed conflicts, missing children, or refugees. The MPCI limits its current work to the challenge of natural disasters in order to place realistic bounds on its activities and to make it easier for cooperating member organizations to collaborate constructively. Once MPCI members have greater experience working together, the community may broaden its scope to include additional missing persons situations. Some organizations that participate in the MPCI process undertake missing persons activities for circumstances other than natural disasters.

[93] Ka-Ping Yee (username "kpy") also assists in the development of Person Finder. *See* "Google Person Finder Project," accessed July 23, 2012, https://code.google.com/u/kpy@google.com/.

[94] Discussions between Ka-Ping Yee, developer of PFIF, and Glenn Pearson, member of the steering group responsible for the development of the new revision of the EDXL standard. See "PFIF v. EDXL," Google Groups: PFIF, last modified Jan. 9, 2012, https://groups.google.com/d/topic/pfif/y0YhV5gjM18/discussion.

Specifically, the MPCI has encouraged the development of the People Finder Information Format (PFIF) as a data exchange format that could be integrated into all participating systems.[95] Ka-Ping Yee, then a graduate student at Berkeley, and a group of volunteers launched PFIF in 2005 as a means of assisting the disaster relief efforts following Hurricane Katrina. PFIF was designed to reduce the difficulties associated with the automated aggregation and sharing of missing persons information.[96] The specifications seek to address the informational needs of the public via the Internet.[97] PFIF also standardizes data retention that is one aspect of information privacy.[98] Currently, Google,[99] the National Library of Medicine,[100] and MISSING.NET routinely share missing persons information using PFIF, including 60,000 PFIF records created after the 2010 Haiti earthquake and 600,000 after the 2011 Japan earthquake.[101]

The second leading design specification is the Emergency Data Exchange Language (EDXL). The US Department of Homeland Security (DHS) originally developed the EDXL Distribution Element in partnership with private and public disaster response and national security organizations. OASIS, a non-profit consortium, publishes and currently maintains the standard. The purpose of the EDXL specification is to address the informational needs of professional emergency response and management workers.[102] A variant still in process is EDXL-Tracking of Emergency Patients (EDXL-TEP)[103] for medical professionals that would enable them to report the location of those involved in a disaster.[104]

MPCI activities include the review of data formats used during disasters to determine if adjustments might be necessary to bring technical standards into alignment with the needs of the missing persons community.[105]

Full descriptions of each design specification and additional technical details are provided in the appendices to this report.

---

[95] See Part IV.B.1(a).
[96] This purpose was articulated in a personal account of the development of the PFIF standard during the aftermath of Hurricane Katrina by David Geilhufe, a fellow participant in the disaster relief efforts. See David Geilhufe, "Personal History of the Katrina PeopleFinder Project Part I," *Social Source* (blog), Oct. 1, 2005, http://socialsource.blogspot.com/2005/10/personal-history-of-katrina.html.
[97] Andy Carvin, "Using Google's Haiti Missing Persons Widget," *Inside NPR.org* (blog), *National Public Radio*, Jan. 17, 2010, https://www.npr.org/blogs/inside/2010/01/using_googles_haiti_missing_pe.html.
[98] See "People Finder Interchange Format 1.4 Specification," Ka-Ping Yee, accessed July 23, 2012, http://zesty.ca/pfif/1.4/.
[99] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[100] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[101] Ka-Ping Yee, interview by Adam Elewa, Aug. 11, 2012 (on file with Fordham CLIP), PFIF Questionnaire, Fordham Law School, New York, NY.
[102] Org. for the Advancement of Structured Info. Standards [OASIS], *Emergency Data Exchange Language* (*EDXL) Distribution Element* (2006), 5-6, http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf.
[103] "Emergency Management Tracking of Emergency Patients (EM TEP) Subcommittee," Org. for the Advancement of Structured Info. Standards [OASIS], accessed July 23, 2012, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency-tep.
[104] Org. for the Advancement of Structured Info. Standards [OASIS], *EDXL-Tracking of Emergency Patients (TEP): Requirements and Draft Messaging Specification* (2010), 7, http://xml.coverpages.org/EDXL-TEP-Reqs-Draft-Messaging.pdf.
[105] See Part IV.B.1(b).

2. Database Systems and Software Design

MPCI members also develop, maintain, and manage five different online database systems and software for identifying and locating missing persons during natural disasters. These systems were used following Hurricane Katrina (2006), the Haiti earthquake (2010), the Chile earthquake (2010), the Brazil earthquake (2011), the Japan tsunami (2011), Hurricane Irene (2011), the Alabama tornadoes (2011, 2012), the Arizona wildfires (2012), the Colorado wildfires (2011, 2012), the Connecticut blizzard (2011), the Dallas-Fort Worth tornadoes (2011), the Minnesota floods (2012), and the Pakistan floods (2012).

These systems are often at work simultaneously during a disaster relief effort and can therefore benefit significantly from sharing information.

a) ICRC Family Links Service

The ICRC is an international private humanitarian organization that "works worldwide to provide humanitarian help for people affected by conflict and armed violence and to promote the laws that protect victims of war."[106] The ICRC operates under a mandate from the Geneva Conventions of 1949 and its Additional Protocols of 1977.[107]

In the Geneva Conventions and its Additional Protocols, as well as in other resolutions adopted at some International Conferences of the Red Cross and Red Crescent Movement Conferences, the ICRC has been entrusted by states to restore family links and clarify the fate of the missing in armed conflicts and other situations of violence.[108] The ICRC also coordinates, advises, and strengthens the capacity of Red Cross and Red Crescent National Societies in restoring family links in armed conflicts and other situations, such as disasters and migration. The use of online resources is one of the methods employed by the ICRC to restore family links, but the method remains a relatively minor part of the ICRC's activities.[109]

[106] Int'l Comm. of the Red Cross [ICRC] About page, accessed July 23, 2012, http://www.icrc.org/eng/who-we-are/index.jsp.
[107] Int'l Comm. of the Red Cross [ICRC] About page, accessed July 23, 2012, http://www.icrc.org/eng/who-we-are/index.jsp.
[108] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[109] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.

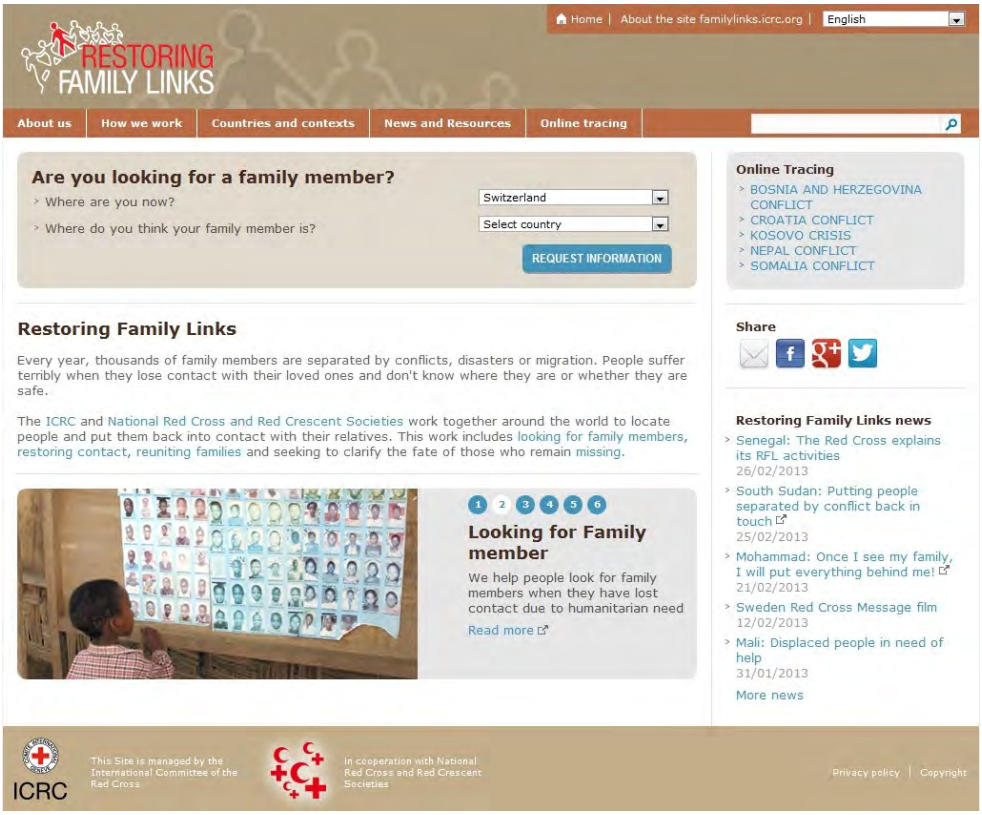


Figure 1. The ICRC Family Links service, available at http://familylinks.icrc.org.

The overall purpose of the ICRC family links website [**Figure 1**] is to put those who have lost contact with loved ones due to armed conflicts, violence, or natural disaster back in touch despite failures of the "postal service, telephone and other regular means of communication."[110] The ICRC uses two different databases for the online collection and dissemination of information about missing persons.[111] The ICRC refers to both as the ICRC Family Links service.[112] The first database contains only data collected and verified by official emergency workers and volunteers.[113] The second database contains data submitted by registered Internet users looking for someone affected by a disaster or reporting on their own status.[114] Both databases are accessible via a web browser.

[110] "What to do if you are looking for a relative," Int'l Comm. of the Red Cross [ICRC], accessed July 23, 2012, http://www.icrc.org/eng/resources/documents/misc/restoring-family-links-what-to-do-220208.htm.
[111] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[112] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP) ICRC Questionnaire, Fordham Law School, New York, NY.
[113] The table in Appendix 5 describes this as "publication of missing person list." *See* Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[114] Although the service mainly facilitates communication between web users, the ICRC does not allow a change in the status of a missing person to deceased without first verifying that the change is accurate. The table in Appendix 5

The databases operated by the ICRC are in Geneva, Switzerland. The ICRC enjoys an explicit exemption in the Swiss Federal Act on Data Protection from all regulations concerning the processing of personal information.[115] However, the ICRC maintains and promotes internal standards regarding the missing persons activities.[116] The ICRC seeks to craft data protection policies that are respectful of international privacy principles.[117]

b) American Red Cross' Safe and Well Service

The American Red Cross is a US non-profit humanitarian organization that focuses on providing aid to victims of war and those devastated by natural disasters.[118] The American Red Cross operates an Internet-accessible database known as Safe and Well [**Figure 2**] that allows anyone affected by a disaster to submit status updates through a web interface.[119] Anyone concerned about someone located in a disaster area can look for a status message but only after supplying a phone number or home address that matches the one on record for the missing person.[120] The database deliberately allows one-way communication from someone affected by a disaster to someone concerned about the affected individual.[121] The database encourages minimal disclosure of personally identifying information by allowing users to provide as little information about their status as desired.[122] An individual's status can simply be "I am safe and well."

---

describes this as "user driven service." *See also* Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.

[115] Bundesgesetz über den Datenschutz [DSG] [Swiss Federal Act on Data Protection] June 19, 1992, SR 235.1, art. 3 (Switz.), *available at* http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.CH.

[116] Int'l Comm. of the Red Cross [ICRC], *Professional Standards for Protection Work Carried Out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence* (Oct. 2009), http://www.icrc.org/eng/assets/files/other/icrc_002_0999.pdf.

[117] Int'l Comm. of the Red Cross [ICRC] Electronic Workshop on the Legal Protection of Personal Data & Human Remains, Apr. 2-May 6, 2002, *The Legal Protection of Personal Data & Human Remains: Final Report and Outcome* 16-22 (July 2002), *available at* http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf. See also Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY. ("The ICRC has a long-standing policy and practice of confidentiality. Confidentiality as a working method is derived from the principles of neutrality and impartiality under which the ICRC operates. This means that the ICRC requires confidential and bilateral communications, including written submissions, with the relevant authorities and that it expects such authorities to respect and protect the confidential nature of its communications. The International Community has accepted and recognized that confidentiality is necessary for the effective performance by the ICRC of its functions. This implies that the ICRC enjoys a privilege of non-disclosure, including a testimonial immunity for its staff before national and international courts. Therefore, for instance, the ICRC could not be compelled by a court to disclose information that has been collected in the context of activities for restoring family links.")

[118] "American Red Cross About," accessed July 23, 2012, http://www.redcross.org/aboutus/.

[119] "American Red Cross FAQs," accessed July 23, 2012, https://safeandwell.communityos.org/cms/faq.

[120] "American Red Cross FAQs," accessed July 23, 2012, https://safeandwell.communityos.org/cms/faq.

[121] "American Red Cross FAQs," accessed July 23, 2012, https://safeandwell.communityos.org/cms/faq.

[122] Users can choose from a list of preformed status updates (i.e., "I am safe and well") or use a text box that allows the submission of any text-based data.

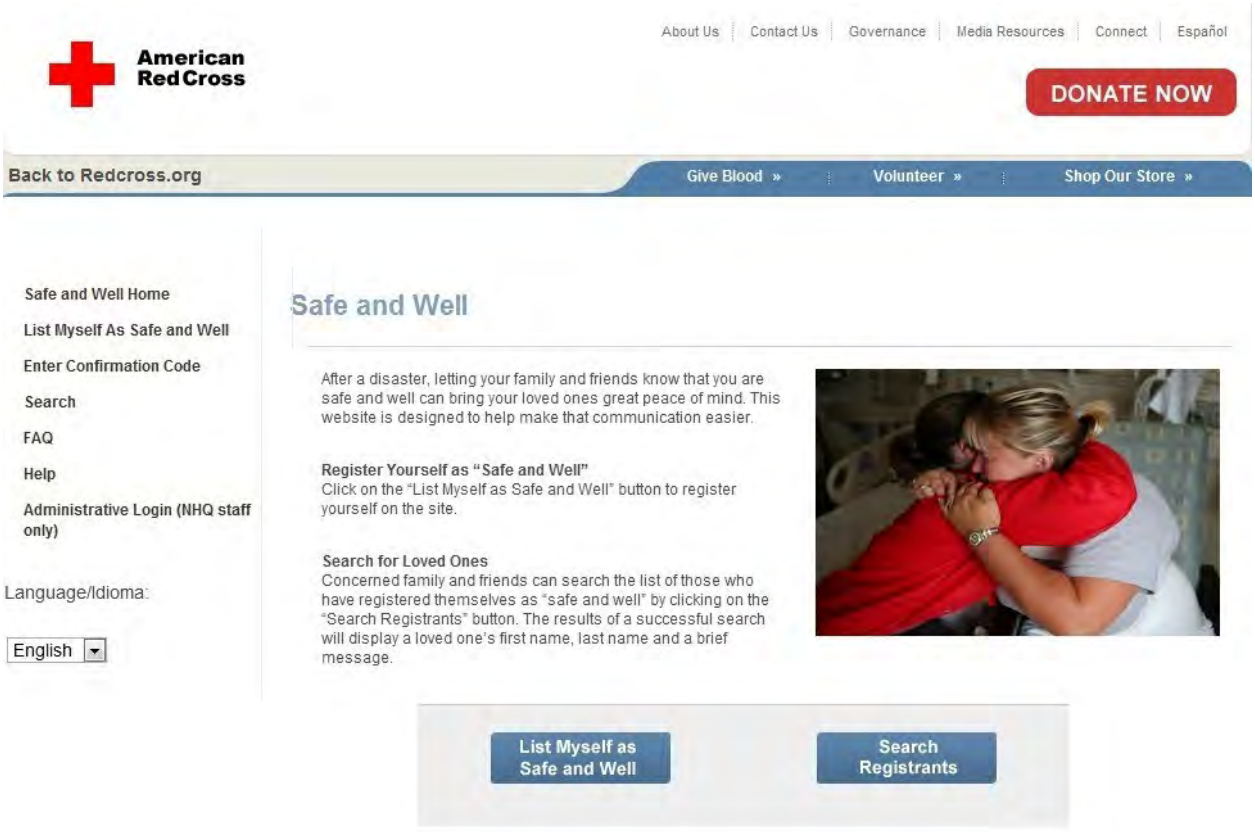


Figure 2. The American Red Cross's Safe and Well website, available at https://safeandwell.communityos.org.

c) Google's Person Finder

Google operates a database, known as Google Person Finder, based on the PFIF standard.[123] The involvement of a commercial enterprise in the missing person space illustrates the diversity of entities involved in open-source activities. Google engineers, including PFIF's original developer, Ka-Ping Yee, built Google Person Finder. The database becomes searchable and open to new entries at the discretion of Google's Crisis Response team.[124] Google's Crisis Response team analyzes the scale of impact of the disaster and then determines which of its tools would be most useful for responding to the given situation. Google may choose to deploy Person Finder as a part of its larger Crisis Response effort in a region. The database allows people to post information about someone they know who has been affected by a disaster, and people can search for information that others have posted. Google does not verify the accuracy of the information submitted or the identity of a submitter.[125]

[123] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[124] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[125] Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.

A user can query information from the database by using the web interface or by writing software that talks to the database directly via the Application Programming Interface (API).[126] Google generally only grants access to its API to government, quasi-government, or established non-profits,[127] and it only grants access to the API after considering the "motivation for the request and the likelihood that the request will meaningfully expand the usefulness of Person Finder and its accessibility to users."[128] In keeping in compliance with the PFIF specification, Google's Person Finder respects the expiration date set on any submitted record by permanently deleting the record on the specified date, and it requires the same of any third parties who make copies of the records.[129] Additionally, Google permanently deletes all records, regardless of expiration date, when the Google Crisis Response team determines the database to no longer be useful to disaster relief efforts.[130]

Lastly, Google Person Finder is also an open-source application. Other organizations may use the application to establish their own databases without operational participation by the Google Crisis Response team.

d) The US National Library of Medicine's People Locator

The US National Library of Medicine (NLM), a federal agency, is a component of the National Institutes of Health, which is part of the US Department of Health and Human Services. The NLM describes itself as the world's largest biomedical library. It maintains and makes available worldwide its electronic information resources at no charge on a wide range of topics. The NLM also supports and conducts research, development, and training in biomedical informatics and health information technology.[131]

The NLM operates a missing persons database known as People Locator as a part of its Lost Person Finder project.[132] The NLM plans to deploy its People Locator service in two different contexts, with different rules guiding data submission and dissemination in each. The NLM refers to the different events that would prompt the launch of the database as community-based events and hospital-based events. The NLM decides when to activate an event on its service.

---

[126] An Application Programming Interface (API) can best be understood by contrasting it with a Graphical User Interface (GUI). Graphical user interfaces—the visual objects such as folders, buttons, and icons—allow humans to talk to computers via the familiar manipulation of visual objects (i.e., opening folders). An API, by contrast, provides a medium that allows software, rather than humans, to talk to other software. Getting software to talk to other software via the GUI is possible, but is typically more complex. See *PC Magazine Encyclopedia*, s.v. "API (Application Programming Interface)," accessed July 23, 2012, http://www.pcmag.com/encyclopedia/ (search "Search Encyclopedia" for "API").

[127] Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.

[128] "Google DataAPI," last modified Aug. 8, 2012, https://code.google.com/p/googlepersonfinder/wiki/DataAPI.

[129] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.

[130] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.

[131] US National Library of Medicine Fact Sheet, accessed July 23, 2012, http://www.nlm.nih.gov/pubs/factsheets/nlm.html.

[132] US National Library of Medicine About page, accessed July 23, 2012, https://pl.nlm.nih.gov/about. NLM uses software from the Sahana Software Foundation.

In community-based events, data comes (1) through a web interface on the NLM web site, (2) by import from Google Person Finder using the PFIF protocol, (3) via submission through an NLM designed iPhone app, or (4) semi-structured email.[133] The NLM has also "screen-scraped"[134] data from CNN iReports[135] and the ICRC Family Links service following the disaster in Haiti.[136] Users seeking to submit data via the NLM web interface or the NLM iPhone app must first establish a user account with NLM by providing personally identifying information.[137]

During hospital-based events, only entities covered under the US health privacy rule (HIPAA) can submit or access data. During large-scale disasters, both HIPAA and the NLM allow for broader dissemination of health information to disaster relief organizations.[138]

Hospital workers first capture a photo and minimal information using a Lost Person Finder-developed Windows application called TriagePic when a victim arrives at the hospital's triage station, with the option to add more information if time permits.[139] As with community-based events, a user needs an account with the system before submitting information. Family reunification counselors and medical personnel in treatment zones can search the records contained in the database and use this information to answer queries from people seeking information.[140]

To date, hospital-based events have been limited to simulated tests, as the NLM is still working with partner hospitals to develop appropriate privacy and operational guidelines. However, the NLM launched the community-based database in disaster events such as major earthquakes in Haiti, Chile, New Zealand, Japan, and Turkey, and the Joplin, Missouri, tornado.[141]

---

[133] This means that missing persons information emailed to NLM can be automatically parsed and input into the database, but it needs to be formatted in a particular manner. For instance, the database may require there to be a new line between every data element, or for each data element to be preceded by a descriptor (i.e., name, address, etc.), for the information to be parsed correctly.

[134] Scraping refers to the practice by which a computer program parses and stores data viewable on a website without the website owner necessarily being aware of, or consenting to, the data extraction. See *PC Magazine*, s.v. "scraping," accessed July 23, 2012, http://www.pcmag.com/encyclopedia/ (search "Search Encyclopedia" for "scraping").

[135] CNN iReport is a social network that allows users to post and read stories created by other users. CNN allows posting of stories without any fact checking. See CNN iReport About page, accessed July 23, 2012, http://ireport.cnn.com/about.jspa.

[136] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[137] See table in Appendix 5.

[138] 45 C.F.R. § 164.510(b)(4) (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-510.pdf. See US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[139] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[140] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[141] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

e) MISSING.NET

MISSING.NET [**Figure 3**] is a missing person database system operated by the Red Helmets Foundation, chaired by Nicole Guedj (a former French minister) in partnership with Bearstech[142] and European Consulting Services,[143] and with some engineering assistance from Google.[144] According to MISSING.NET, the purpose of the site is to "facilitate the action of humanitarian rescue workers and victims mainly in the first crucial hours of the crisis."[145]

Accessible via a web browser, the MISSING.NET database allows a visitor to create a user profile in advance of a disaster.[146] A user creates the profile by submitting personally identifying information, including home address. MISSING.NET does not delete user profiles, but never publicly displays the profiles.[147] Information about missing persons can be submitted only during an active "disaster event." The website's administrators determine when disaster events begin and end.[148] Besides submissions by MISSING.NET users, the system updates its missing person records from Google's database by means of the Person Finder API key.[149]

f) Sahana Software Foundation

The Sahana Software Foundation is a California not-for-profit organization. The mission of the foundation is to provide "management solutions that enable organizations and communities to better prepare for and respond to disasters."[150] The foundation develops both software and design specifications that can be used by missing persons systems. The software and design specifications are open source. Sahana Software Foundation products have been deployed for missing persons activities following many natural disasters, including the 2004 Indian Ocean tsunami and the 2006 Kashmir earthquake. Other missing persons organizations use Sahana products as platforms, such as the NLM's use of Sahana software in People Finder.[151]

As indicated by these descriptions, each of the databases and the software are subject to unique designs and operate under distinct rules, so developing a sharing protocol is a complex project. Each system houses different types of data, has unique requirements about who may input data into the system, and has distinct rules on how users may access the information. For example, the

---

[142] Bearstech is a private web hosting company located in France. See Bearstech About page, accessed July 23, 2012, http://bearstech.com/english/.
[143] European Consulting Services is a private technology consulting company located in France. See "Accueil," European Consulting Services, accessed July 23, 2012, http://www.european-cs.com.
[144] MISSING.NET About page, accessed July 23, 2012, http://www.missing.net/pages/about.html.
[145] MISSING.NET About page, accessed July 23, 2012, http://www.missing.net/pages/about.html.
[146] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[147] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[148] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[149] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[150] Sahana Software Foundation, History, accessed Nov. 15, 2012, http://sahanafoundation.org/about-us/history/.
[151] Sahana Software Foundation, Deployments, accessed Nov. 15, 2012, http://sahanafoundation.org/community/deployments/.

Safe and Well system requires that a user input some personally identifiable information about a missing person before he or she is able to access the files about that person, while Google Person Finder has no similar access restriction. Similarly, some systems, like Family Links and MISSING.NET require users to register before they can submit information about missing persons, while others freely allow the public to access the database. The Google Person Finder system has a well-developed set of rules about record expiration and deletion while MISSING.NET has no set procedures about record deletion.

After every disaster or usage of an MPCI member's system, the group works together to document and share each organization's experience. These reviews assess when and how the member organization decided to launch its system, how the system was used, what issues or new solutions the organization came across, and what lessons can be learned from the experience.[152]

B. Privacy Considerations for MPCI Information Sharing Systems

The design of the technical specifications for sharing and the structure of the database systems affect privacy. Choices made about what information will be stored, who will have access to the missing persons information and how that information will be shared with third parties has significant implications for privacy. Design decisions that minimize data collection to essential elements and place some restrictions on access or use will be more protective of individual privacy.

However, privacy is not the sole concern for the members of the MPCI. These parties are primarily interested in aiding disaster relief efforts by helping to reconnect victims with their friends and family. That goal is best met when information is readily accessible in a timely manner. Missing persons organizations have a strong interest in sharing information broadly in order to help locate the missing.

Achieving a balance between privacy and ease of access is an important objective for the MPCI community. This section discusses some of the design choices currently implemented by MPCI members in order to highlight how the choices implicate privacy interests. The differences among the various systems demonstrate that there is a wide variety of ways that organizations can choose to achieve the tradeoff between privacy and access. The differences reflect different priorities and values and illustrate how collaboration can be complex.

Access. One design choice that implicates privacy is the determination regarding who will have access to the missing person information contained within a database system. Some systems share data liberally with Internet users while others share data only with those who can show a relationship to the missing person or membership in a medical or humanitarian organization. The American Red Cross's database, for instance, tries to limit access to those who have preexisting

[152] Crisis Commons hosts the archive of MPCI materials at http://wiki.crisiscommons.org/wiki/Missing_Persons.

knowledge of the missing person by requiring searching parties to know the phone number or address of the missing person before displaying that person's record.[153] The database operated by MISSING.NET, on the other hand, allows a registered user to display all the missing person records contained in the database without knowing any information about the person in advance. The National Library of Medicine intends to limit access to data collected during a hospital-based event to a select group of medical professionals, a limit required by law rather than by choice.[154]

Record retention. Another design choice that impacts privacy interests is whether the database imposes any restrictions on data retention. Storing data only as long as necessary for missing persons activities is protective of data security and privacy. However, the time that records should be stored depends on the scope and purpose of a given missing person database. Some databases store missing person records for longer periods than others. Some limit the retention of missing person records to the approximate duration of the crisis[155] which might end when conventional forms of communication resume or when the database administrator otherwise determines that the database is no longer useful. The ICRC, for example removes missing persons information from its database accessible through the Internet after conventional modes of communication have resumed, but it retains the removed data in its archives for research purposes.[156]

Registration. Requiring registration is yet another design choice that can impact privacy. Requiring users to register before searching or submitting data has advantages and disadvantages. Registration protects records contained in the database as it presents a modest obstacle to the unauthorized automated copying of the database. This is especially true if registration requires a user to satisfy a Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA).[157] Registration may also simplify access for returning submitters.

Many databases require those who submit missing person records to also submit their personal contact information. Registration may result in better quality data if submitters feel accountable. On the other hand, some submitters may be reluctant to share their own personal data while serving a public interest and may provide false or inaccurate data. Registering submitters imposes costs and complexity, and it may have some security disadvantages. For example, the long-term storage of user profiles may create a liability for disclosure of data resulting from a security breach. In addition, an applicable privacy law may apply differently to the processing of information about submitters than information about missing persons.

Information sharing. Finally, decisions about how the database will gather or share information with third parties reflect different tradeoffs between privacy and access. Some databases routinely pull data from or push data to other databases. For example, the automated sharing and

[153] "American Red Cross FAQs," accessed July 23, 2012, https://safeandwell.communityos.org/cms/faq.
[154] Missing Persons Community of Interest [MPCI] Docs.
[155] See Table in Appendix 5.
[156] MPCI Documents.
[157] CAPTCHAs are a widely used challenge-response system designed to frustrate the automated access of digital resources and services. See "CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart)," SearchSecurity, accessed July 23, 2012, http://searchsecurity.techtarget.com/definition/CAPTCHA.

copying of data are fundamental to the design of the PFIF standard[158] and to Google's Person Finder database using PFIF.[159] The practice of routinely sharing missing person records has some clear advantages. If records are not freely shared, someone seeking a missing person may need to find and search multiple databases. This can become a significant obstacle when there are many missing persons databases.[160] However, an advantage of not sharing information is that the system owner controls information storage and access, decreasing the chance of misuse and increasing accountability. Database operators can diminish security and privacy concerns by setting standards for cooperating databases. For example, Google requires all third parties who want access to their data to abide by the same privacy policy as Google does.[161]

Striking an appropriate balance between privacy and utility calls for a series of choices that will be influenced by the emergency circumstances that result from natural disasters. A privacy option that may be improper for an organization to make under routine circumstances may nevertheless be appropriate when meeting the challenges of disaster response and the humanitarian needs that follow. Different organizations operating in different cultures and with different methods, objectives, values, and legal regimes may legitimately take different approaches.

IV. Legal Analysis for Privacy and Missing Persons Activities

This Part analyzes major privacy principles applicable to missing persons activities in order to demonstrate the issues that disaster relief organizations must consider as they develop their databases and begin to share information with third parties. For the analysis, this report focuses on privacy law in the European Union and the United States because these jurisdictions serve as important examples of privacy regulation around the globe. The report offers a general analysis rather than a detailed assessment of any particular activity that would depend on the application of the law of a specific jurisdiction.

The European Union has a well-established and comprehensive approach to data protection that provides a high degree of commonality among its more than two dozen Member States. This commonality comes from the 1995 European Directive on Data Protection[162] that requires each

[158] Design principles promote the convergence of data via the process of synchronizing or copying missing persons records from PFIF-compliant and non–PFIF-compliant sources. "People Finder Interchange Format 1.4 Specification," Ka-Ping Yee, accessed July 23, 2012, http://zesty.ca/pfif/1.4/.
[159] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[160] Director of the Center for Future Civic Media at the Massachusetts Institute of Technology, Chris Csikszentmihalyi, warned of the dangers that too many unconnected sites pose for successful reunions and discussed the role that Google's Person Finder plays in alleviating that danger. Christopher P. Csikszentmihalyi, "Information on Haiti Is Getting Siloed," *Pogue's Posts* (blog), *New York Times*, Jan. 17, 2010, http://pogue.blogs.nytimes.com/2010/01/17/information-on-haiti-is-getting-siloed/.
[161] "Google Person Finder API Terms of Service," last modified Mar. 15, 2012, https://code.google.com/p/googlepersonfinder/wiki/TermsOfService.
[162] 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, art. 28, 1995 O.J. (L 281) 31, 47, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Member State to have a national law establishing processing rules for personal information. Because privacy laws within each EU Member State are not identical, this report focuses on the principles of the EU Data Protection Directive that must be incorporated into the national law of each EU Member State.[163] Changes to the EU privacy regime are pending,[164] but the report's analysis does not review proposed changes as they are too preliminary as of the publication of this report. EU policies are important worldwide not only because of the size and significance of the European Union, but because many nations that are not EU members model their privacy laws in varying degrees on standards of the 1995 EU Directive.

The second jurisdiction analyzed here is the federal level in the United States, whose privacy laws offer a contrast with the EU approach. The United States was chosen because of the critical role that US-based actors play in disaster assistance, including the reach of US-based Internet organizations, communications services, and economic relief efforts. The United States lacks a comprehensive federal privacy law equivalent to EU national data protection laws, but instead has a series of discrete, narrowly focused privacy laws—often described as sectoral laws—that cover particular types of records or particular record keepers. Large sectors of the economy and many classes of record keepers are wholly unregulated for privacy by federal law. In addition to federal laws—the focus of this report—states within the United States sometimes have their own laws regulating the privacy of some types of records and some classes of record keepers.

The United States contrasts with the European Union on other aspects of privacy. For example, EU policy addresses both the processing of personal information within its borders and the export of that information to other nations. The United States regulates only some domestic personal information processing, and its laws rarely address exports of personal data to other jurisdictions.

The focus here on the European Union and the United States should not suggest that the laws of other nations are unimportant or irrelevant. For some disasters, it is foreseeable that neither US nor EU privacy rules will be of prime relevance. However, to the extent that a government agency, commercial enterprise, non-profit organization, or other entity in the United States or the European Union operates a missing persons information system, the privacy laws of these two jurisdictions may be inextricably entangled with missing persons activities even when the individuals whose data is primarily at issue may reside in other areas of the world.

Section A provides an overview of privacy. Section B maps out the key legal privacy issues and discusses how they may impact missing persons activities. In each case, the report contrasts the application of EU law with US law to provide perspective on different legal approaches to privacy.

---

[163] 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, art. 5, 1995 O.J. (L 281) 31, 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[164] See Press Release, European Commission, "Commission Proposes a Comprehensive Reform of the Data Protection Rules" (Jan. 25, 2012), http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

A. Overview of Privacy

This section offers a brief introduction to information privacy issues relevant to missing persons and provides a basic outline to EU and US privacy law.

To understand information privacy activities in the world today, it is helpful to use Fair Information Practices (FIPs) as a framework for describing privacy regulatory activities found in many nations.[165] FIPs are a set of basic principles for addressing concerns about information privacy. FIPs form the basis of privacy laws around the world, including the United States, although reliance on FIPs in the United States is not as comprehensive as in other countries.[166] International policy convergence around FIPs has remained substantially consistent for several decades.

FIPs originated in the 1970s with a report from a predecessor of the federal Department of Health and Human Services.[167] A few years later, the Organisation for Economic Cooperation and Development (OECD) revised the original statement of FIPs.[168] The OECD's version became the most influential statement of the principles.[169]

The eight principles set out by the OECD are as follows:

1. **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.
2. **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.
3. **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
4. **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.

---

[165] 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.
[166] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, (Ithaca, NY: Cornell University Press, 1992), 6.
[167] Dep't of Health, Educ. and Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973), http://epic.org/privacy/hew1973report/default.html.
[168] Org. for Econ. Cooperation and Dev. [OECD], OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
[169] The Asian Pacific Privacy Framework, an alternative international approach to privacy, has much in common with the OECD FIPs principles, *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

5. **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.
6. **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.
7. **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 them; (b) to have communicated to them, data relating to them 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 them; (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.
8. **Accountability Principle.** A data controller should be accountable for complying with measures, which give effect to the principles that have been stated.

The substantive privacy provisions in the EU Data Protection Directive map well to the FIPs framework, with each FIP's principle addressed in varying levels of detail. The Directive calls on each Member State to enact the Directive's standards for the processing of personal data by data controllers within the Member State.[170] Some state functions (e.g., defense and national security) fall outside the scope of the directive, and exceptions apply to individuals engaged in personal or household activities.[171] The Directive allows special rules for the press and for artistic expression.[172] Generally, however, the design of the Directive is that most organizations in an EU Member State that process personal data are subject to data protection rules that meet common EU standards. The mechanisms in national laws applying those standards may vary as long as they satisfy the basic requirements of the Directive.

[170] 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, art. 3, 1995 O.J. (L 281) 31, 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[171] 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, art. 3(2), 1995 O.J. (L 281) 31, 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[172] 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, art. 9, 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Personal Information and Personal Data

Legal obligations for the protection of privacy generally attach only to information that is considered "personal information." However, the definition of "personal information" has some variance.[173]

The EU Data Protection Directive defines *personal data* to mean:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[174]

US laws use a variety of terms, including *record* found in the Privacy Act of 1974.[175] In general, US law and practice emphasize the terms *personal information* or *personally identified information*. This report uses these terms—personal information, personal data, and record—interchangeably.

Individuals, Data Subjects, and Persons

The EU Data Protection Directive calls on Member States to provide protection for the personal data about identifiable natural persons (also called *data subjects*). The typical American equivalent is *individual*. In either jurisdiction, a *person* in some contexts can include an individual, government agency, corporation, and other legal entity. Privacy generally protects the interest of individuals.[176]

The EU Data Protection Directive also requires Member States to limit the export of personal information to third countries[177] (countries that are not EU Member States) and requires each Member State to have an independent privacy supervisory authority.[178] Supervisory authorities, sometimes called data protection authorities, are important in the operation of many data protection laws as they enforce and interpret the laws.

[173] For an extended discussion of issues with the definition of personal information, see Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U L. Rev. 1814 (2011), *available at* SSRN: http://ssrn.com/abstract=1909366.

[174] 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, art. 2(a) (definition of 'personal data'), 1995 O.J. (L 281) 31, 38, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[175] 5 U.S.C. § 552a (a)(4) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.

[176] The laws in some European jurisdictions extend privacy rights to legal persons. Even where privacy laws do not apply to legal persons like corporations, legal persons still have confidentiality interests. These interests are beyond the scope of this analysis.

[177] 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, arts. 25, 26, 1995 O.J. (L 281) 31, 45-46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[178] 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, art. 28, 1995 O.J. (L 281) 31, 47, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Processing

Processing generally means the collection, maintenance, use, and disclosure of personal information. Any aspect of the life cycle of personal information from creation to ultimate destruction falls within the term *processing*. The EU Data Protection Directive expansively defines processing as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[179]

Data Controller and Record Keeper

Under the EU Data Protection Directive, the controller or data controller is responsible for compliance with data protection rules and for fulfilling the rights exercised by data subjects.[180] The Directive defines *controller* as any person who determines the purposes and means of processing of personal data.[181] US privacy laws take different approaches to defining the person responsible for processing personal data and complying with privacy law. A familiar US term used in this report as the equivalent of *data controller* is *record keeper*.

The situation in the United States is markedly different.[182] No general privacy statute covers all record keepers of personal information. At the federal level, a handful of privacy laws cover specific types of records or specific types of record keepers.[183]

As illustrated by several examples of targeted privacy protections, few apply directly to information sharing systems for missing persons. The principal laws relevant to this report are:

[179] 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, art. 2(b) (definition of 'processing of personal data'), 1995 O.J. (L 281) 31, 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[180] See, generally, Art. 29 Data Prot. Working Party, 00264/10/EN, WP 169, *Opinion 1/2010 On the Concepts of "Controller" and "Processor"* (Feb. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
[181] 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, art. 2(d)(definition of 'controller'), 1995 O.J. (L 281) 31, 38, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[182] See Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law: A Study of U.S. Data Protection*, (Charlottesville, VA: Michie, 1996).
[183] See, e.g., The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006)(credit reporting), *available at* http://www.law.cornell.edu/uscode/text/15/1681; Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2006)(educational records), *available at* http://www.law.cornell.edu/uscode/text/20/1232g; Video Privacy Protection Act, 18 U.S.C. § 2710 (2006)(video rental records), *available at* http://www.law.cornell.edu/uscode/text/18/2710; Driver's Privacy Protection Act, 18 U.S.C. § 2721 et seq. (2006)(driver license information), *available at* http://www.law.cornell.edu/uscode/text/18/2721; Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq. (2006)(collection of information from minors); Gramm-Leach-Bliley Act, 15 U.S.C. §6801-6809 (notice of privacy policies for financial institutions).

The Privacy Act of 1974[184] applies to most compilations of personal information held by federal agencies and by some agency contractors (see Section B [1][a]). The Act implements all elements of FIPs. Indeed, the advisory committee that originally proposed FIPs also proposed much of the wording that became the Privacy Act of 1974. Importantly in an international context, the Act generally grants privacy rights only to citizens of the United States and aliens admitted for permanent residence.[185] Foreign nationals have no rights under the Act.[186] This law is relevant for missing persons information processed by US federal agencies.

The federal health privacy and security rules[187] issued under the authority of HIPAA[188] apply to covered entities, which are most health care providers and all health insurers and health clearinghouses. The rules also extend to business associates of covered entities. The privacy rule expressly seeks to establish a basic set of FIPs for health records.[189] The privacy rule sets a nationwide floor of privacy protection and allows more stringent state laws to remain in force. In addition, some health record keepers are also subject to other federal health privacy rules covering specific categories of records, such as the rules governing the Confidentiality of Alcohol and Drug Abuse Patient Records.[190] The HIPAA privacy rule does not cover many institutions that maintain health information such as schools, websites, banks, casualty insurers, health clubs, advocacy organizations, and others. The law applies to missing persons information sharing by covered entities.

In the United States, the privacy protections that apply to a record in the hands of one record keeper typically do not apply if the original record keeper discloses the record to a third party. For example, if a medical provider shares a patient record with a missing persons organization, that organization will not be bound by HIPAA. For many record keepers and sectors of the economy, no privacy laws apply at all. For example, no federal information privacy laws cover most marketing activities, Internet records, records of non-profit organizations, or merchants of goods and services.

---

[184] 5 U.S.C. § 552a (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[185] 5 U.S.C. § 552a (a)(2) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[186] Foreign nationals can use the federal Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(6), *available at* http://www.law.cornell.edu/uscode/text/5/552, to seek access to records held by federal agencies, but no other privacy rights are available under the FOIA.
[187] 45 C.F.R. pts. 160, 164 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-chapA-subchapC.pdf.
[188] Pub. L. No. 104–191, tit. 2, § 264, Aug. 21, 1996, 110 Stat. 2033, 42 U.S.C. § 1320d-2 note, *available at* http://www.law.cornell.edu/uscode/text/42/1320d-2.
[189] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000), 45 C.F.R. pts. 160, 164, *available at* http://www.gpo.gov/fdsys/pkg/FR-2000-12-28/pdf/00-32678.pdf.
[190] 42 C.F.R. pt. 2 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title42-vol1/pdf/CFR-2011-title42-vol1-part2.pdf.

Information Privacy and Data Protection

In the United States, the term *information privacy* describes concerns related to the collection, use, maintenance, and disclosure of personal information. The broader term—*privacy*—includes information privacy as well as many other concerns about freedom from intrusion or disturbance in private life or affairs. Most of the rest of the world typically uses the term *data protection* rather than information privacy. In this report, information privacy and data protection are equivalent.

The United States has no privacy supervisory agency comparable to those in Europe. The Federal Trade Commission (FTC) is an independent regulatory agency with a broad consumer protection jurisdiction whose privacy activities include specific regulatory authority over several privacy statutes.[191] It also can take action against some commercial enterprises that engage in unfair or deceptive trade practices.[192] The FTC sometimes uses this authority to enforce privacy promises made by companies through privacy policies on their websites. The FTC's jurisdiction over privacy is not as broad as that of EU data protection authorities. For example, the FTC has limited or no authority over privacy activities of agencies of the federal government, agencies of state and local governments, most non-profit organizations, and many commercial entities engaged in transportation, insurance, banking, and telecommunications common carriage. The FTC's jurisdiction over privacy activities of those engaged in missing persons activities may depend in part on location and the profit or non-profit status of participants. The FTC is an unlikely regulator or overseer of missing persons data activities.

In the context, however, of both EU and US law, some limits of FIPs warrant attention. First, while a policy consensus around FIPs generally exists, statutory and other formulations of FIPs can vary considerably. [193] The number of principles and the descriptions of each principle can differ even when the overall content is similar. For example, the accountability principle for compliance with privacy principles can be fulfilled with criminal penalties, civil lawsuits, administrative enforcement, arbitration, internal or external audits, complaint processing, staff training, and more. The high-level FIPs principles do not prescribe implementation details, making the application of FIPs in a particular context more complex than a mechanical application of rules. And, second, some—especially in the United States—apply the term *Fair Information Practices* to shortened or amended collections of principles that diverge from the international consensus. Nevertheless, FIPs remain a key to understanding both the EU and US legal frameworks.

[191] The recently created Consumer Financial Protection Bureau now shares or exercises exclusively some FTC authority under the Fair Credit Reporting Act and other laws. The FTC retains its role under the Children's Online Protection Act.
[192] 15 U.S.C. § 45 (2006), *available at* http://www.law.cornell.edu/uscode/text/15/45.
[193] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 Stan. L. Rev. 1315 (2000), *available at* http://reidenberg.home.sprynet.com/international_rules.pdf.

Box 2: Do Privacy Rights and Interests Survive Death?

Privacy is usually an attribute of living individuals. Whether privacy rights and interests survive death is a complex question that can vary from context to context. The Article 29 Working Party established under the EU Data Protection Directive wrote that because the protections afforded by the Directive apply to natural persons, personal data protected by the Directive is data relating to identified or identifiable living individuals.[194] However, the Working Party also observed that it may not be clear if an individual is living, that information on dead individuals may also relate to living individuals, that rules other than data protection rules may extend specific privacy rights after death (noting that medical confidentiality obligations do not end with death), and that Member States may extend data protection to cover dead individuals.

In the United States, the answer varies from law to law. For information held by federal agencies, the Privacy Act of 1974[195] does not grant deceased individuals or their next of kin any privacy rights.[196] The federal health privacy rule, however, offers a completely different approach. The rule issued under the Health Insurance Portability and Accountability Act (HIPAA)[197] currently provides that the right of privacy extends forever.[198]

For missing persons purposes, it may be impractical for any dedicated system to function with a rule that terminates privacy interests at death. Even though data may come from sources or countries that have privacy-ends-at-death rules, some missing persons information, particularly health data, is likely to fall under a policy or law that extends privacy interests after death. Further, in the case of missing persons, whether an individual is dead or alive may be unknown. There may be a great deal of uncertainty for considerable amounts of data, and it is inevitable that some systems will at times wrongly describe individuals as either dead or alive. Commercial search engines and some other data systems may provide information regardless of the status of the data subject and may not be able to make determinations for data provided from disparate sources.

It will likely be impractical for a dedicated missing persons system operating under the pressures that accompany disasters to function with privacy rules that vary based on the status of individuals. However, it may be possible to consider a different policy with respect to data once a disaster ends and missing persons activities for that disaster terminate. Much will depend on the longevity of the information in the missing persons data system.

The identification of human remains, an activity often associated with natural disasters, is beyond the scope of this report. Even if privacy protections under a national law do not apply to dead individuals, legal protections and appropriate procedures will remain relevant. The 2002 International Committee of the Red Cross (ICRC) report discussed commonly accepted principles applicable to the identification of human remains, and that report remains a valuable resource.[199]

---

[194] Art. 29 Working Party, 01248/07/EN, WP 136, *Opinion 4/2007 on the Concept of Personal Data* 21-22 (June 20, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
[195] 5 U.S.C. § 552a (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[196] U.S. Dep't of Justice, Overview of the Privacy Act of 1974, at 12 (2010), *available at* http://www.justice.gov/opcl/1974privacyact.pdf.
[197] Pub. L. No. 104–191, tit. 2, § 264, Aug. 21, 1996, 110 Stat. 2033, 42 U.S.C. § 1320d-2 note (2006), *available at* http://www.law.cornell.edu/uscode/text/42/1320d-2.
[198] 45 C.F.R. § 164.502(f) (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-502.pdf. The policy is under review.

B. Key Legal Privacy Issues

An organization engaged in missing persons activities should consider several key privacy issues in order to evaluate whether its system and its information sharing practices conform to applicable law. In this section the report reviews these key issues, in each instance comparing the US and EU law in order to demonstrate the potential diversity of the legal analysis. The considerations for compliance with privacy laws are (1) identification of laws applicable to data controllers or record keepers; (2) recognizing the responsibilities of data controllers or record keepers (collection, purpose specifications and use limitations); (3) providing the required rights to data subjects (notice, consent, access and correction); (4) conforming to export controls; and (5) consideration of any special treatment for sensitive data (health information, race, religion).

1. Data Controllers and Privacy Regulation

The first step a missing persons organization must take is to establish which legal regime or regimes will apply to its data system. The location of a data controller or record keeper and the type of entity involved typically determine what privacy regime applies. For any missing persons organization located in the European Union, the policies set out in the EU Data Protection Directive apply through the applicable Member State law.[200] However, for many organizations located in the United States, it is likely that no privacy statute applies at all.

a) United States

Since the United States lacks a uniform privacy law, organizations based in the United States will be subject to privacy regulation only if there is a specific sectoral law addressing their industry or type of data collection. No US privacy law applies generally to the data processing activities of a non-profit organization or to individuals.[201] Federal laws apply, if at all, to particular records or record keepers based on the type of entity or the type of records maintained. Of existing federal laws, only two appear highly relevant. The first is the Privacy Act of 1974. [202] The second is the health privacy and security rules issued under HIPAA .[203]

---

[199] International Committee of the Red Cross [ICRC] Electronic Workshop on the Legal Protection of Personal Data & Human Remains, Apr. 2-May 6, 2002, *The Legal Protection of Personal Data & Human Remains: Final Report and Outcome* 16-22 (July 2002), *available at* http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf.

[200] The analysis here assumes that the missing persons entity will not be operated by a defense, public security, or criminal law agency not covered by the Directive. See Article 3.

[201] It is possible that a missing persons organization could collect information online from children under 13, which would make COPPA relevant, although that result is far from clear. COPPA applies to websites anywhere in the world that collect information from children in the United States, but the law does not apply to a non-profit entity. See 16 C.F.R. § 312.2 (2012) (definition of *operator*), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2012-title16-vol1/pdf/CFR-2012-title16-vol1-sec312-2.pdf.

[202] 5 U.S.C. § 552a (2006), http://www.law.cornell.edu/uscode/text/5/552a.

[203] Pub. L. No. 104–191, tit. 2, § 264, Aug. 21, 1996, 110 Stat. 2033, 42 U.S.C. § 1320d-2 note, *available at* http://www.law.cornell.edu/uscode/text/42/1320d-2.

The Privacy Act of 1974 applies to all federal agencies and to some federal contractors[204] that maintain qualifying records on behalf of an agency to accomplish an agency function. The Privacy Act of 1974 requires agencies to comply with a set of FIPs. The Act does not apply to federal grantees, individuals or others working with federal agencies in non-contractual relationships, recipients of federal funds, non-profits, or other non-federal institutions such as corporations, state government, and unions. For missing persons organizations that are not federal agencies or contractors, the Privacy Act of 1974 does not apply.

A second class of organizations that might occasionally play a role in missing persons activities includes health care providers and health care insurers.[205] Most providers and all insurers are subject to the HIPAA health privacy and security rules.[206] Most dedicated missing persons organization would not be considered a covered entity directly subject to the HIPAA rules.[207] However, a missing persons organization might cooperate with HIPAA covered entities in a variety of ways. For example, a hospital might be a source of information on the location of individuals receiving treatment or a clinic might play another role in coordinating missing persons activities for a local disaster. Accepting HIPAA records from a covered entity does not subject most recipients to any obligations under the HIPAA rules.

Most US-based organizations and grassroots volunteer groups involved in missing persons activities, however, will not fall within the Privacy Act or HIPAA rules and will therefore not be subject to privacy regulation under US law with one caveat. In very rare or unlikely scenarios, other statutes might conceivably apply. For example, if a financial institution were to operate a missing persons database, the privacy rules of the Gramm-Leach-Bliley Act might apply. Similarly, if a commercial organization were to collect personal information through a website directed at children in the United States under the age of 13, the Children's Online Privacy Protection Act would apply to its missing persons activities. In practice, these possibilities are quite remote.

b) European Union

Under the EU Data Protection Directive, the data controller is responsible for compliance with data protection rules and for fulfilling the rights exercised by data subjects.[208] The Directive defines *controller* as the person who determines the purposes and means of personal data processing.[209] Under this broad definition, any missing persons organization that processes

[204] 5 U.S.C. § 552a (m) (2006), http://www.law.cornell.edu/uscode/text/5/552a.
[205] The rule applies to *personal health information* held by covered entities, but its privacy protections generally do not follow with information disclosed to third parties.
[206] 45 C.F.R. pts. 160, 164 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-chapA-subchapC.pdf.
[207] Most components of the US Department of Health and Human Services that provide treatment or pay for health care are covered entities subject to HIPAA rules. The National Library of Medicine, an HHS component, is not a HIPAA covered entity for its routine functions.
[208] See, generally, Art. 29 Data Prot. Working Party, 00264/10/EN, WP 169, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"* (Feb. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
[209] 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, art. 2(d), 1995 O.J. (L 281) 31, 38, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

personal data in the European Union, whether government, corporate, or non-profit, is subject to the regulations set forth in the Directive.

For missing persons information systems, the following organizations may qualify as data controllers:

- Organizations maintaining missing persons databases
- Organizations offering defined search parameters for third-party data
- Organizations conducting online searches

The location of a data controller is also essential for determining the application of national law. Within the European Union, a Member State applies its national law to processing "carried out in the context of an establishment of the controller on the territory of the Member State."[210] If a controller is established in more than one Member State, each establishment of the controller must comply with the applicable national law.[211] A proposed European data privacy regulation would, however, result in a single applicable European level law.

Modern information and communications technologies compound the problems of determining the applicable national law under the EU Data Protection Directive. The Article 29 Working Party (a group established by the EU Data Protection Directive and comprised of the national data protection agencies) expressed the difficulties well in a recent report:

> The complexity of applicable law issues is also growing due to increased globalisation and the development of new technologies: companies are increasingly operating in different jurisdictions, providing services and assistance around-the-clock; the Internet makes it much easier to provide services from a distance and to collect and share personal data in a virtual environment; cloud computing makes it difficult to determine the location of personal data and of the equipment being used at any given time.[212]

Determining the location of data processing activities is a challenge in a world characterized by expansive Internet connectivity and global cloud computing. Not only is it hard to determine the actual location of some processing activities, but that location may vary from day to day or from minute to minute. Nevertheless, each data controller participating in missing persons data activities has a physical location somewhere that likely determines which national law (or laws) applies to that controller.

While all EU Member State laws must meet the standards established in the Data Protection Directive, national privacy laws are not identical. For example, sensitive data protections are not

---

[210] 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, art. 4(1)(a), 1995 O.J. (L 281) 31, 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[211] 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, art. 4(1)(a), 1995 O.J. (L 281) 31, 39, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[212] Art. 29 Data Prot. Working Party, 0836-02/10/EN, WP 179, *Opinion 8/2010 on Applicable Law* 6 (Dec. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

always identical, and laws may conflict. This presents strategic choices to a data controller that has the ability to select a location for its activities. The variance in national laws suggests that there may be an advantage for a data controller to be located in one country rather than another because of (a) the substantive requirements of one country's law (e.g., presence or terms of a security breach notification requirement); (b) different penalties for noncompliance; (c) the Data Protection Authority that has primary jurisdiction to enforce the law or to grant broad processing authority; or (d) other strategic operational reasons.

A complication arises if an organization in an EU Member State processes data under a contractual arrangement with an entity or person in the European Union or in a third country. That organization might be a processor rather than a controller with respect to the data. A processor is someone who processes personal data on behalf of a controller.[213] Privacy obligations attach to processors through their contractual arrangements rather than by direct application of the EU Data Protection Directive's standards.

Determining whether an entity is a controller or processor can be difficult. For example, if an individual within Europe uses someone else's data through an Internet link just as any other user around the world, the data protection status of the data does not change. However, if an EU entity uses, accesses, updates, or otherwise actively processes data from a third country in some independent fashion—perhaps because the data includes information about EU citizens or their relatives—the status may be more ambiguous. Merely processing data on the instructions of a foreign entity would likely leave processor status unchanged. However, if an EU entity on its own initiative modifies the data, it might no longer be a mere processor but rather become a data controller with respect to the data. The status of a controller and a processor depends on the relationship and the legal arrangements between them. The allocation of processing responsibilities among multiple parties determines the application of EU data protection rules.

2. Collection, Purpose Specification, and Use Limitation

Missing persons organizations collect, use, and disclose personal information to each other and to the public in order to assist individuals affected by disasters including the families and friends of those missing. Data protection rules and policies set some boundaries on this personal data processing. This section discusses some of the boundaries.

Under US law, the Privacy Act and the HIPAA rules limit how information may be collected, what purposes the information may be used for, and to whom it may be disclosed. However, as discussed in the previous section, these restrictions apply only to a limited subset of missing persons organizations.

---

[213] 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, art. 2(e), 1995 O.J. (L 281) 31, 38, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. A processor must be a separate legal entity from the controller for which it processes data. Art. 29 Working Party, 00264/10/EN, WP 169, Opinion 1/2010 on the Concepts of "Controller" and "Processor" 25 (Feb. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

In contrast, in the European Union, anyone processing personal data must adhere to regulations requiring that data is fairly and lawfully collected and processed only as provided under the Directive.

a) United States

Many US record keepers engaged in missing persons activities, and especially non-profit record keepers, are not subject to statutory limits on collection, use, or disclosure of the personal information they maintain. Where federal privacy laws apply, some impose restrictions on use, disclosure, or both. First, the Privacy Act of 1974 imposes some limits on collection, use, and disclosure for federal agencies engaged in missing persons activities.[214] Second, the health privacy rules under HIPAA set some additional rules for certain health care entities.

Several federal agencies utilize existing authority[215] to coordinate missing persons activities within the United States and these agencies are subject to some restrictions under the Privacy Act. First, the Act requires collection of information "to the greatest extent practicable" directly from the data subject when the information may result in an adverse determination about the individual under a federal program.[216] This restriction on information collection is not likely to be limiting in disaster situations because adverse determinations are not likely outcomes of missing persons databases, though they are possible if someone listed as missing loses benefits as a consequence.

Second, the Privacy Act of 1974 generally limits an agency's ability to disclose data to third parties, including other federal agencies. The Act does, however, authorize two broad categories of disclosure for records maintained in a system of records.[217] The first category of authorized disclosure relevant to a missing person function is found in subsection (b)(8), which provides for disclosure

> to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual. [218]

---

[214] 5 U.S.C. § 552a (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.

[215] The Act requires that an agency maintain in its records only information relevant and necessary to accomplish a purpose of the agency as determined by statute or Executive Order. 5 U.S.C. § 552a(e)(1) (2006), http://www.law.cornell.edu/uscode/text/5/552a.

[216] 5 U.S.C. § 552a(e)(2) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.

[217] Most of the requirements of the Privacy Act of 1974 attach to a *system of records* maintained by a federal agency. A *system of records* is a group of records controlled by an agency from which information is retrieved by an individual identifier. 5 U.S.C. § 552a(a)(5), *available at* http://www.law.cornell.edu/uscode/text/5/552a. The test set out in the law is a factual one. Whether an agency actually retrieves a record by individual identifier determines whether the Act applies to a collection of records.

[218] 5 U.S.C. §552a(b), *available at* http://www.law.cornell.edu/uscode/text/5/552a. The Act does not cover all personal information held by federal agencies. The Act applies only to *records* maintained in a *system of records* if the agency actually retrieves the records by individual identifier. The definitions of the italicized terms are at 5 U.S.C. § 552a(a). While personal information held by agencies that is not subject to the Privacy Act may often be unrestricted in how it can be disclosed, the likelihood is that most federal agency records relevant to disaster situations will be kept in systems of records subject to the Act.

Some disaster disclosures might qualify under this exception, but the mere sharing of location information in non-emergency situations may not meet the "compelling circumstances affecting the health or safety of an individual" test. Further, the requirement for sending notification of the disclosure would be troublesome and perhaps meaningless in disasters. The provision illustrates how an existing privacy law, even one containing an exception for emergency disclosures, does not adequately address the circumstances of missing persons.

The second category of allowable disclosures gives each agency the ability to establish an additional legal basis for disclosure without consent.[219] The Act allows each agency to define for itself a set of disclosures—called routine uses[220]—that the agency is authorized to make. Under this authority, an agency engaged in any type of disaster relief activity can decide within broad limits how to share information about missing persons.

The Federal Emergency Management Agency (FEMA) is frequently involved in disaster relief and provides an example of how this "routine use" exception can play out in a real disaster scenario. FEMA operates a system of records entitled *National Emergency Family Registry and Locator System (NEFRLS) System of Records*.[221] Two of the routine uses articulated by FEMA for this system allow disclosure:

> I. To the National Center for Missing and Exploited Children and voluntary organizations as defined in 44 CFR 206.2(a)(27) that have an established disaster assistance program to address the disaster-related unmet needs of disaster victims, are actively involved in the recovery efforts of the disaster, and either have a national membership, in good standing, with the National Voluntary Organizations Active in Disaster, or are participating in the disaster's Long-Term Recovery Committee for the express purpose of reunifying families.
>
> J. To Federal, state, local, tribal, territorial, international, or foreign agencies that coordinate with FEMA under the National Response Framework (an integrated plan explaining how the Federal government will interact with and support state, local, tribal, territorial, and non-governmental entities during a Presidentially-declared disaster or emergency) for the purpose of assisting with the investigation on the whereabouts of or locating missing persons.

These routines uses are reasonable examples of how an agency with the requisite mission can use its Privacy Act authority to allow wholesale disclosures to fulfill that mission. In this case, those purposes are to reunite families and help to locate missing persons by cooperating with others engaged in missing persons activities. The FEMA system allows broad disclosure to voluntary organizations and to federal, state, and international agencies involved in missing persons

---

[219] An agency may always disclose a record with the written consent of the data subject. 5 U.S.C. § 552a (b) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.

[220] 5 U.S.C. § 552a(b)(3) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a. A *routine use* is a use compatible with the purpose for which the record was collected. *Id.* at § 552a(a)(7).

[221] "DHS/FEMA–001 National Emergency Family Registry and Locator System (NEFRLS) System of Records," Office of the Federal Register, Privacy Act Issuances online database, accessed July 23, 2012, http://www.ofr.gov/Privacy/2011/fema.aspx#fema1. A statute expressly directs the establishment and operation of the system. 6 U.S.C. § 775 (2006), *available at* http://www.law.cornell.edu/uscode/text/6/775.

activities. The routine use exception also allows FEMA to disclose information as routine uses to the Department of Justice (for litigation); to the Congress (for constituent assistance); to the Department of Homeland Security (for computer security); and to federal, state, local, tribal, territorial, international, or foreign law enforcement agencies (for prosecuting violations of law).[222]

These routine uses, commonly found in many Privacy Act systems of records, are in addition to routine uses that would allow disclosures for missing persons activities. Other federal agencies that engage in disaster relief activities by statutory mandate likely have similarly broad authority to define expansive routine uses and those that do not have a specific statutory mandate might establish a routine use authority under a presidential executive order issued in connection with the disaster. However, an agency seeking to establish a routine use must first publish a notice in the *Federal Register* and consider public comments, a lengthy process.[223] This means that it is not practical to create a routine use following a disaster because a routine use normally cannot take effect until 30 days after publication. Ideally, an agency will anticipate the need for disaster disclosures.

One noteworthy consequence of the FEMA routine use disclosure authority is that the Privacy Act of 1974's disclosure restrictions do not apply to a third party, such as an individual volunteer, who receives a record disclosed under a routine use. Recipients of Privacy Act records can use and disclose the records without restriction under the Act. The only exception to this general rule is when a federal agency discloses a record to another federal agency that maintains the record in its own system of records.[224] In that case, the disclosed record then becomes subject to the disclosure authority of the recipient agency's system of records.

The Privacy Act of 1974 has other relevant provisions. For example, the law allows an agency to maintain only information as is relevant and necessary to accomplish a purpose of the agency as established by law.[225] In addition, the Privacy Act limits internal agency use to officers and employees of the agency that maintains a record who have a need for the record in the performance of their duties.[226]

Other specific laws applicable to an agency may further restrict an agency's authority to disclose personal information pursuant to a routine use, or they may give the agency expanded authority to make disclosures. For example, the HIPAA health privacy rule narrows the authority to disclose records otherwise found in the Privacy Act of 1974 for certain entities. HIPAA generally applies to health care providers and health insurers, and some federal agencies are

[222] National Emergency Family Registry and Locator System, 76 Fed. Reg. 53,918 (noticed Aug. 30, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-08-30/html/2011-22167.htm.
[223] 5 U.S.C. § 552a(e)(4)(d), (e)(11), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[224] Disclosure under the Privacy Act of 1974 would not stop other laws from applying. Thus, information about an individual disclosed from a federal system of records to a hospital covered by the HIPAA privacy rule would normally be subject to the HIPAA rule in the hands of the recipient hospital. In addition, an agency might use a contract or other instrument to control reuse and redisclosure.
[225] 5 U.S.C. § 552a(e)(1) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[226] 5 U.S.C. § 552a(b)(1) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.

covered entities under HIPAA for some functions.[227] The health privacy rule limits use and disclosure without consent, but has many exceptions to those limitations. For example, disclosures of health records to law enforcement, national security agencies, public health agencies, research entities, and many others are allowable under varying procedures and conditions.[228] The health privacy rule does not limit collection in any meaningful way.

Of particular relevance, HIPAA gives a covered entity considerable authority to disclose patient information without patient consent in disaster situations.[229] One provision expressly covers disaster relief:

> (4) Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) and (3) of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.[230]

The effect of this provision is to allow a HIPAA covered entity to cooperate with public or private disaster relief organizations.[231] Information disclosed to a disaster relief organization that is not a covered entity itself is not subject to HIPAA restrictions in the hands of the recipient. Thus, a recipient can use and disclose the information without regard to the HIPAA standards.

---

[227] 45 C.F.R. pts. 160, 164 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-chapA-subchapC.pdf.

[228] 45 C.F.R. § 164.512 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-512.pdf.

[229] In promulgating the health privacy rule, the Department of Health and Human Services said: "We encourage disaster relief organizations to protect the privacy of individual health information to the extent practicable in a disaster situation. However, we recognize that the nature of disaster situations often makes it impossible or impracticable for disaster relief organizations and covered entities to seek individual agreement or authorization before disclosing protected health information necessary for providing disaster relief. Thus, we note that we do not intend to impede disaster relief organizations in their critical mission to save lives and reunite loved ones and friends in disaster situations." 65 Fed. Reg. 82,524 (Dec. 28, 2000), 45 C.F.R. pts. 160 & 164, *available at* https://www.federalregister.gov/articles/2000/12/28/00-32678/standards-for-privacy-of-individually-identifiable-health-information#h-148.

[230] 45 C.F.R. § 164.510(b)(4) (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-510.pdf. Paragraph (b)(2) effectively gives some patients the ability to prevent disaster relief disclosures, while paragraph (b)(3) gives covered entities discretion to disclose when the patient is not present or is incapacitated. The disclosure authority in the disaster relief section is broad, but the general HIPAA rule that disclosures must be limited to the minimum amount of information necessary to accomplish the purpose of the disclosure serves to limit the breadth of any disclosure. 45 C.F.R. § 164.502(b), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-502.pdf.

[231] In the aftermath of Hurricane Katrina in 2005, the Department of Health and Human Services published a bulletin reminding covered entities of their authority. U.S. Dep't of Health and Human Servs. Office for Civil Rights, Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations (2005), http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/katrinanhipaa.pdf.

A separate provision of HIPAA addresses disclosures to a public health authority. This provision allows a covered entity to disclose protected health information to:

> A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.[232]

Some public health functions are relevant to disaster activities, though it is not clear on the face of the rule whether public health activities include locating missing persons. However, HIPAA's main disaster relief disclosure provision is broad enough to allow disclosures to public health authorities engaged in appropriate disaster relief efforts, including locating missing persons.

For missing persons organizations that are neither federal agencies nor HIPAA covered entities, no federal privacy laws apply. Importantly, for the relevant federal agencies and health care providers engaged in disaster relief, the federal privacy laws are not likely to erect any insurmountable barriers to cooperation with missing persons organizations.

b) European Union

The standards in the EU Data Protection Directive require Member States to establish privacy rules covering collection, use, and disclosure. The general policy that the Directive implements is that anyone processing personal data must respect privacy, must process data fairly and lawfully, and must have consent or a lawful reason to process the data. The Directive states that "personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes."[233] This is a sharp contrast with the United States, where most record keepers face no similar statutory privacy barrier to processing.

Another Directive provision lays out legitimate purposes for data processing. One basis for processing is the unambiguous consent of the data subject,[234] but consent is infrequently an option for missing persons activities.

---

[232] 45 C.F.R. § 164.512(b)(1)(i) (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-512.pdf.

[233] 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, art. 6(1)(b), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. The Directive's incompatibility standard and the definition of a routine use under the Privacy Act of 1974 both suggest a significant degree of vagueness. A *routine use* is a disclosure "compatible with the purpose" for which a record was collected. The *compatible standard* and the *incompatible standard* share a common root. Both standards reflect the fundamental difficulty of establishing a bright-line rule defining allowable disclosures for disparate activities.

[234] 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, art. 7(a), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

The Directive's other processing justifications potentially relevant to missing persons organizations allow processing when it is necessary:

- "for compliance with a legal obligation to which the controller is subject"[235]
- "in order to protect the vital interests of the data subject"[236]
- "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed"[237]
- "for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject"[238]

Under the first prong of this justification, the entity must find the processing necessary. While the meaning of necessary is subject to national interpretation and thought to be a high standard, the compelling urgency expressed by individuals worldwide to learn of the safety and location of their loved ones following natural disasters ought to rise to the level of necessity for most missing persons information processing.

Next, the processing must satisfy either a vital interest, a public interest, or a legitimate interest. The processing of missing persons information could qualify under each of the interest standards in the context in which they appear.

An Article 29 Working Party document discusses what it means to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent. The Working Party concludes:

> The processing must relate to essential individual interests of the data subject or of another person and it must—in the medical context—be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions. Accordingly, this exception could be applied only to a small number of cases of treatment and could not be used at all to justify processing personal medical data for purposes other than treatment of the data subject such as, for example, to carry out general medical research.[239]

---

[235] 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, art. 7(c), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[236] 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, art. 7(d), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[237] 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, art. 7(e), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[238] 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, art. 7(f), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[239] Art. 29 Data Prot. Working Party, 00323/07/EN, WP 131, *Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR)* 9 (Feb. 15, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.

This suggests that the vital interest test might be available to justify individual actions but not large-scale data activities.

A strong case can be made that data subjects have a vital interest in sharing information about their status with remote relatives in disaster situations. Similarly, connecting individuals with missing relatives and friends appears to be a task in the public interest. Finally, a data controller seeking to connect families and missing persons pursues a legitimate interest. In addition, the non-profit nature of missing persons activities—no matter the actual profit or non-profit status of the data controller carrying out the function—underscores that both public and legitimate interests are involved. Under these standards, the processing of personal information by a missing persons organization would likely be consistent with the EU Data Protection Directive.

However, many data controllers holding information that may be relevant to missing persons activities are not primarily missing persons organizations. Often these controllers have not established in advance that their data processing may have value following a natural disaster. Questions therefore arise whether the disclosure of their records for missing persons purposes is allowable under data protection rules.

For EU purposes, missing persons processing by other data controllers would, hopefully, qualify under one or more of the vital interest, public interest, or legitimate interest standards just as processing by missing persons organizations would. The EU Data Protection Directive provides that information collected for specified, explicit, and legitimate purposes may not be further processed "in a way incompatible with those purposes."[240] The processing of information not explicitly collected for missing persons purposes is potentially compatible with the original purposes in most cases because of the humanitarian objective of the disclosure. This interpretation, however, likely requires confirmation in each Member State.

The issue is well-illustrated by the New Zealand temporary code, which expressly authorized data controllers to collect, use, or disclose personal information for purposes directly related to the government response to the Christchurch earthquake emergency.[241] The code effectively authorized appropriate disclosures by other data controllers for disaster purposes. Whether the New Zealand code provided new authority or merely confirmed that existing law was broad enough to allow for disaster disclosures, the policy and the result are the same.

There is a strong case to be made that processing of personal information by missing persons organizations and by other data controllers engaged in missing persons activities is permissible under the EU Data Protection Directive. However, in both cases, official clarification from national legislation or from a Data Protection Authority would be reassuring to all so that no one

[240] 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, art. 6(1)(b), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[241] Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) (N.Z.), Feb. 24, 2011, *available at* http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-incorporating-Amendments-No-1-and-No-2.doc.

need raise the question in the middle of a disaster.[242] Confirmation would be particularly useful for disclosure models that provide broad public access to the missing persons information. Collecting personal information—especially information of the breadth included in missing persons databases—for public access is not a familiar model of data processing. Because it appears that at least some public access to the information may be essential to carry out the mission of reuniting families, clarification that the processing meets legal standards would be reassuring.

This is not to suggest that a natural disaster is *carte blanche* to process data without any regard to privacy obligations. The processing of missing persons data is still subject to the privacy rules applicable to data controllers. An important element of these policies is the durational limit placed on processing activities. Policies that can adapt to allow processing activities in emergency circumstances need not remain loosened indefinitely. When an emergency ends, restoring traditional privacy standards and relying more on consent are part of an appropriate balance of interests.

Missing persons organizations also may face more routine requests or demands for personal information from law enforcement agencies, public health agencies, health care providers, litigants, and others who may seek to avoid normal restrictions on their access to information. Here, too, missing persons organizations are in a similar situation to other data controllers, and they must take the range of possible disclosures into account in privacy policies and in operating rules. More traditional privacy analyses and balancing of interests are likely to apply to these disclosure possibilities. When these potential disclosures do not relate to emergency circumstances, traditional balancing of interests may apply as they would with any other record keeper.

3. Rights of Individuals: Notice, Consent, Access, and Correction

Missing persons organizations also must be aware of rights granted to data subjects by data protection regimes and must respect these rights where applicable. The rights typically include notice, access, the ability to seek correction of personal data, and the ability to give consent or object to processing of data. None of these rights is absolute, and exceptions typically exist. In the United States, there is no universal privacy law, and many data subjects have no legally required individual privacy rights. In the European Union, however, data subjects are granted a comprehensive list of rights that processors must respect.

---

[242] The 2002 ICRC Workshop reached a similar conclusion. International Committee of the Red Cross [ICRC] Electronic Workshop on the Legal Protection of Personal Data & Human Remains, Apr. 2-May 6, 2002, *The Legal Protection of Personal Data & Human Remains: Final Report and Outcome* 12 (July 2002), *available at* http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf. ("In obtaining data on natural living or deceased persons from private or public sources, assurances should thus be sought that the data may be disclosed because:

- the data were collected to establish the identity, whereabouts or fate of missing persons;
- disclosure is not incompatible with the purpose for which the data were collected or obtained;
- the data are derived from publicly accessible sources (such as public or professional registers or published directories); or
- the disclosure serves a vital interest of the data subject or a close relative of the data subject and the data subject is physically or legally incapable of consenting to the disclosure.")

a) United States

The absence of a universal data protection law in the United States means that data subjects have no uniform rights. For many types of records and for many types of record keepers, no law gives data subjects any privacy rights at all.

A few laws do provide rights for certain types of records or data subjects. The Privacy Act of 1974[243] requires public notice of record keeping activities[244] and mandates some disclosures to data subjects at the time of data collection.[245] The law gives citizens and aliens lawfully admitted for permanent residence (but not foreign nationals) a right of access to many personal records held by federal agencies.[246] The law provides the right to seek amendment of records as well.[247] A data subject may consent to disclosure, but the statute and agency implementation provide for nearly all disclosures so that agencies rarely seek consent in practice.[248]

The HIPAA health privacy rule applicable to health care providers and health insurers gives all data subjects (including foreign nationals) rights of access,[249] amendment,[250] and consent.[251] HIPAA provides for a public notice of information practices.[252] Data subjects may consent[253] to or object to disclosures.[254] As with the Privacy Act of 1974, the rights to consent or object often have limited practical value. A few other laws provide comparable rights for some other records, but legally enforceable data subject privacy rights are not common in the United States.

Some private sector record keepers in the United States choose to give data subjects rights of notice, access, amendment, or consent. Because of variability in practice, it is difficult to describe the extent to which data subjects have these rights or whether they can enforce the rights

[243] 5 U.S.C. § 552a (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a. The federal Freedom of Information Act (FOIA) provides a foreign national with a process to access federal agency records, including records about himself or herself. 5 U.S.C. § 552, *available at* http://www.law.cornell.edu/uscode/text/5/552. The law provides a partial substitute for rights available to citizens and resident aliens under the Privacy Act of 1974. However, the FOIA does not provide correction opportunities. At times, federal agencies will as a matter of discretion honor requests from foreign nationals for access and correction in accordance with Privacy Act of 1974 procedures. However, even if an agency accepts a request on a discretionary basis, a foreign national may have no right to appeal or enforce an agency decision.
[244] 5 U.S.C.§ 552a(e)(4) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[245] 5 U.S.C.§ 552a(e)(3) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[246] 5 U.S.C.§ 552a(d) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[247] 5 U.S.C.§ 552a(d)(2) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[248] 5 U.S.C.§ 552a(b) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.
[249] 45 C.F.R.§ 164.524 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-524.pdf.
[250] 45 C.F.R.§ 164.526 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-526.pdf.
[251] 45 C.F.R.§ 164.508 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-508.pdf.
[252] 45 C.F.R.§ 164.520 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-520.pdf.
[253] 45 C.F.R.§ 164.508 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-508.pdf.
[254] 45 C.F.R.§ 164.524 (2011), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-524.pdf.

in any effective way. On the Internet, it has become a more common practice in recent years for websites (commercial and non-commercial) to post privacy policies that offer data subjects notice of privacy practices, the ability to request access to records, and the opportunity to request amendment. These practices are not universal, and the promises offered in privacy policies may not be legally enforceable, especially for non-commercial websites. Further, voluntary privacy policies and terms of service are typically changeable at any time for any reason by a website operator. State laws occasionally impose requirements on commercial website operators to provide some data subject rights.

It is possible for a website in the United States—particularly a non-commercial website—to process personal data without providing data subjects any rights at all. The processing of personal data for missing persons purposes by organizations that are neither federal agencies nor health care providers faces few, if any, statutory data protection mandates in the United States.

b) European Union

The EU Data Protection Directive provides data subjects with a range of rights that data controllers must respect. These rights include a right of access, right of correction, right to notice, and right to consent to processing. Each is discussed in turn below.

The Directive provides subjects with the right to access their records and the right to correct the records if inaccurate or incomplete.[255] A data subject may also ask for the erasure or blocking of data if processing does not comply with the Directive's standards "in particular because of the incomplete or inaccurate nature of the data."[256]

Data subjects also are granted a right to notice of data processing, which can be complex for missing persons activities. When a data controller collects information from the data subject, the EU Data Protection Directive's standards oblige the data controller to provide basic information about the processing, including the identity of the controller, the purposes of the collection, the

[255] 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, art. 12, 1995 O.J. (L 281) 31, 42, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. The 2002 ICRC Workshop considered allowing third parties (e.g., relatives) to exercise data subject access rights for "humanitarian reasons." This may be a possibility, although providing information to these third parties as a disclosure rather than as an exercise of data subject access rights may work just as well. See International Committee of the Red Cross [ICRC] Electronic Workshop on the Legal Protection of Personal Data & Human Remains, Apr. 2-May 6, 2002, *The Legal Protection of Personal Data & Human Remains: Final Report and Outcome* 6 (July 2002), *available at* http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf. ("For humanitarian reasons—to help locate missing persons and human remains—it may therefore be necessary for data protection legislation in some States to be amended to allow access by third parties to such personal information for humanitarian reasons. Provisions in data protection legislation that allow disclosure 'in the public interest' may be too vague to ensure that third parties seeking to locate missing persons can obtain access to the necessary information. These third parties could include family members or others with a legitimate interest in helping to locate the person. Alternatively, freedom of information legislation could be amended to allow certain persons a right of access to information about missing persons if that is in the interests of the missing person or family members, or if it would otherwise serve the public interest.")

[256] 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, art. 12(a), 1995 O.J. (L 281) 31, 42, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

recipients of the data, and the rights of the data subjects, at the time of collection.[257] When information comes from a source other than the data subject, the Directive's standards call for notice "at the time of undertaking the recording of personal data" or at the time of the first disclosure to a third party.[258] When data is collected from a third party, notice is not required if it would be "impossible" or "involve a disproportionate effort."[259] For data controllers of missing persons information, these exceptions to the notice requirement likely apply because the data subjects are, by definition, missing. However, to the extent that missing persons information is collected from known individuals (e.g., emergency workers, friends, etc.), those data subjects may be entitled to notice.

When notice is required in a missing persons context, compliance will be a particular challenge. A missing persons organization may collect information from disparate sources, may process it in various locations, may share the information with governmental or other organizations, and may disclose the information publicly. Often many uses of the data will be unknown at the time of collection. An individual seeking information about another might be the source of some information. Public authorities or anyone else might publicly post information about found persons. Disclosure could occur through the publication of a list of found individuals with current locations, through sharing with other missing persons organizations, or through an inquiry–response system that supports queries about the location and status of individuals identified by the inquirer.

For missing persons, notice to a data subject would in many circumstances be impossible because the location of the individual is unknown or because communications are not possible. Providing notice would also likely involve a disproportionate effort because of the difficulty or expense of providing notice to an individual at the site of a disaster. A data protection notice would be a low priority at a time when resources are scarce and communications are challenging.

Data subjects also have a right to consent to processing. Like the right to notice, this right can pose logistical hurdles for missing persons activities. Missing persons organizations often process personal data about individuals without notice to the individuals and without consent. Obtaining consent from a missing person is clearly impractical at best and impossible at worst.[260]

---

[257] 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, art. 10, 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[258] 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, art. 11(1), 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[259] 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, art. 11(2), 1995 O.J. (L 281) 31, 42, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. Other exceptions cover recording or disclosure expressly required by law. In cases where notice is not required, Member States provide "appropriate safeguards." *Id.*

[260] The 2002 ICRC Workshop discussed the difficulty of obtaining consent. International Committee of the Red Cross [ICRC] Electronic Workshop on the Legal Protection of Personal Data & Human Remains, Apr. 2-May 6, 2002, *The Legal Protection of Personal Data & Human Remains: Final Report and Outcome* 6 (July 2002), *available at* http://www.icrc.org/eng/assets/files/other/icrc_themissing_072002_en_1.pdf. ("Given the nature of the information relative to missing persons, obtaining the consent of subjects on whom information is collected and processed may be inappropriate or impossible. The collection of personal data for the purpose of locating a missing

The processing may nevertheless be consistent with the Directive's policy under the impossibility or disproportionate effort standards.

This discussion of the rights of data subjects is not exhaustive. It is foreseeable that not all individuals whose information resides in a missing persons database will be missing. A database may maintain information on aid workers, individuals who provide data, individuals providing assistance ("John Doe is living at the home of Mary Smith"), or others. For some of these individuals, missing persons organization may be more able to provide standard data protection rights without relying on exceptions or special circumstances. If individuals provide their own information directly, it may not be difficult to provide notice at the time of collection through a website. If information about aid workers comes through a third-party assistance organization, it may take some cooperation to ask the organization to provide the notice.

4. Export Controls

The international transfer of personal information is a basic activity for all organizations involved in missing persons activities. Transfers may not arise in every instance, but many disasters affect more than one country, result in the movement of individuals from one country to another, or give rise to inquiries across borders. For this reason, the imposition of limits on the export of personal data is a significant issue. This section reviews the export restrictions in place under both US and EU law. In the United States there are no relevant export restrictions on missing persons information systems. The European Union however has complex regulations about data export that may limit many transfers of personal information in missing persons activities.

a) United States

US privacy law imposes few personal data export restrictions and none known to be relevant to missing persons activities.[261] The location of data storage may be a disclosure requirement in privacy notices under some laws. Security requirements may make some international transfers more challenging in some administrative or technical ways. However, in general, nothing in US law prevents record keepers in commercial or non-profit organizations from exporting personal data collected for missing person purposes to another country regardless of the privacy rules applicable in that country.

b) European Union

The European Union treats personal data exports much differently than the United States. The European Union limits the export of personal data from the European Union to third countries, though personal data can move from third countries to EU missing persons organizations

---

person can, however, be considered to be clearly in the interests of that person. Hence, personal information to be used for that purpose could be collected without the individual's consent or knowledge.")

[261] Some data export restrictions exist, but they appear to be rare. For example, Internal Revenue Service rules prohibit disclosure of Social Security Numbers to a tax return preparer outside the United States even with taxpayer consent. 26 C.F.R. § 301.7216-3(b)(4) (2012), *available at* http://www.gpo.gov/fdsys/pkg/CFR-2012-title26-vol18/pdf/CFR-2012-title26-vol18-sec301-7216-3.pdf.

because EU data protection laws do not specifically restrict data imports. A major part of the EU Data Protection Directive specifically addresses the transfer of personal data to third countries that are not EU Member States. The policy objective of data export restrictions is clear: personal data protected in the European Union may lose its protection if transferred to a third country that does not provide similar legal protections. A recital in the Directive states the policy thusly:

> Whereas … the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited.[262]

Articles 25 and 26 of the Directive establish the principles and procedures behind export controls and set out permissible derogations from those controls. The law and practice governing transfers is one of the most complex parts of the Directive and national laws of Member States.

Article 25 provides that data transfers to a third country are permissible if the third country "ensures an adequate level of protection."[263] The details and procedures for an adequacy determination are not simple. The European Commission recognizes twelve countries that provide adequate protection. These are Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, Paraguay, and Uruguay. In addition, the Commission recognizes as adequate the transfer of personal data under the US Department of Commerce's Safe Harbor Framework and the transfer of Air Passenger Name Records to the US Bureau of Customs and Border Protection.[264]

Data transfers among EU Member States and data transfers from EU Member States to a data controller in a country found adequate are permissible. However, that does not end the data export inquiry. In order for a third country to be adequate, the third country must itself impose data export restrictions. As explained by the Article 29 Working Party, one of the basic requirements for a finding of adequacy for data protection in a third country is a restriction on further transfers.

> [F]urther transfers of the personal data from the destination third country to another third country should be permitted only where the second third country also affords an adequate level of protection. The only exceptions permitted should be in line with Article 26 of the directive.[265]

---

[262] 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 57, 1995 O.J. (L 281) 31, 37, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[263] 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, art. 25(1), 1995 O.J. (L 281) 31, 45, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[264] European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated Apr. 10, 2012).

[265] Art. 29 Working Party, XV D/5020/97-EN final, WP 4, *First orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy* 3(i) (June 26, 1997), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf.

Thus, locating a missing persons activity in an adequate country does not completely solve the export issue.

In the absence of adequacy, EU law may still allow data exports. Article 26 of the EU Data Protection Directive provides exceptions. The exceptions that may be helpful in a missing persons context are discussed in the following:

- **Consent.** Transfers are permissible when the data subject has given unambiguous consent to the transfer.[266] As previously indicated, consent is not likely to be practical for many missing persons disclosures, but might be helpful in the case of personal information related to data submitters, such as relief workers or family members.
- **Contractual Performance.** Transfers are permissible when necessary for the performance of a contract between the data subject and the controller.[267] Transfers are also permissible when necessary for the conclusion of or performance of a contract concluded in the interest of the data subject between the controller and a third party. Missing persons activities do not involve contracts with data subjects, but transfers under agreements between controllers and missing persons organizations to help locate missing persons may qualify for this exception.
- **Contractual Clauses.** Transfers to a data controller in a country not found to be adequate can occur if accomplished pursuant to contractual clauses meeting standards established by the European Union.[268] Missing persons organizations sharing information among themselves might use the model contracts approved by the EU Commission.[269] An alternative is to develop contracts specifically for transfers among missing persons organizations.[270] However, contracts would allow transfers only between the parties to the contracts. Contracts might not authorize disclosures to others (e.g., individuals, public health agencies, other disaster relief organizations, health care providers, etc.) so that the benefits of exports via contracts would be limited.
- **Register.** Personal data from a public register may be transferred to the extent allowed by law.[271] A recital in the Directive states that "a transfer should not involve the entirety of

[266] 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, art. 26(1)(a), 1995 O.J. (L 281) 31, 46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[267] 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, art. 26(1)(b), 1995 O.J. (L 281) 31, 46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[268] European Commission, *Model Contracts for the Transfer of Personal Data to Third Countries*, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (last updated Feb. 3, 2012).
[269] Commission Decision of 15 June 2001, 2001/497/EC, *On Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC*, 2001 O.J. (L 181) 19, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:en:PDF.
[270] 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, art. 26(2), (3), 1995 O.J. (L 281) 31, 46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[271] 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, art. 26(1)(f), 1995 O.J. (L 281) 31, 46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

the data or entire categories of the data contained in the register."[272] Information from a public register may be useful to a missing persons organization on occasion.

Two remaining provisions in Article 26 offer some prospect of help for missing persons data exports. The first allows a transfer necessary or legally required on important public interest grounds.[273] The second provision allows a transfer necessary in order to protect the vital interests of the data subject.[274]

Both of these transfer permissions share some common characteristics. First, the standards in both cases are quite high. In one case, the standard is "necessary or legally required" and in the other case "necessary." Since missing persons disclosures are not likely to be legally required, this leaves the necessary standard as a hurdle for both. Second, both authorities use broad and uncertain phrases as the touchstone for disclosure, "public interest grounds" in one instance, and "vital interest of the data subject" in the other. Third, there appears to be little in the way of commentary or explanation for either transfer authority. Fourth, transfers allowed under the two provisions do not appear to have downstream controls that limit use of the information by the recipients. Thus, if missing persons can transfer personal information under this authority, recipient organizations would not face controls over use and redisclosure of the information.

These two transfer permissions are, in any case, subject to national interpretations as indicated by two recitals to the Directive. One recital addresses a similar public interest standard in a different context and states that it is for national legislation to determine whether a controller carrying out a task in the public interest should be a public administration or another national or legal person.[275] A second recital also using the public interest standard in another context suggests that it is up to Member States to decide when the public interest authorizes derogation from a provision of the Directive.[276] Together, these two recitals suggest that Member States have broad authority to decide about interpretation of the public interest standard.

A third recital in the Directive addresses the data transfer issue directly. It gives an example of an important public interest that may require protection: "for example in cases of international

---

[272] 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 58, 1995 O.J. (L 281) 31, 37, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[273] This section also allows transfers necessary or legally required for the establishment, exercise, or defense of legal claims. This authority is not useful in a missing persons context. 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, art. 26(1)(d), 1995 O.J. (L 281) 31, 46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[274] 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, art. 26(1)(e), 1995 O.J. (L 281) 31, 46, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[275] 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 32, 1995 O.J. (L 281) 31, 34, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[276] 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 34 (processing sensitive categories of data), 1995 O.J. (L 281) 31, 34, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

transfers of data between tax or customs administrations or between services competent for social security matters."[277] While there is nothing directly addressing missing persons transfers in the Directive, there is no specific reason to think such transfers would be outside the scope of permissible public interest transfers.

[277] 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 58, 1995 O.J. (L 281) 31, 37, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Box 3: The US–EU Safe Harbor Framework

Could the Safe Harbor Framework operated by the US Department of Commerce help with the transfer of personal information from EU Member States to a missing persons organization located in the United States? The answer is clearly no for non-profit organizations.

The Safe Harbor Framework resulted from negotiations between the Department and the European Commission[278] to address problems with the international transfer of personal information from the European Union to the United States. It allows some US organizations to publicly declare that they will comply with the requirements. A data controller can transfer personal data from Europe to a US company in the Safe Harbor because the European Commission found the Safe Harbor program adequate.[279]

However, only organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DOT) are eligible to participate.[280] Action by the FTC or by DOT is the principal means of enforcing compliance with a Safe Harbor promise. This limitation means that many companies and organizations that transfer personal information internationally cannot qualify for participation either in whole or in part.

The Safe Harbor Framework cannot help any non-profit because non-profits do not fall within the jurisdiction of either agency. A private sector company in the Safe Harbor could cite its membership as grounds for accepting data exports from an EU Member State. However, the Safe Harbor Framework itself includes restrictions on onward transfer of personal information that roughly approximate requirements under the Safe Harbor Framework.[281] No one in the Safe Harbor is free from restrictions on forward transfers of personal data, and even those commercial companies in the Safe Harbor would face data export challenges.

Within the context of the Missing Persons Community of Interest (MPCI), Google is an example of an organization providing missing persons information services that is both a commercial company subject to FTC jurisdiction and on the US–EU Safe Harbor Framework list.[282] Thus, information sharing companies like Google may be able to rely on the Safe Harbor to support data exports from EU Member States to the United States.

---

[278] US–EU Safe Harbor documents are at http://www.export.gov/safeharbor/eg_main_018237.asp (last updated Apr. 11, 2012).

[279] European Commission, *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, accessed May 24, 2012, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[280] "Any US organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or US air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. Organizations generally not subject to FTC jurisdiction include certain financial institutions, …, telecommunication common carriers, labor associations, *non-profit organizations …* " [emphasis added]. "Welcome to the US-EU & US-Swiss Safe Harbor Frameworks," US Dep't of Commerce, Export.gov, last updated Apr. 11, 2012, http://export.gov/safeharbor/.

[281] "To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles." "US–EU Safe Harbor Overview," US Dep't of Commerce, Export.gov, last updated Apr. 26, 2012, http://export.gov/safeharbor/eu/eg_main_018476.asp.

[282] Safe Harbor Google Company Information Page, US Dep't of Commerce, Export.gov, accessed July 23, 2012, http://safeharbor.export.gov/companyinfo.aspx?id=13346.

5. Sensitive Data (Health, Race, Ethnicity, Religion, Political Views)

It is inevitable that missing persons organizations will process some sensitive data. Basic identification information about individuals will often include racial or ethnic descriptions. Health information will also be part of some records. Privacy rules often regulate the processing of sensitive data, and missing persons organizations need to be aware of how their activities may implicate these laws. In the United States there are few, if any, restrictions on how missing persons organizations may use or process sensitive data. By contrast, the European Union and its Member States have carved out several categories of sensitive data and have place restrictions on how that information may be processed.

a) United States

US law does not define any general categories of sensitive data. Each sectoral privacy law defines the terms for specific types of records or for specific record keepers but most do not appear to restrict the processing of sensitive data. Even health data, which most people in the United States would likely consider sensitive, is regulated in only limited ways. HIPAA rules normally regulate only health data held by health care providers and insurers, and the restrictions rarely apply to a third-party recipients.

The HIPAA rule allows a covered entity to make numerous disclosures without consent under specified conditions and procedures. For disaster relief, HIPAA permits disclosures about an individual without that individual's consent to a disaster relief entity to notify or assist in the notification of a family member, personal representative, or another person responsible for the care of the individual.[283] Here, too, the HIPAA restrictions do not follow the information downstream, and HIPAA penalties do not apply to recipient organizations. Whether a data subject or anyone else could enforce the purpose standard in the HIPAA rule against a disaster relief entity is speculative.[284]

In general, however, US law rarely defines or restricts sensitive categories of information, though state laws may contain separate restrictive rules. Processing of sensitive information by missing persons organizations is not likely to be restricted in any material way.

---

[283] 45 C.F.R. § 164.510(b)(4) (2012) ("Use and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph [b][1][ii] of this section. The requirements in paragraphs [b][2] and [3] of this section apply to such uses and disclosure to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances."). The purpose language is at *Id.* § 164.510(b)(1)(ii) ("A covered entity may use or disclose protected health information to notify, or assist in the notification of [including identifying or locating], a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs [b][2], [3], or [4] of this section, as applicable."), *available at* http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=0e9e1d1cd738cf748301308c6f8b7d12&rgn=div8&view=text&node=45:1.0.1.3.79.5.27.7&idno=45.

[284] Neither the HIPAA statute nor the HIPAA rule provides a private right of action, so a legal basis for an action against a disaster relief entity would have to be found elsewhere in federal or state law.

b) European Union

The European Union has a broad, and generally applicable, rule about the processing of special categories of data, more commonly called sensitive data.[285] The basic provision states:

> Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[286]

Definitions of sensitive information vary from country to country and from culture to culture. The EU Data Protection Directive allows Member States to add additional categories of sensitive information, and some have done so for criminal records, genetic information, and biometric data.[287]

Two provisions in Article 8 are particularly helpful to the processing of sensitive information for missing persons purposes. One allows processing when "necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent."[288] The precise boundaries of a data subject's vital interests are not clear. Processing of sensitive information in the context of missing persons activities may qualify, but the requirement that the data subject be physically or legally incapable of giving consent may be harder to satisfy. A data subject unavailable because of a disaster or similar circumstances may be incapable of giving consent. It seems possible to read the Directive to support missing persons processing, but a physical incapability may not be the same as being unavailable.

A second provision allows Member States for reasons of substantial public interest to establish exceptions by law or decision of the supervisory authority.[289] This test is likely easier to satisfy

---

[285] 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, art. 8, 1995 O.J. (L 281) 31, 40-41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[286] 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, art. 8(1), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML. The definitional problems for the various special categories are challenging, but they are not important here based on assumptions that some missing persons data will be sensitive and that missing persons organizations will need legal authority for processing. The Article 29 Working Party discusses some of the definitional issues in Ref. Ares(2011)444105, *Advice Paper on Special Categories of Data ("Sensitive Data")* (Apr. 20, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf at pt. II.3.2.1 at 8 and III.1 at 10.

[287] See Art. 29 Data Prot. Working Party, Ref. Ares (2011) 444105, *Advice Paper on Special Categories of Data ("Sensitive Data")* 7 (Apr. 20, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf.

[288] 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, art. 8(2)(c), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[289] 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, art. 8(4), 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

for the purposes of missing persons activities. Finding missing persons and providing information to relatives is likely to meet a public interest test. However, the Directive also requires a legally based exception. The exception could potentially be a national law or a decision by a supervisory authority. New Zealand offers a precedent for a decision by a supervisory authority following a natural disaster, although the temporary Christchurch earthquake code did not address sensitive information.

Several other exceptions authorizing the processing of sensitive data are potentially relevant to missing persons. Sensitive data may be processed:

1. With explicit consent of the data subject (unless consent is not allowed under national law).[290] While consent may be a possibility at times, it will certainly not provide a complete solution to the needs of missing persons organizations.
2. If conducted by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious, or trade union aim that relates to its members and some other persons and disclosures only happen with consent. This provision applies to many non-profits, but it covers membership organizations, not missing persons organizations.[291]
3. If the data subject clearly made the information public or if the information is necessary for legal claims. This provision may help, if at all, only in rare instances.[292]
4. If processed by a health professional for preventive medicine, diagnosis, treatment, or management of health care services.[293] This provision will not justify most processing by missing persons organization.

[290] 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, art. 8(2)(a), 1995 O.J. (L 281) 31, 40, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[291] 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, art. 8(2)(d), 1995 O.J. (L 281) 31, 40-41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[292] 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, art. 8(2)(e), 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.
[293] 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, art. 8(3), 1995 O.J. (L 281) 31, 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Box 4: Children's Information

Children's information is sometimes treated differently than adults' information under privacy laws and organizational practice. For example, the US Children's Online Privacy Protection Act,[294] a law not specifically relevant to disaster activities, establishes separate rules for the online processing of information about children under the age of 13. There is no consensus about the age at which children's information should receive special consideration for privacy. It is not always easy to determine if or how an organization treats children's information, and it is not essential for this report to do so as each organization makes its own policy.

The International Committee of the Red Cross (ICRC) systematically collects data about children separated from their families in order to locate, protect, assist, and reunite them. The ICRC distinguishes between data that it publicly displays to help identify a child's relatives and data considered to be sensitive, such as the address or contact details of the child and information necessary to check the veracity of a claim. The ICRC does not publicly display sensitive data and shares it only with professionals in charge of assisting children and reunifying families.[295]

The US government also treats personal information about missing children differently, particularly in the post–Hurricane Katrina Emergency Management Reform Act. Due to the difficulties displaced individuals experienced in reuniting with family and household members during the hurricane, Congress mandated the establishment of the National Emergency Family Registry and Locator System (NEFRLS), and the National Emergency Child Locator Center (NECLC).[296] Following a Presidential declaration of national disaster, the Federal Emergency Management Agency (FEMA) activates the NEFRLS, a web-based system that allows displaced adults[297] to voluntarily register and share information on their well-being status or location with specified family members or friends. NEFRLS is subject to the Privacy Act of 1974 because FEMA, a federal agency, operates it.

Continued on next page

[294] 15 U.S.C. § 6501 et seq. (2006). The regulations are at 16 C.F.R. pt. 312, *available at* http://www.ftc.gov/privacy/privacyinitiatives/COPPARule_2005SlidingScale.pdf.
[295] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011, (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[296] 6 U.S.C. § 774 (2006); U.S. Dep't of Homeland Sec. (DHS), Fed. Emergency Mgmt. Agency (FEMA), DHS/FEMA/PIA-014, Privacy Impact Assessment for the National Emergency Family Registry and Locator System (NEFRLS) 1 (2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_nefrls.pdf.
[297] The Act defines a "displaced adult" as an individual 21 years of age or older who is displaced from the habitual residence of that individual as a result of a declared event. 6 U.S.C. § 774 (a)(3) (2006), *available at* http://www.law.cornell.edu/uscode/text/6/774.

Box 4: Children's Information continued

FEMA collaborates with the National Center for Missing and Exploited Children (NCMEC)[298] to activate the NECLC and directs anyone searching for or reporting on a missing child under 21 years of age to the NECLC.[299] The NCMEC operates the NECLC with an overall mandate to help reunite children with their parents and guardians. When a natural disaster occurs, the NECLC establishes a hotline to receive reports of displaced children and a website to provide information about them. It deploys staff to a declared disaster area to gather information about displaced children; partners with federal, state, and local law enforcement agencies; and gives the public information about additional resources. It directs those seeking displaced adults to the NEFRLS system operated by FEMA. Because the NCMEC is not a federal agency, its records for children are not subject to the Privacy Act of 1974.

V. Options and Strategies for Missing Persons Organizations and Privacy Policy Makers

Those engaged in missing persons activities and those responsible for establishing and enforcing privacy standards can work together to find ways to accommodate all of the interests at stake while allowing modern technology to meet the information needs that arise following natural disasters. This section sets out options and strategies for consideration by different organizations that play a role in missing persons activities and in privacy.

A. Missing Persons Community of Interest

The MPCI already provides leadership on privacy,[300] and that work should continue in the future. Specific activities may include:

[298] In 1984, Congress established a national resource center and information clearinghouse for missing and exploited children through the Missing Children's Assistance Act and designated the National Center for Missing and Exploited Children to fulfill this role. Missing Children's Assistance Act, Pub. L. No. 98–473, Oct. 12, 1984, 98 Stat. 1837, sec. 404, 42 U.S.C. § 5773 (1984) (prior to 1999 amendment). See "The National Center for Missing and Exploited Children [NCMEC] Mission and History," accessed August 7, 2012, http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362. The organization works in partnership with federal agencies, including the Department of Justice and Federal Bureau of Investigation, to find missing children, reduce child sexual exploitation and prevent child victimization. NCMEC is a private non-profit organization, and receives annual grants from the US Department of Justice's Office of Juvenile Justice and Delinquency Prevention. 42 U.S.C. § 5773 (2006), *available at* http://www.law.cornell.edu/uscode/text/42/5773.

[299] 6 U.S.C. § 775 (2006), *available at* http://www.law.cornell.edu/uscode/text/6/775; US Dep't of Homeland Sec. (DHS), Fed. Emergency Mgmt. Agency (FEMA), DHS/FEMA/PIA-014, Privacy Impact Assessment for the National Emergency Family Registry and Locator System (NEFRLS) 2 (2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_nefrls.pdf.

[300] See, e.g., "Missing Persons Community of Interest Code of Conduct, Engagement Framework and Existing Resources," accessed June 19, 2012, https://docs.google.com/document/d/1kDqTVbGraI4x0L-7UzPDuU2IXxZKpGjcWCFUMpJLxUQ/edit?hl=en&authkey=CKfZlzA.

1. Assist in Privacy-Friendly Design Choices

The design of an infrastructure for sharing missing persons information implicates different privacy concerns and creates varying legal responsibilities for different parties. Some designs more carefully balance privacy interests than others, and some designs create more onerous compliance obligations.

Several examples illustrate the point:

- **Search protocol.** A design that defines a set of data held by each participant and a search protocol to display the data online has specific legal implications. The participant collecting and storing the data is a data controller with all the attendant responsibilities. The participant/data controller would be required to comply with the local laws of the place where data is input into the search fields as well as where the controller is located. These obligations may include notice to searchers of data practices, heightened protection for sensitive data and limitations on data exports. The searcher, if an organization, may also qualify as a data controller, depending on the search interface and the methods for executing the search (e.g., staff member searches or a website makes the results available to anyone).
- **Mirrored common data set.** A design that involves sharing a common set of data with all participants whereby each participant locally stores the common data set would also have context-specific privacy implications. Each participating organization is a data controller and subject to its country's privacy rules and data export limitations. Those export limitations might even prevent participation because of global sharing. Similarly, notice and disclosure obligations are difficult to navigate, as would be data subject access and data security.
- **Central database.** A design that involves transferring data to a central repository will have clearer lines of responsibility and compliance, but a central repository potentially raises more difficult transborder export issues. The jurisdictional choice for the location of such a database is critical. For example, if the central database is located within the European Union, the legal restrictions on data exports will be challenging.

The MPCI should seek to highlight the specific legal needs for any design emerging by consensus and encourage the participants to steer toward more carefully balanced designs with compliance obligations that can be met. This might be accomplished by use of privacy impact assessments of emerging designs.

2. Coordinate the Privacy Policies of Collaborating Organizations

The MPCI should consider helping coordinate the privacy policies and ethical codes of conduct of collaborating organizations that process missing persons information. The coordination efforts should evolve over time to reflect the actual processing activities of the organizations and the changes in those processing activities. Although each missing persons organization must be responsible for its own privacy policies and for complying with applicable national laws, the MPCI can sponsor and share best practices for privacy using its existing collaboration methods.

Useful areas for best practices may include common definitions for terms, similar procedures for the exercise of data subject rights, and compatible rules for data termination. Coordination activities might also include an MPCI-sponsored shared library that contains relevant missing persons legislation, as well as privacy law interpretations that a collaborating organization receives from its Data Protection Authority. A common privacy code for missing persons data processing is a possibility and might also qualify for approval by EU data protection authorities under Article 27 of the EU Data Protection Directive as compliant with EU legal obligations.

3. Work with Data Protection Authorities and Other Governmental Agencies on Missing Persons Privacy Issues

This report identifies several areas where missing persons activities would benefit from authoritative interpretations of the EU Data Protection Directive. Similar issues may arise under the law in other jurisdictions. Bringing questions and problems to the attention of data protection authorities, including the Article 29 Working Party, can educate data protection authorities about the processing needs of missing persons data. Collaboration with data protection authorities can help identify ways to address information system needs with data protection objectives. In jurisdictions without data protection authorities, the MPCI may find it useful to address legal ambiguities with other government entities to help find appropriate responses to privacy and MPCI needs.

4. Be Prepared If the MPCI Ever Takes a Direct Role in the Processing of Missing Persons Information

Current MPCI activities do not include the direct or central processing of missing persons information by the MPCI itself. It is possible, however, that future developments might lead toward a more central structure for information or for information sharing. If missing persons activities develop in that direction, an MPCI role as a data controller would create compliance challenges. If and when appropriate, the MPCI should be ready to address new privacy obligations that would accompany that role. Privacy requirements for any centralized missing persons data would take time and effort to address. Selection of a location for any centralized functions would require deliberation. It is possible, for example, that a country with broadly compatible privacy laws and with a history of organizations engaged in missing persons activities might create a legislative environment specifically designed to address the privacy needs and requirements of a centralized missing persons.

5. Develop a Privacy Policy for the MPCI

Even if the MPCI does not directly process missing persons information, it may still need a privacy policy and professional code of conduct if the MPCI collects personal information. This may include a policy covering MPCI websites, the MPCI roster of participants, individual donors to the MPCI, and perhaps others.

B. Missing Persons Organizations

Because this report did not include reviews of individual organizations' compliance with privacy laws, the options listed here for missing persons organizations may reflect activities that many of the organizations have already considered and addressed.

1. Assure Legal Compliance

Each missing persons organization determines the extent to which it is a data controller or record keeper for purposes of identifying its legal obligations with respect to personal information. The design choices made by the organization will affect this determination. Each missing persons organization should then assure compliance with those obligations.

2. Take Responsibility for Privacy Policy

Each missing persons organization cooperating through the MPCI should have its own privacy policy that reflects its own personal data processing activities and its own legal requirements. The use of formal privacy impact assessments may be appropriate.

3. Coordinate Privacy Policies to the Extent Practicable

Each missing persons organization should coordinate its privacy policy with other similar organizations. The MPCI might provide the means for coordination and privacy policy document sharing. Different operations and different legal requirements may make it difficult or impossible for the same privacy policy to work for all organizations. Nevertheless, different organizations may be able to use common definitions for terms, similar procedures for the exercise of data subject rights, and compatible rules for data termination.

4. Share Official Interpretations and Guidance

Each missing persons organization should share interpretations of privacy law or guidance from data protection authorities. Each organization might also share other useful materials related to privacy, including new or changed privacy policies. This would be particularly beneficial for organizations with fewer resources, because those with greater expertise and funding could provide information (and models) that would otherwise be unattainable.

C. Data Protection Authorities

The world's data protection authorities created their own agenda for action in the 2011 resolution of the International Conference of Data Protection and Privacy Commissioners on Data Protection and Major Natural Disasters, which called on data protection authorities "to review whether their domestic data protection and privacy laws are suitably framed and flexible to best serve the vital interests of individuals in the event of a major natural disaster."[301]

[301] The text of the resolution appears in Appendix 1.

In any jurisdiction, the most appropriate response by a data protection authority might vary because of legal, structural, or other factors. The best response in any country might require a change in legislation, change in a policy directive, or formal publication of an interpretation of data protection law. To the greatest extent possible, it would be appropriate for data protection authorities to consult with all other relevant parties, including other government agencies, disaster relief organizations, and missing persons organizations, while developing a response to data protection and natural disaster problems. Consultations may be most effective when done in advance of an immediate need.

Other, more specific and more focused tasks might include:

1. Issue Specific or Generic Data Protection Response to Missing Persons or Natural Disaster Activities

While the New Zealand temporary code is a stellar example of an immediate, pointed, and useful response by a data protection authority to emergency needs, it will not always be possible for one or more data protection authorities to respond so promptly following a natural disaster. Disasters may disrupt the functioning of data protection authorities just as much as that of other institutions. Communications problems may make it difficult for a data protection authority to effectively convey a new policy or policy interpretation to data controllers.

It is appropriate for a national data protection authority to develop and adopt the advance guidance called for by the 2011 Data Protection Commissioners' Resolution.

Generic guidance, applicable to any natural disaster, may be the most useful action. If DPAs used their authority to address how data protection rules should be adjusted or interpreted in response any natural disaster, data controllers would know in advance what they may do without the need for immediate action by or consultation with one or more data protection authorities.

Guidance might take effect following a government's emergency declaration or equivalent. Adjustments authorized under generic guidance might remain in effect until the government declares an end to the emergency, a fixed period of time (with the possibility of extensions), an announcement by the relevant data protection authority, or other defined circumstances. For natural disasters directly affecting more than one country, a coordinated ending period may be appropriate.

Further, it may be appropriate to have several levels of generic guidance. A first level might apply when a natural disaster has a direct and immediate effect in a particular country and when broader relaxation of data protection rules may be more appropriate. A second level of guidance might apply when a natural disaster occurs near a country not directly affected by the disaster but that still receives refugees from the affected area. In this case, adjustments might be appropriate for refugees but not for citizens. A third level of guidance might apply when a disaster occurs in a third country geographically remote and the principal local consequences of the disaster are to its citizens or relatives of its citizens living in the disaster area. A different level of guidance might apply during the immediate aftermath of a natural disaster than during the long-term

circumstances that continue after responding to the most urgent consequences of a natural disaster.

2. Provide Interpretative Guidance

Action by European data protection authorities might be directly helpful in resolving ambiguities that exist in the EU Data Protection Directive. In some instances, action by European data protection authorities is required to allow some data processing activities. European data protection authorities and missing persons organizations may profitably work together to address these issues.

a) Legitimate Processing

The Directive requires that anyone processing personal data must respect privacy, must process data fairly and lawfully, and must have consent or a lawful reason to process the data. The Directive recognizes several purposes that make data processing legitimate, including when processing is "necessary to protect the vital interests of the data subject, for the performance of a task carried out in the public interest, or for the purposes of the legitimate interests pursued by the controller or by a third party." Action by one or more data protection authorities to clarify that these standards permit the processing needed to allow the work of missing persons organizations would be helpful to establish the legitimacy of that processing.

b) Sensitive Information

The EU Data Protection Directive requires Member States to include additional controls over the processing of sensitive information. Two provisions may be helpful to allow the processing of sensitive information that may be part of missing persons activities. One allows processing when "necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent." A second provision allows Member States for reasons of "substantial public interest" to establish exceptions by law or decision of the supervisory authority. Action by one or more data protection authorities to clarify these standards as transposed into national law could provide clear guidance that would allow information transfers needed to sustain the work of missing persons organizations.

c) Export Controls

Under the EU Data Protection Directive's data export controls, two provisions that might authorize information transfers use standards that appear to be applicable to missing persons activities. The first allows a transfer "necessary or legally required on important public interest grounds." The second provision allows a transfer "necessary in order to protect the vital interests of the data subject." Action by one or more data protection authorities to clarify these standards as transposed into national laws could provide guidance that would allow transfers needed to sustain the work of missing persons organizations.

D. Article 29 Working Party

The Article 29 Working Party provides advice and opinions regarding data protection issues arising under the EU Data Protection Directive and the members of the Article 29 Working Party are also members of the International Conference of Data Protection and Privacy Commissioners. The Article 29 Working Party can fulfill some objectives of the 2011 resolution by addressing disasters and data protection in its advice and opinions and by addressing these issues in its advice on the evolution of the proposed EU regulation.

1. Issue Interpretative Guidance

Like the data protection authorities, the Article 29 Working Party could issue interpretive guidance to help resolve the ambiguities that exist in the EU Data Protection Directive. Specifically, the Article 29 Working Party may consider issuing guidance in the areas of legitimate processing, sensitive information and export controls mentioned above.

2. Issue a Progress Report on the 2011 Resolution

Data protection authorities might regularly review and report on the progress of the action items in the 2011 resolution of the International Conference of Data Protection and Privacy Commissioners. As part of a report on progress toward providing advance guidance, it would be particularly useful for data protection authorities to address how they determine which organizations are involved in natural disaster responses, how privacy laws affect those organizations, and how data protection authorities might encourage those organizations to address privacy.

E. European Commission

In January 2012, the Commission of the European Union proposed comprehensive reform of the 1995 data protection rules with the goal of strengthening online privacy rights and boosting Europe's digital economy.[302] The proposal would replace national data protection laws that transposed the standards established by the EU Data Protection Directive with a single regulation on data protection that would apply throughout the European Union.[303]

The draft of the proposed rule under consideration refers in a recital to the possible need to restrict some data protection principles and rights in certain circumstances, "including the protection of human life especially in response to natural or man-made disasters."[304] This appears to be a useful step, responding perhaps to the 2011 Resolution of the Data Protection

[302] Press Release, European Commission, "Commission Proposes a Comprehensive Reform of the Data Protection Rules" (Jan. 25, 2012), http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[303] Press Release, European Commission, "Commission Proposes a Comprehensive Reform of the Data Protection Rules Increase Users' Control of Their Data and to Cut Costs for Businesses" (Jan. 25, 2012), http://europa.eu/rapid/searchAction.do (search "Optional Search Criteria: Reference" for "IP/12/46").
[304] *Commission Proposal for a Regulation of the European Parliament and of the Council On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),* at Recital 59, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Commissioners calling on international organizations to consider the issues arising from major natural disasters in their reviews of the international instruments on privacy and data protection.[305] As the proposed regulation is finalized, more direct statements or provisions clarifying the application of data protection rules to missing persons activities would be useful.

1. Address Personal Information Related to Missing Persons Activities and Natural Disasters in the New Regulation

The current focus in the recital on protecting human life in response to a disaster could be broadened to more clearly incorporate missing persons activities. Such activities may not rise to the level of protecting human life, but they do nevertheless warrant adjustment of data protection rules at least during emergency circumstances.

2. Provide More Specific Direction on Disaster and Missing Persons Activities

The development of a new regulation offers an opportunity to address ambiguities in the existing policy so that uncertainties do not carry over to a new regulation. It would be more efficient if the new EU data protection regulation expressly covered the need for temporary adjustments to data protection rules for disasters in general and for missing persons in particular. While the draft rule is still in process, it might be appropriate to add language specifically addressing disasters and associated missing persons activities. The Australian Privacy Act 1988, as amended in 2006, identifies three broad purposes for processing in emergencies and disasters: identifying individuals missing, injured, or affected by the event; assisting individuals involved in the event to obtain services; and informing appropriate individuals of the involvement of others in the event.[306] It may be advisable for the EU data protection regulation to recognize these three purposes as within the scope of allowable data processing.

F. United States

The US government's general privacy law for federal agencies—the Privacy Act of 1974—imposes broad restrictions on disclosure of personal information that might limit disclosures for disaster activities, either through substantive standards or procedural requirements. Following a disaster, some federal agencies may have personal information useful for missing persons activities, but the Act might limit or prevent sharing without additional effort. The law's limits could usefully change in two alternate ways.

---

[305] International Conference of Data Protection and Privacy Commissioners, Mexico City, Mex., Nov. 2-3, 2011, *Resolution on Data Protection and Major Natural Disasters*, 2011/GA/RES/004 (Nov. 1, 2011), *available at* http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_GA_RES_004_Natural_Disasters_ENG.pdf.

[306] Privacy Act 1988 (Cth) s 80H(2) (Austl.), *available at* http://www.comlaw.gov.au/Details/C2012C00414. The text of Australia's Privacy Act emergency provision appears in Appendix 3.

1. Authorize Missing Persons or Disaster Disclosures Using Existing Executive Branch Authority

The Privacy Act of 1974 allows agencies to authorize by regulation the disclosure of personal information from any system of records as defined routine uses. An agency that maintains information that might be useful following a disaster could establish an appropriate routine use within the limits of its legal authority.

The US government could also take broader action to allow for disaster or missing persons disclosures. One precedent comes from a 2007 Executive Branch response to the growing problem of identity theft. A presidentially established identity theft task force[307] offered ideas for agency responses that included the adoption by all federal agencies of a routine use to specifically permit the disclosure of information in connection with response and remediation efforts in the event of a data breach.[308] It may be possible under existing authority for agencies to adopt a similar routine use covering disasters and missing persons disclosures. A model routine use limited to missing persons activities only might authorize disclosure using language similar to this:

> Following a presidentially-declared disaster or a comparable disaster in another nation and for the purpose of assisting with investigating the whereabouts of, locating missing persons, or informing relatives and friends of the location and status of individuals affected by a natural disaster, records may be disclosed to (1) a federal, state, local, tribal, territorial, international, or foreign agency that coordinates natural disaster activities with the Federal Emergency Management Agency, or (2) a duly recognized U.S. or foreign entity that provides disaster assistance or missing persons services.

The adoption of this or a similar routine use statement could follow an Executive Order, instructions from the Office of Management and Budget, or an action taken by the head of any agency that maintains records useful for missing persons purposes. Because the promulgation of a new routine use can take months to accomplish, it is not practical for an agency to issue a new routine use in response to a particular disaster. To be prepared for any disaster, it would be appropriate for an agency to establish a routine use for appropriate systems in advance so the authority is available when needed.

2. Amend the Privacy Act of 1974 to Allow Disclosures Following Natural Disasters

The Privacy Act of 1974 restricts disclosure of personal information from systems of records maintained by federal agencies. The law allows certain types of disclosures from all systems, and these disclosures cover some standard activities, including archiving of records, use for research, and disclosure to Congress.[309] One provision allows a standard

---

[307] Exec. Order No. 13,402, 71 Fed. Reg. 27,945 (May 15, 2006), http://www.gpo.gov/fdsys/pkg/FR-2006-05-15/pdf/06-4552.pdf.

[308] The President's Identity Task Force, *Combating Identity Theft: A Strategic Plan* (Apr. 11, 2007), 30-31 http://www.identitytheft.gov/reports/StrategicPlan.pdf.

[309] 5 U.S.C. § 552a (b) (2006), *available at* http://www.law.cornell.edu/uscode/text/5/552a.

disclosure in compelling circumstances affecting health or safety of an individual. This particular disclosure is not broad enough to cover all disaster-related disclosures or missing persons disclosures. Congress could amend the Act to allow disclosures responsive to disaster or missing persons needs from all systems of records.

G. Other National or Sub-National Governments

The options addressed here apply to the United States and the European Union and grew out of this report's detailed analysis of privacy laws in those jurisdictions. This report establishes no specific analytic foundation on which to suggest detailed options for changes to laws in other jurisdictions. Nevertheless, it may also be appropriate that other governments adjust or amend their laws to address privacy and missing persons issues to allow for appropriate use of personal information for missing persons purposes following natural disasters.

VI. Conclusion

Missing persons activities that occur during natural disasters provide a valuable service to help reconnect people affected by disasters with their friends and families. These activities require, by their nature, a certain amount of information collection and sharing and this data processing must typically be done within urgent time frames.

These activities, therefore, present unique privacy problems. This report encourages missing persons organizations to recognize the privacy concerns implicated by their information sharing systems and balance the need for accessible data against the privacy interests of data subjects. Each entity must determine the system design that will best help it achieve its disaster relief efforts without impinging substantially on individual privacy rights. In addition, those involved in missing persons activities need to be aware of the privacy laws applicable to their actions and ensure legal compliance.

Finally, the various stakeholders and policy makers involved in missing persons activities and in privacy regulation should begin to take steps to (1) outline privacy friendly designs and practices that organizations can use to effectively share valuable information, (2) clarify the privacy obligations applicable to missing persons activities, and (3) amend current law or provide interpretive guidance in order to allow missing persons activities to proceed without the threat of legal liability.

Appendices

1. Summary of the Design Specifications and Database Systems of MPCI Member Organizations

2. NZ Christchurch Earthquake (Information Sharing) Code 2011 (Temporary)

3. Privacy Act 1988 (Australia), Part VIA—Dealing with personal information in emergencies and disasters

4. ICRC Recommendations for the Development of a Domestic Law on the Missing and Their Families

5. Table: Details and Specifications for Missing Persons Systems in Use

Appendix 1

Summary of the Design Specifications of MPCI Member Organizations

People Finder Interchange Format

Ka-Ping Yee, an engineer from Google, and a group of volunteers created the first draft of the People Finder Interchange Format (PFIF) in 2005 as means of assisting in the disaster relief efforts of Hurricane Katrina. The guiding purpose of designing PFIF was to reduce the difficulties associated with the automated aggregation and sharing of missing persons information.[310]

PFIF also standardizes data retention, which is one aspect of information privacy. To be compliant with the standard, all record creators must be able to set an expiration date for the permanent deletion of the record.[311]

Currently, Google,[312] the National Library of Medicine,[313] and MISSING.NET routinely share missing persons information using PFIF, including 60,000 PFIF records created after the 2010 Haiti earthquake and 600,000 after the 2011 Japan earthquake.[314] Ka-Ping Yee continues to maintain PFIF, with version 1.4 released May 29, 2012.[315]

Emergency Data Exchange Language

The US Department of Homeland Security (DHS) originally developed the EDXL Distribution Element in partnership with private and public disaster response and national security organizations. The stated purpose is "facilitat[ing] emergency information sharing and data exchange across the local, state, tribal, national and non-governmental organizations of different professions that provide emergency response and management services."[316] This EDXL standard requires all communications, regardless of purpose or content, to be encapsulated in a defined format for forwarding and display by any EDXL compliant device.[317]

---

[310] This purpose was articulated in a personal account of the development of the PFIF standard during the aftermath of Hurricane Katrina by David Geilhufe, a fellow participant in the disaster relief efforts. See David Geilhufe, "Personal History of the Katrina PeopleFinder Project Part I," *Social Source* (blog), Oct. 1, 2005, http://socialsource.blogspot.com/2005/10/personal-history-of-katrina.html.

[311] See "People Finder Interchange Format 1.4 Specification," Ka-Ping Yee, accessed July 23, 2012, http://zesty.ca/pfif/1.4/.

[312] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.

[313] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[314] Ka-Ping Yee, interview by Adam Elewa, Aug. 11, 2012 (on file with Fordham CLIP), PFIF Questionnaire, Fordham Law School, New York, NY.

[315] "People Finder Interchange Format 1.4 Specification," Ka-Ping Yee, accessed July 23, 2012. http://zesty.ca/pfif/1.4/.

[316] Org. for the Advancement of Structured Info. Standards [OASIS], *EDXL Distribution Element* (2006), 5-6, http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf.

[317] Org. for the Advancement of Structured Info. Standards [OASIS], *EDXL Distribution Element* (2006), 5-6, http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf.

The standard is currently maintained by OASIS,[318] a non-profit consortium that provides a structured forum for private and public organizations to reach consensus on guidelines for interoperability among products.[319] Numerous private and public organizations work within the deliberative framework established by OASIS to extend and customize EDXL standards for a wide range of emergency communications.[320] Given the scope of this report, the focus here extends only to EDXL standards for transmission of information about missing persons. Another relevant standard still in process is EDXL–Tracking of Emergency Patients (EDXL–TEP).[321] The driving concern in the development of EDXL–TEP was the needs of medical professionals. The National Association of State EMS Officials led the effort.[322] The types of emergencies for which EDXL–TEP could be used is broad, with anticipated uses ranging "across the EMS incident continuum of care" from routine car accidents to nationwide pandemics. The standard concerns missing persons because it gives medical professionals the ability to report the location of those involved in a disaster.[323]

[318] "OASIS Emergency Management Technical Committee," Org. for the Advancement of Structured Info. Standards [OASIS], accessed July 23, 2012, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency.
[319] OASIS About page, accessed July 23, 2012, https://www.oasis-open.org/org.
[320] "Emergency Data Exchange Language (EDXL) Overview," Org. for the Advancement of Structured Info. Standards [OASIS], accessed July 23, 2012, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency#overview.
[321] "Emergency Management Tracking of Emergency Patients (EM TEP) Subcommittee," Org. for the Advancement of Structured Info. Standards [OASIS], accessed July 23, 2012, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency-tep.
[322] Org. for the Advancement of Structured Info. Standards [OASIS], *EDXL-Tracking of Emergency Patients (TEP): Requirements and Draft Messaging Specification* (2010), 7, http://xml.coverpages.org/EDXL-TEP-Reqs-Draft-Messaging.pdf.
[323] Org. for the Advancement of Structured Info. Standards [OASIS], *EDXL-Tracking of Emergency Patients (TEP): Requirements and Draft Messaging Specification* (2010), 7, http://xml.coverpages.org/EDXL-TEP-Reqs-Draft-Messaging.pdf.

Appendix 2

NZ Christchurch Earthquake (Information Sharing) Code 2011 (Temporary)

http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/Christchurch-Earthquake-Information-Sharing-Code-2011-Temporary-incorporating-Amendments-No-1-and-No-2.doc

Christchurch Earthquake (Information Sharing) Code 2011 (Temporary)

I, MARIE SHROFF, Privacy Commissioner, now issue under section 51 of the Privacy Act 1993, and in accordance with section 52 of the Act, the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).

Issued by me at Wellington on 24 February 2011

The SEAL of the Privacy Commissioner was affixed to this Code of Practice by the Privacy Commissioner) *[L.S.]*

Marie Shroff
Privacy Commissioner

This version of the code contains notes which are set out in italics. This material is not part of the code but is intended to assist users.

***Note**: A code of practice issued under s.46 of the Privacy Act 1993 is deemed to be a regulation for the purposes of the Regulations Disallowance Act 1989 – Privacy Act, s.50.*

***Note:** This version of the Code incorporates Amendment No.1 and Amendment No 2.*

1. Title

This code of practice may be referred to as the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary).

***Note**: The code is identified as temporary as it has been issued under special urgency procedures – Privacy Act, s.52.*

2. Commencement and expiration

This code will:
(a) come into force on 24 February 2011 at 5pm;
[(b) expire on [30 June 2011].]

***Note:** The Code originally provided that it would expire 'on 24 May 2011'or on the date on which the emergency declaration terminates, whichever is the earlier'. Amendment No.1 omitted the words 'or on the date on which the emergency declaration terminates, whichever is the earlier'.*

***Note**: Amendment No 2 substituted 30 June 2011 as the expiry date.*

3. Interpretation

In this code:

Christchurch earthquake means the earthquake that occurred in Christchurch on 22 February 2011.

…

permitted purpose has the meaning set out in clause 4.

***Note**: Several terms used in the code are defined in the Privacy Act including e.g. agency, collect, enactment, individual, information privacy principle, news medium, personal information, public sector agency – Privacy Act, s.2.*

***Note**: Amendment No 2 deleted the definition of emergency declaration. This had provided 'emergency declaration means the declaration of a state of national emergency made on 23 February 2011 under the Civil Defence Emergency Management Act 2002'.*

4. Meaning of permitted purpose

(1) A *permitted purpose* is a purpose that directly relates to the government and local government response to the Christchurch earthquake emergency ….

***Note**: Amendment No 2 deleted the words 'in respect of which an emergency declaration exists'.*

(2) Without limiting subclause (1), any of the following is a permitted purpose in relation to the Christchurch earthquake emergency:
(a) identifying individuals who:
(i) are or may be injured, missing or dead as a result of the

emergency;

(ii) are or may be otherwise involved in the emergency;

(b) assisting individuals involved in the emergency to obtain services such as repatriation services, medical or other treatment, health services, financial and other humanitarian assistance;

(c) assisting with law enforcement in relation to the emergency;

(d) coordination and management of the emergency;

(e) ensuring that people who are responsible for individuals who are, or may be, involved in the emergency are appropriately informed of matters that are relevant to:

(i) the involvement of those individuals in the emergency; or

(ii) the response to the emergency in relation to those individuals.

(3) For the purposes of subclause (2), a person is responsible for an individual if the person is:

(a) a parent of the individual;

(b) a child or sibling of the individual and at least 18 years old;

(c) a spouse, civil union partner or de facto partner of the individual;

(d) a relative of the individual, at least 18 years old and a member of the individual's household;

(e) a guardian of the individual;

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health;

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

***Note**: This clause is based upon Privacy Act 1988 (Australia), Part VIA, in particular, s.80H.*

5. Authority for collection, use and disclosure of personal information

(1) In relation to the Christchurch earthquake emergency, an agency may collect, use or disclose personal information relating to an individual if the agency believes on reasonable grounds that:

(a) the individual concerned may be involved in the emergency; and

(b) the collection, use or disclosure is for a permitted purpose in relation to the emergency; and

(c) in the case of a disclosure of personal information - the disclosure is to:

(i) a public sector agency; or

(ii) an agency that is, or is likely to be, involved in managing, or assisting in the management of, the emergency; or

(iii) an agency that is directly involved in providing repatriation services, medical or other treatment, health services or financial or other humanitarian assistance services to individuals involved in the emergency; or

(iv) a person who is responsible for the individual (within the meaning of clause 4(3)); and

(d) in the case of a disclosure of personal information—the disclosure is not to a news medium.

***Note**: This subclause is based upon Privacy Act 1988 (Australia), Part VIA, in particular, s.80P.*

Note: *Questions of disclosure of personal information to the news media are not affected by this code and are subject to any normal legal considerations under the Privacy Act or other applicable law such as the Official Information Act 1982. This code applies no additional restrictions on such disclosures.*

(2) The authority in subclause (1) is in addition to, and does not restrict, any other authority for collection, use or disclosure contained in the information privacy principles, any code of practice or other enactment.

Explanatory note

This code modifies the application of the applicable information privacy principles by providing that agencies are authorised in certain circumstances to collect, use or disclose personal information for certain permitted purposes related to the government response to the Christchurch earthquake emergency.

Legislative history

24 February 2011	*Code issued*
24 February 2011 (5pm)	*Code commenced*
3 March 2011	*Code notified in NZ Gazette*
9 March 2011	*Amendment No.1 issued*
10 March 2011	*Amendment No.1 commenced*
17 March 2011	*Amendment No.1 notified in NZ Gazette*
13 May 2011	*Amendment No 2 issued*
19 May 2011	*Amendment No.2 commenced*
19 May 2011	*Amendment No.2 notified in NZ Gazette*

Appendix 3

Privacy Act 1988 (Australia) Part VIA—Dealing with Personal Information in Emergencies and Disasters

http://www.comlaw.gov.au/Details/C2012C00414

Division 1—Object and interpretation

80F Object

The object of this Part is to make special provision for the collection, use and disclosure of personal information in emergencies and disasters.

80G Interpretation

(1) In this Part:

duty of confidence means any duty or obligation arising under the common law or at equity pursuant to which a person is obliged not to disclose information, but does not include legal professional privilege.

emergency declaration means a declaration under section 0J or 80K.

permanent resident means a person, other than an Australian citizen:

(a) whose normal place of residence is situated in Australia; and

(b) whose presence in Australia is not subject to any limitation as to time imposed by law; and

(c) who is not an illegal entrant within the meaning of the *Migration Act 1958*.

secrecy provision means a provision of a law of the Commonwealth (including a provision of this Act), or of a Norfolk Island enactment, that prohibits or regulates the use or disclosure of personal information, whether the provision relates to the use or disclosure of personal information generally or in specified circumstances.

(2) For the purposes of this Part, a reference in the definition of ***personal information*** in subsection 6(1) to an individual is taken to include a reference to an individual who is not living.

80H Meaning of *permitted purpose*

(1) For the purposes of this Part, a ***permitted purpose*** is a purpose that directly relates to the Commonwealth's response to an emergency or disaster in respect of which an emergency declaration is in force.

(2) Without limiting subsection (1), any of the following is a ***permitted purpose*** in relation to an emergency or disaster:

(a) identifying individuals who:

(i) are or may be injured, missing or dead as a result of the emergency or disaster; or

(ii) are or may be otherwise involved in the emergency or disaster;

(b) assisting individuals involved in the emergency or disaster to obtain services such as repatriation services, medical or other treatment, health services and financial or other humanitarian assistance;

(c) assisting with law enforcement in relation to the emergency or disaster;

(d) coordination or management of the emergency or disaster;

(e) ensuring that people who are ***responsible*** (within the meaning of subclause 2.5 of Schedule 3) for individuals who are, or may be, involved in the emergency or disaster are appropriately informed of matters that are relevant to:

(i) the involvement of those individuals in the emergency or disaster; or

(ii) the response to the emergency or disaster in relation to those individuals.

Division 2—Declaration of emergency

80J Declaration of emergency—events of national significance

The Prime Minister or the Minister may make a declaration under this section if the Prime Minister or the Minister (as the case may be) is satisfied that:

(a) an emergency or disaster has occurred; and

(b) the emergency or disaster is of such a kind that it is appropriate in the circumstances for this Part to apply in relation to the emergency or disaster; and

(c) the emergency or disaster is of national significance (whether because of the nature and extent of the emergency or disaster, the direct or indirect effect of the emergency or disaster, or for any other reason) ; and

(d) the emergency or disaster has affected one or more Australian citizens or permanent residents (whether within Australia or overseas).

Note: A declaration under this section is merely a trigger for the operation of this Part and is not directly related to any other legislative or non-legislative scheme about emergencies.

80K Declaration of emergency—events outside Australia

(1) The Prime Minister or the Minister may make a declaration under this section if the Prime Minister or the Minister (as the case may be) is satisfied that:

(a) an emergency or disaster has occurred outside Australia; and

(b) the emergency or disaster is of such a kind that it is appropriate in the circumstances for this Part to apply in relation to the emergency or disaster; and

(c) the emergency or disaster has affected one or more Australian citizens or permanent residents (whether within Australia or overseas).

(2) The Minister must consult the Minister administering the *Diplomatic Privileges and Immunities Act 1967* before the Minister makes a declaration under this section.

Note: A declaration under this section is merely a trigger for the operation of this Part and is not directly related to any other legislative or non-legislative scheme about emergencies.

80L Form of declarations

(1) An emergency declaration must be in writing and signed by:

(a) if the Prime Minister makes the declaration—the Prime Minister; or

(b) if the Minister makes the declaration—the Minister.

(2) An emergency declaration must be published, as soon as practicable after the declaration has effect:

(a) on the website maintained by the Department; and

(b) by notice published in the *Gazette*.

(3) An emergency declaration is not a legislative instrument.

80M When declarations take effect

An emergency declaration has effect from the time at which the declaration is signed.

80N When declarations cease to have effect

An emergency declaration ceases to have effect at the earliest of:

(a) if a time at which the declaration will cease to have effect is specified in the declaration—at that time; or

(b) the time at which the declaration is revoked; or

(c) the end of 12 months starting when the declaration is made.

Division 3—Provisions dealing with the use and disclosure of personal information

80P Authorisation of collection, use and disclosure of personal information

(1) At any time when an emergency declaration is in force in relation to an emergency or disaster, an entity may collect, use or disclose personal information relating to an individual if:

(a) the entity reasonably believes that the individual concerned may be involved in the emergency or disaster; and

(b) the collection, use or disclosure is for a permitted purpose in relation to the emergency or disaster; and

(c) in the case of a disclosure of the personal information by an agency—the disclosure is to:

(i) an agency; or

(ii) a State or Territory authority; or

(iii) an organisation; or

(iv) an entity not covered by subparagraph (i), (ii) or (iii) that is, or is likely to be, involved in managing, or assisting in the management of, the emergency or disaster; or

(v) a person who is ***responsible*** for the individual (within the meaning of subclause 2.5 of Schedule 3); and

(d) in the case of a disclosure of the personal information by an organisation or another person—the disclosure is to:

(i) an agency; or

(ii) an entity that is directly involved in providing repatriation services, medical or other treatment, health services or financial or other humanitarian assistance services to individuals involved in the emergency or disaster; or

(iii) a person or entity prescribed by the regulations for the purposes of this paragraph; or

(iv) a person or entity specified by the Minister, by legislative instrument, for the purposes of this paragraph; and

(e) in the case of any disclosure of the personal information—the disclosure is not to a media organisation.

(2) An entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by subsection (1), unless the secrecy provision is a designated secrecy provision (see subsection (7)).

(3) An entity is not liable to any proceedings for contravening a duty of confidence in respect of a disclosure of personal information authorised by subsection (1).

(4) An entity that is an agency does not breach an Information Privacy Principle in respect of a collection, use or disclosure of personal information authorised by subsection (1).

(5) An entity that is an organisation does not breach an approved privacy code or a National Privacy Principle in respect of a collection, use or disclosure of personal information authorised by subsection (1).

(6) A collection, use or disclose of personal information by an officer or employee of an agency in the course of duty as an officer or employee is authorised by subsection (1) only if the officer or employee is authorised by the agency to collect, use or disclose the personal information.

(7) In this section:

designated secrecy provision means any of the following:

(a) sections 18 and 92 of the *Australian Security Intelligence Organisation Act 1979*;

(b) section 4 of the *Inspector-General of Intelligence and Security Act 1986*;

(c) section 39, 39A, 40 and 41 of the *Intelligence Services Act 2001*;

(d) a provision of a law of the Commonwealth prescribed by the regulations for the purposes of this paragraph;

(e) a provision of a law of the Commonwealth of a kind prescribed by the regulations for the purposes of this paragraph.

entity includes the following:

(a) a person;

(b) an agency;

(c) an organisation.

Appendix 4

ICRC Recommendations for the Development of a Domestic Law on the Missing and Their Families

This Appendix reproduces "Recommendations for the Development of a Domestic Law on the Missing and Their Families." ICRC prepared these recommendations in a 2003 report entitled *The Missing and Their Families: Summary of the Conclusions Arising from Events Held Prior to the International Conference of Governmental and Non-Governmental Experts*. The ICRC report resulted from studies and workshops the ICRC conducted with government representatives; other components of the International Red Cross and Red Crescent Movement; international, regional and national governmental and non-governmental organizations; experts; and families of missing persons to address the plight of persons missing as a result of armed conflict and internal violence and their relatives. The part of the recommendations geared towards domestic law was then reproduced in an October 2003 report, entitled *Recommendations for the Development of a Domestic Law on the Missing and Their Families*. Part 9 of the recommendations from the October 2003 report is included here because it relates to the management and protection of personal data in determining the fate of missing persons. While missing persons arising from armed conflicts or internal violence does not fall within the work of the MPCI, the proposed standard reflects basic data protection principles.

The recommendations on the protections for genetic information are included because genetic information may become more relevant in the future to "routine" missing persons activities.

Thirty-seven countries implemented some of these recommendations into their domestic laws relating to missing persons.[324] For example, Kyrgyzstan implemented ICRC's model provisions on personal data retention, recommended data processor access controls, as well as the rights of a data subject.[325] Bosnia and Herzegovina implemented recommended provisions on maintaining the accuracy of data, adding a verification process to ensure accuracy.[326]

[324] Int'l Comm. of the Red Cross, *International Humanitarian Law National Implementation: Implementing Laws and Regulations*, http://www.icrc.org/ihl-nat.nsf/ (follow "Implementing Laws & Regulations by keyword" hyperlink; then follow "Missing" hyperlink).
[325] Law of the Kyrgyz Republic on Information of a Personal Nature, bishkek no. 59 (2008), (Kyrg.), *available at* http://www.icrc.org/ihl-nat.nsf/ (follow "Implementing Laws & Regulations by keyword" hyperlink; then follow "Missing" hyperlink; then follow Kyrgyzstan; then follow Law on the Kyrgyz Republic on Information of a Personal Nature).
[326] Law on Missing Persons, art. 22 (2004) (Bosn. & Herz.), *available at* http://www.icrc.org/ihl-nat.nsf/ (follow "Implementing Laws & Regulations by keyword" hyperlink; then follow "Missing" hyperlink; then follow Bosnia & Herzegovina; then follow Law on Missing Persons).

Recommendations for the Development of a Domestic Law on the Missing and Their Families

This document is an extensive reproduction of Chapter V of the *ICRC Report: The Missing and their Families. Summary of the Conclusions arising from the Events held prior to the International Conference of Governmental and Non-Governmental Experts (19-21 February 2003)*. The present annex corresponds to paragraphs 28 to 36 of the original Report; the paragraph numbering hereunder has been modified to make the recommendations easier to follow.

1. KNOWING THE FATE OF THEIR RELATIVES

***

2. GENERAL PROTECTION

***

3. USE OF FORCE BY LAW ENFORCEMENT OFFICIALS

***

4. PROTECTION OF PERSONS DEPRIVES OF THEIR LIBERTY

***

5. COMMUNICATION BETWEEN FAMILY MEMBERS

***

6. TREATMENT OF THE DEAD AND GRAVES AND IDENTIFICATION OF HUMAN REMAINS

***

7. IDENTIFICATION AND THE COLLECTING AND FORWARDING OF INFORMATION

***

8. THE LEGAL SITUATION OF MISSING PERSONS AND OF THEIR RELATIVES

***

9. PROTECTION AND MANAGEMENT OF PERSONAL DATA

Protection of personal data: the principles described below should be incorporated into domestic law.

A. Personal data should be collected and processed fairly and lawfully.
   a. The method of collection should not be deceptive, fraudulent or contrary to the law. This implies that consent with respect to the collection of the data should not be obtained through deception.
   b. This principle should not prevent the collection from a third party of data that may have been gathered improperly or unlawfully, when the purpose of the data collection is considered to be overriding.
   c. It may be appropriate to make it mandatory to register certain databases containing personal data with a public authority.

B. The collection and use of personal data should be subject to the consent of the individual to whom the data relate.
   a. Consent should be freely given and informed. In particular, the purpose of the collection and the destination of the data, including their transfer to a third party, should be disclosed.
   b. In certain circumstances, the consent of the individual may be presumed or implied, in particular when the individual to whom the data relate cannot be reached and the collection of data is considered to be clearly in his/her best interest in the circumstances.
   c. The data may not be used, disclosed or transferred for purposes other than those for which they were collected without the consent of the person concerned, except if required by a substantial public interest or for the protection of the vital interests of the person concerned or of others.

C. The collection and processing of personal data should be limited to that which is necessary for the purpose identified at the time of collection, or beforehand.

D. Personal data should be collected, processed and stored with appropriate safeguards.
   a. Sensitive data should only be collected and processed with safeguards commensurate

with their sensitivity.

b. Personal data should be protected by physical and technical security measures to prevent loss and unauthorized access or disclosure.

c. The data controller should be accountable for compliance with the rules governing the protection of personal data.

d. A supervising authority should be established to monitor respect for data protection rules and to prescribe appropriate remedies in the event of a breach.

E. The personal data collected should be accurate, complete and updated as is necessary for the purpose for which they were used.

F. Personal data may not be used, disclosed or transferred for purposes other than those for which they were collected without the consent of the person concerned, except if required by a substantial public interest or for the protection of the vital interests of the person concerned or of others.

a. When the consent of the person cannot be practically or legally obtained, personal data may be transferred or disclosed without explicit consent where:

I. disclosure would serve a substantial and overriding public interest;

II. disclosure is required to prevent or lessen a serious or immediate threat to the health or safety of the individual concerned, or of other persons;

III. disclosure would clearly benefit the individual concerned.

b. When the consent of the person cannot be practically or legally obtained, public disclosure of personal data should be considered only if it manifestly serves to protect or to ensure the vital interests of the person concerned or of another person.

c. Personal data may only be transferred to third parties that respect the international standards applicable to the protection of personal data.

G. Personal data should be destroyed as soon as the purpose of their collection has been fulfilled, or when they are no longer needed. They may, however, be retained for a given period (to be defined) if required for the benefit of the individual to whom they relate or if they are essential for the performance of the humanitarian tasks of the organization that collected the data.

H. Access to personal data should be granted to the individual to whom the information relates. A right to challenge the accuracy and completeness of the data and to have them amended as appropriate should also be provided for.

a. The following general principles should govern access to personal data by the individual concerned:

I. all persons have to be informed of the existence, use and disclosure of personal information relating to them;

II. on request, a person has a right of access to that information and the right to obtain a copy;

III. all persons have the right to challenge the accuracy and completeness of the personal information relating to them and to have it amended as appropriate, or at least to have a notation placed on their file indicating their desire to have the information corrected;

IV. remedies should be provided for in case those rights are denied.

b. The controller of the files should be allowed to deny access, in part or totally, where the information sought:

I. contains references to other individuals or sources of information received in confidence, including information protected by confidentiality agreements concluded for a humanitarian purpose;

II. could be expected to seriously threaten an important public interest (national security, public order, etc.);

III. could be expected to be seriously detrimental to the interests of other persons;

IV. could impede or jeopardize the purpose for which the information was collected, including humanitarian purposes.

I. Where relevant, exceptions to the above-mentioned principles should be provided for when the purpose of the data collection and processing is the protection of the human rights and fundamental freedoms of the individual concerned or is connected to the

mandate and activities of the ICRC or an intergovernmental humanitarian organization.

J. In the context of the clarification of the fate of missing persons:
  a. the collection and processing of personal data should be considered a lawful purpose;
  b. the primary objectives of collecting data are:
    I. to establish the identity, location, conditions and fate of:
      i. living persons who are unaccounted for;
      ii. deceased persons who are unaccounted for;
    II. to give information to the families on the whereabouts, condition and fate of their lost relatives;
  c. the personal data collected (for instance, *ante mortem* and *post mortem* data) on:
    I. living persons who are unaccounted for might include:
      i. administrative data (name, place of residence, etc.);
      ii. qualitative data (professional details, activities, known whereabouts, etc.);
      iii. physical and biological data (sex, age, description, etc.);
    II. deceased persons who are unaccounted for (human remains) might include:
      i. administrative data (name, place of residence, etc.);
      ii. qualitative data (professional details, activities, known whereabouts, etc.);
      iii. physical and biological data (sex, age, description, etc.), including DNA information;
    III. families and relatives might include:
      i. administrative data (name, place of residence, etc.);
      ii. DNA information collected and used in conformity with applicable principles;
  d. data collected for purposes other than to clarify the fate of missing persons may be disclosed or used only if:
    I. their disclosure and use are not incompatible with the purpose for which the data were collected or obtained; or
    II. the data were derived from publicly accessible sources (such as public registers, professional registers or published directories); or
    III. their disclosure and use are in the vital interest of the individual to whom the data relate or of a close relative, and the individual is physically or legally incapable of consenting to the disclosure;
  e. once the data have been collected, their processing may include:
    I. matching of information from different sources;
    II. public disclosure of collected information, subject to the applicable rules;
    III. *ante* and *post mortem* data analysis and matching;
    IV. DNA analysis and matching;
    V. providing information on the results of the process, subject to the applicable rules, possibly to:
      i. living persons who are unaccounted for (when found);
      ii. families and relatives;
      iii. the public authorities;
      iv. private organizations.

Protection of genetic information: the following principles should be incorporated into domestic law.

A. The collection, use and disclosure of DNA profiles should be subject to the rules relative to the protection of personal data, in particular the management, use, storage and transfer of DNA samples and profiles.

B. Identification of human remains through DNA typing should only be undertaken when other investigative techniques of identification are not adequate. The application of this principle does not preclude the taking of samples in order to perform DNA analysis at a later stage, in the event that other investigative techniques prove fruitless.

C. DNA information collected to identify missing persons or human remains may only be used or

disclosed for that specific purpose. In particular, the use of DNA analyses to derive or disclose health information or personal characteristics (except gender) other than those required for the purposes of identification should be prohibited.

D. DNA samples may only be collected and analysed with the informed consent of the individual, except where an overriding public interest dictates otherwise.
   a. Consent should be freely given and informed.
   b. Consent may be implied when it cannot be physically or legally obtained, in particular in circumstances where human remains are unidentified.
   c. DNA samples and analyses may not be used, disclosed or transferred for purposes other than those for which they were collected without the consent of the person concerned, except if required by a substantial public interest or for the protection of the vital interests of the person concerned or of others.

E. DNA samples and profiles should be destroyed / deleted when the missing persons have been identified, unless they are required for related purposes.

F. Forensic procedures should be carried out by an appropriately qualified person. Domestic law and regulations should determine the categories of persons authorized to carry out forensic procedures.

G. DNA samples, profiles and records should be adequately protected from unauthorized access and use.
   a. Protection should include both physical and technical / electronic security measures.
   b. The processing of DNA samples and profiles should be independent of the processing of *ante* and *post mortem* data.
   c. A unique anonymous reference should be the only link between DNA samples and profiles, on the one hand, and *ante* or *post mortem* data on the other. The link should only be accessible to the controllers of *ante* and *post mortem* data.

H. DNA analyses should only be performed by certified or accredited laboratories. A procedure for the regular supervision of accredited laboratories should be established. Certified laboratories should meet the following criteria:
   a. high level of professional knowledge and skill, scientific integrity, and appropriate quality control procedures;
   b. adequate security of the installations and of the substances under investigation;
   c. adequate safeguards to ensure absolute confidentiality in respect of the identity of the person to whom the DNA analysis relates.

I. DNA profiles or samples should only be disclosed, transferred or compared in the context of international cooperation for the purpose of identification, and only with the consent of the persons concerned.
   a. The authorities who transfer data should specify the permissible uses and disclosures by the recipient and receive valid assurances from the recipient that the information will be used and disclosed accordingly, and that applicable standards on the protection of personal data will be respected.
   b. DNA samples should not be transferred abroad except where the analysis is to be performed abroad.

Appendix 5

Details and Specifications for Missing Persons Systems in Use

Policies and Procedures of Database System Controllers

	Google Person Finder	**American Red Cross "Safe And Well"**	**Family Links Database**	**Lost Person Finder Project**	**MISSING.NET**
Controlling Organization	Google, Inc.	American Red Cross	International Committee of The Red Cross (ICRC)	US National Library of Medicine (NLM)	Red Helmets Foundation
Physical Location	Data could be stored in any one of Google's data centers.[327]	Denver, Colorado[328]	Geneva, Switzerland	Bethesda, Maryland	Paris, France
Web Address	http://google.org/personfinder/global/home.html	https://safeandwell.communityos.org/cms/index.php	http://www.icrc.org/familylinks	http://lpf.nlm.nih.gov	http://www.missing.net/disasters/
Privacy Polices	Google's Universal Privacy Policy: https://www.google.com/intl/en/policies/privacy/ No system specific policy. However, FAQs addressing privacy issues:	Red Cross's Universal Privacy Policy: http://www.redcross.org/en/privacy/ No system specific policy. However,	ICRC's Universal Privacy Policy: http://www.icrc.org/eng/home/privacypolicy/index.jsp System Specific	System Specific Privacy Policy: https://pl.nlm.nih.gov/privacy	System Specific Privacy Policy: http://www.missing.net/media/files/Confidentiality-Charter-MISSING.NET.pdf

[327] Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.
[328] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.

	https://support.google.com/personfinder/?hl=en	FAQs addressing privacy issues: https://safeandwell.communityos.org/cms/faq	Policy: http://www.icrc.org/familylinks (See right: "Privacy and Accuracy")		
Data Sources	People impacted by disasters enter information into Person Finder. Data is available to the public and viewable and usable by anyone. Google does not review or verify the accuracy of this data and users can update their records at any time.[329]	Individuals affected by disasters report their status by using either web interface or paper form with assistance of Red Cross volunteer. Data is never verified, and it can be modified by data subject at anytime.	*Publication of Missing Person List:* The main sources of testimonies are families of the missing interviewed by ICRC staff. ICRC also collects data from various humanitarian agencies such as UNICEF, Save the Children, as well as National Societies volunteer groups, and local authorities. ICRC verifies that data to the greatest degree possible under the circumstances	*Hospital-Based Events:* Medical personnel submit data about incoming patients through the website or a specialized application developed by NLM.[332] *Community-Based Events:* Voluntarily submitted by medical and relief personnel or members of the public who are seeking family members, friends, or other loved	Data submitted by unverified, registered internet users seeking missing persons or professional emergency personnel.[335] MISSING.NET confirms the identity of any user claiming to be a professional emergency worker, and denotes the source of submitted information in each missing person record.[336] -OR-

[329] Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.

			before publishing it.[330] *User Driven Service:* Unverified, registered internet users submit data either about their own status, or as a means to inquiry about the status of a person thought to be missing. ICRC will also input data from official list published by other organizations.[331] However, only	ones, through the website or by means of either a specialized application developed by NLM for the iPhone (other platforms are under development) or submit to NLM by e-mail via computer or cell phone.[333] The system also routinely pulls information from other publicly available systems that collect and	Pulled from the Google Person Finder database using API.[337]

[332] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[335] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[336] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.
[330] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[331] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[333] Proposed Collection: Lost People Finder System, 75 Fed. Reg. 6207 (Feb. 8, 2012), http://www.gpo.gov/fdsys/pkg/FR-2010-02-08/pdf/2010-2691.pdf.
[337] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.

			ICRC workers, after performing due diligence, can change a record to deceased. ICRC does not typically display deceased status on the web, instead working with local authorities to find a more appropriate and sensitive way to make the announcement.	store missing person information (i.e., Google Person Finder instances).[334]	
Limitations and Restrictions on Accessing Data	**Accessing Data From Internet:** Database allows "wildcard" searches, allowing multiple records to be returned by inputting the first few letters of name of missing person.[338] **Receiving Copy of Entire Database:**	**Accessing Data From Internet**: Records are not displayed unless user knows the name and either address or phone number contained in the record.[341]	**Accessing Data From Internet:** All records can be displayed without knowing any information. **Receiving Copy of Entire Database:**	**Accessing Data From Internet:** *Hospital-Based Events*: Viewed in the context of hospital policies, reflective of US HIPAA privacy constraints and HIPAA waivers	**Accessing Data From Internet**: All records can be displayed without knowing any information. **Receiving Copy of Entire**

[334] Proposed Collection: Lost People Finder System, 75 Fed. Reg. 6207 (Feb. 8, 2012), http://www.gpo.gov/fdsys/pkg/FR-2010-02-08/pdf/2010-2691.pdf.
[338] For example, searching for "Ad" would display all records for a missing person by the name of "Adam" as well as records for those with the first name "Adly". The exact number of letters required to display all relevant records varies according to language of submitted names. Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.
[341] "American Red Cross FAQs," accessed July 23, 2012, https://safeandwell.communityos.org/cms/faq.

	Google issues Application Programming Interface (API) keys, granting third party software developers the right and ability to make copies of all records in the database.[339] Google generally requires those requesting API keys to be a government organization, quasi-governmental entity, or established non-profit actively responding to the crisis in question. The Person Finder API TOS requires that recipients of the data use it only for non-commercial purposes, abide by Google's API Terms of Service, and commit to storing records obtained through the API in compliance with the expiry mechanisms set forth in Section 3.3 of the PFIF 1.3 specification.[340]	**Receiving Copy of Entire Database:** Data is not released to third parties. However, there are circumstances where the Red Cross might share some information with emergency personnel if it will be of use in a life-threatening situation. [342]	*Publication of Missing Person List*: Data may be disclosed to third parties, but only after the ICRC performs an investigation into how the third party plans to use and store the data, and an agreement is made limiting the use of the data.[343] *User Driven Service*: Data is not released to third parties.[344]	available during large-scale disasters.[345] *Community-Based Events*: Public portions of all records can be displayed without knowing any information. **Receiving Copy of Entire Database**: *Hospital-Based Events*: Only partnering hospitals can receive data.[346] *Community-Based Events*: Information submitted directly	**Database**: MISSING.NET issues Application Programming (API) keys, granting third party software developers the right and ability to retrieve records from database. All third parties who retrieve records must comply with certain terms and conditions. Notably, all parties who receive a copy of the database must delete the data two months after MISSING.NET determines the disaster to be

[339] "Google Person Finder API Key Request," accessed July 24, 2012, https://support.google.com/personfinder/bin/request.py?&contact_type=pf_api.
[340] Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.
[342] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.
[343] As a general principle, ICRC will share a set of data with a party only after an agreement and when (1) the scope, objectives and processes (notably for data publication, deletion, correction, transfer, archiving and for communication to beneficiaries and other actors) are clear; (2) the purpose is humanitarian only and not different from the purpose under which these data were initially collected by ICRC; (3) it is in the best interest of the beneficiaries; (4) beneficiaries are informed and consent; 5) it is not detrimental to ICRC activities and reputation (as an independent, impartial and neutral humanitarian organization); 6) the party

				to NLM's Lost People Finder System could be transferred to other systems that are endorsed by US government agencies. [347]	ended and the MISSING.NET service no longer useful to disaster relief efforts.[348]
Policies Regarding Cross-Border Data Exports	N/A	N/A	The sites privacy policy does not say anything about cross data exports. The MPCI doc simply says that third parties, among other things, must respect data protection principles/regulation before they can	N/A	Yes, privacy policy guaranteeing a level of security at least equivalent to that offered by European regulations on the protection of personal data.[349]

respects data protection principles/regulations; and (7) the party commits to not share data with other actors without ICRC prior consent. See Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.

[344] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.

[345] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[346] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.

[347] Proposed Collection: Lost People Finder System, 75 Fed. Reg. 6207 (Feb. 8, 2012), http://www.gpo.gov/fdsys/pkg/FR-2010-02-08/pdf/2010-2691.pdf.

[348] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.

[349] "MISSING.NET Confidentiality Charter," accessed July 24, 2012, http://www.missing.net/media/files/Confidentiality-Charter-MISSING.NET.pdf.

			receive data."		
Data About Children	Users are not required to submit age information about individuals they are searching for, and Google does not verify the accuracy of the information submitted. Google does not segment the database based on age.[350]	No set policy.[351]	Data is collected about children, but the ICRC does not display the location or contact details of children.[352]	Data is collected about children. *Hospital-Based Events:* NLM supportive of hospital policies that treat data of children more sensitively.[353] *Community-Based Events:* No set policy yet.[354]	Data is collected about children.[355]
Database Becomes Active (accepts new	Discretion of Google Crisis Response team. Team considers usefulness of tool for given disaster.[356]	Always active.[357]	Discretion of ICRC team. Team considers the risk/utility of	*Hospital-Based Event:* No set policy yet. Never launched before,	Overall database always active, but event allowing submission of data

[350] Dorothy Chou (Google), interview by Adam Elewa, Aug. 15, 2012 (on file with Fordham CLIP), Google Interview, Fordham Law School, New York, NY.
[351] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.
[352] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[353] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[354] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[355] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[356] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[357] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.

data)			launching. [358]	only used in drills.[359] *Community-Based Event:* The creation of a new "event" allowing the submission of data occurs at the discretion of the NLM staff.[360]	started at discretion of MISSING.NET team.[361]
Database Becomes Non-Active (no new data accepted)	Discretion of Google Crisis Response team. Team considers whether "normal" forms of communication have resumed.[362]	Always active.[363]	*Publication of Missing Person List*: No set limit. Persons will be added to the list as they are reported missing.[364] *User Driven*	No set policy yet. Preliminary policy of 1 – 2 years.[366]	After MISSING.NET determines a disaster to be ended for the purposes of the service, no new records can be submitted concerning that

[358] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[359] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[360] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[361] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[362] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[363] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.
[364] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.

			Service: Database is taken offline at the discretion of ICRC team. Team considers whether normal communications have resumed, and whether the database is still needed.[365]		disaster event.[367] New user accounts containing information of submitting party can always be created.[368]
Data Contained in Database No Longer Publically Readable/Searchable	Record can be submitted with expiration date, after which the record is deleted in accordance with Google's Privacy Policy.[369] -OR- After the immediate crisis has passed and more usual forms of communication are able to serve users' needs, Google's Crisis Response team takes	Records expire, and are permanently deleted, after 365 days.[371]	*Publication of Missing Person List:* No set limit. Records can stay online indefinitely. ICRC respects wishes of the missing person's family.[372] *User Driven Service*: Database	No set policy yet. Preliminary policy of 3 years.[374]	Records regarding missing person deleted two months after MISSING.NET determines the disaster to be ended and the MISSING.NET service no longer useful to disaster relief efforts.[375]

[366] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[365] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[367] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[368] MISSING.NET, interview by Missing Persons Community of Interest, Nov. 2011 (on file with Fordham CLIP), MISSING.NET Questionnaire, Fordham Law School, New York, NY.
[369] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.

	down the Google Person Finder instance, and deletes the data in accordance with Google's Privacy Policy.[370]		is taken offline at the discretion of ICRC team. Team considers whether normal communications have resumed, and whether the database is still needed.[373]		User accounts containing information about submitting party are never deleted, but are also never publically viewable.[376]
Data in Database Permanently Deleted	Record can be submitted with expiration date, after which the record is deleted in accordance with Google's Privacy Policy.[377] -OR-	Records expire, and are permanently deleted, after 365 days.[379]	After closure of family links website, ICRC decides whether to archive records at ICRC headquarters in Geneva. ICRC has no policy	No set policy yet. No preliminary policy either.[381]	Records regarding missing person deleted after two months two months after MISSING.NET determines the disaster to be

[371] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.
[372] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[374] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[375] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.
[370] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[373] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[376] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.
[377] "Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en.
[379] Sharon Hawa (senior associate of mass care, American Red Cross), interview by Adam Elewa, July 20, 2012 (on file with Fordham CLIP), Red Cross Questionnaire, Fordham Law School, New York, NY.

	After the immediate crisis has passed and more usual forms of communication are able to serve users' needs, Google's Crisis Response team takes down the Google Person Finder instance, and deletes the data in accordance with Google's Privacy Policy.[378]		regarding how long data should be archived.[380]		ended and the MISSING.NET service no longer useful to disaster relief efforts.[382] User accounts containing information about submitting party are never deleted, but are also never publically viewable.[383]

[381] US National Library of Medicine, interview by Missing Persons Community of Interest, Nov. 10, 2011 (on file with Fordham CLIP), NLM Questionnaire, Fordham Law School, New York, NY.
[378]"Google Person Finder FAQs," accessed July 23, 2012, https://support.google.com/personfinder/?hl=en..
[380] Romain Bircher (head of Data Management and Restoring Family Links unit, International Committee of the Red Cross), interview by Missing Persons Community of Interest, Nov. 29, 2011 (on file with Fordham CLIP), ICRC Questionnaire, Fordham Law School, New York, NY.
[382] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.
[383] Sarah Aizenman (MISSING.NET), interview by Adam Elewa, Aug. 13, 2012 (on file with Fordham CLIP), MISSING.NET Interview, Fordham Law School, New York, NY.

Notable Data Fields of Database Specifications and Database Systems

KEY

Limitations and Restrictions on Accessing Data	
Data Is Publicly Searchable	**P**
Data Is Private/Not Disclosed	**X**
Data Is Not Disclosed/Treated Sensitively When Concerning A Child	**x**
Data Entry	
Required	**R**
Optional	**O**
Data Entry Method	
User Must Select From List	**( )**
User Can Enter Any Text	**__**

	Google Person Finder	**Red Cross "Safe And Well"**	**Family Links Database**	**Lost Person Finder Project**	**MISSING.NET**	**People Finder Interchange Format (PFIF)**	**Emergency Data Exchange Language (EDXL): Tracking of Emergency Patients (TEP)**
Data Collected Regarding Missing Person			**Publication of missing person list:** **"Self Registration" Service:**	**Hospital Based Events:** **Community Based Events:**			
First Name	**P, R, __**	**P, R, __**	**P, R, __** **P, R, __**	**X, O, __** **P, O, __**	**P, R, __**	**P, R, __**	**X, O, __**
Last Name	**P, R, __**	**P, R, __**	**P, R, __** **P, R, __**	**X, O, __** **P, O, __**	**P, R, __**	**P, R, __**	**X, O, __**
Farther or Mother's Name / "Family Name"	**P, O, __**		**P, R, __** **P, R,__**			**P, O, __**	

Sex/Gender	**P, O, __**		**P, R, ( )** _____ **P, R, ( )**	**X, O, __** _____ **P, O, __**	**P, O, __**	**P, O, __**	**X, R, __**
Age/Date of Birth	**P, O, __**	**P, O, __**	**P, O, __** _____ **P, R, __**	**X, O, ( )** _____ **P, O, ( )**	**P, O, __**	**P, O, __**	**X, R, __**
Hair Color	**P, O, __**			**X, O, __** _____ **P, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Eye Color	**P, O, __**			**X, O, __** _____ **P, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Weight	**P, O, __**			**X, O, __** _____ **P, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Distinguishing Marks/Clothing	**P, O, __**			**X, O, __** _____ **P, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Nationality					**P, O, __**		**X, O, __**
Home Address: Street	**P, O, __**	**X, R, __**		**X, O,__** _____ **X, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Home Address: City	**P, O, __**	**X, R, __**		**X, O, __** _____	**P, O, __**	**P, O, __**	**X, O, __**

				X, O, __			
Home Address: State	**P, O, __**	**X, R, __**		_____ **X, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Home Address: Country	**P, O, __**	**X, R, __**		_____ **X, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Home Address: Zip	**P, O, __**	**X, R, __**		_____ **X, O, __**	**P, O, __**	**P, O, __**	**X, O, __**
Photo	**P, O**		**P, O, __** _____	**X, R** _____ **P, O**	**P, O**	**P, O**	**X, O**
Status (e.g., alive, dead, found,etc.)	**P, O, ( )**	**P, R, ( ) or __**	**P, R, ( )** _____ **P, R, ( )**	**X, R, ( )** _____ **P, O, ( )**		**P, O, ( )**	**X, R, ( ) or __**
Medical Needs/Allergies							**X, O, __**
Current/Last Seen Location	**P, O, __**	**X, R, __**	**P/x, O, __** _____ **P/x, R, __**	**X, R, ( )** _____ **P, R, ( )**	**P, O, __**	**P, O, __**	**X, O, __**
Email	**P, O, __**	**X, O, __**	_____ **P/x, R, __**			**P, O, __**	**X, O, __**
Phone #	**P, O, __**	**X, O,**				**P, O, __**	**X, O, __**

		__	**P/x, R, __**				
Language Spoken					**P, O, __**		**X, O, __**
Data Collected Regarding Seeker							
First Name	**P, O, __**		**P or X, O, __** **P, R, __**	**X, R, __**	**X, O, __**	**P, O, __**	
Last Name	**P, O, __**		**P or X, O, __** **P, R, __**	**X, R, __**	**X, O, __**	**P, O, __**	
Relationship to Missing			**P, O, ( )** **P, R, ( )**				
Email	**P, O, __**		**X, R, __**	**X, R, __**	**X, R, __**	**P, O, __**	
Phone #	**P, O, __**		**X, R, ___**		**X, O, __**	**P, O, __**	
Home Address: Street			**X, O, __**		**X, R, __**		

Home Address: City			**P, R, __**		**X, R, __**		
Home Address: State			**P, O, __**		**X, R, __**		
Home Address: Country			**P, R, ( )**		**X, R, __**		
Home Address: Zip					**X, O, __**		